Cisco Wireless Controller Configuration Guide, Release 8.8

First Published: 2018-08-17

Last Modified: 2020-09-16

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018–2020 Cisco Systems, Inc. All rights reserved.

CONTENTS

Full Cisco Trademarks with Software License ?

PREFACE

Preface liii

Audience liii

Conventions liii

Related Documentation liv

Communications, services, and additional information lv

Cisco Bug Search Tool lv

Documentation feedback lv

PART I

Overview 57

CHAPTER 1

Cisco Wireless Solution Overview 1

Core Components 2

Overview of Cisco Mobility Express 3

CHAPTER 2

Initial Setup 5

Cisco WLAN Express Setup 5

Setting up Cisco Wireless Controller using Cisco WLAN Express (Wired Method) 8

Default Configurations 10

Configuring the Controller Using the Configuration Wizard 11

Configuring the Controller (GUI) 11

Configuring the Controller—Using the CLI Configuration Wizard 22

Using the AutoInstall Feature for Controllers Without a Configuration 25

Managing the Controller System Date and Time 26

Restrictions on Configuring the Controller Date and Time 26

Configuring the Date and Time (GUI) 26
Configuring the Date and Time (CLI) 28

PART II Management of Controllers 31

CHAPTER 3 Administration of Controller 33
Using the Controller Interface 33
Using the Controller GUI 33
Guidelines and Restrictions on using Controller GUI 34
Logging On to the GUI 34
Logging out of the GUI 35
Using the Controller CLI 35
Logging on to the Controller CLI 35
Using a Local Serial Connection 35
Using a Remote Telnet or SSH Connection 36
Logging Out of the CLI 37
Navigating the CLI 37
Enabling Web and Secure Web Modes 38
Enabling Web and Secure Web Modes (GUI) 39
Enabling Web and Secure Web Modes (CLI) 39
Telnet and Secure Shell Sessions 41
Configuring Telnet and SSH Sessions (GUI) 42
Configuring Telnet and SSH Sessions (CLI) 42
Configuring Telnet Privileges for Selected Management Users (GUI) 44
Configuring Telnet Privileges for Selected Management Users (CLI) 44
Management over Wireless 44
Enabling Management over Wireless (GUI) 45
Enabling Management over Wireless (CLI) 45
Configuring Management using Dynamic Interfaces (CLI) 46

CHAPTER 4 Monitoring Dashboard 47
Monitoring Dashboard 47
Numerical Statistics 48
Graphical Widgets 48

Network Summary 50
Network Summary—Access Points 50
Network Summary—Clients 50
Rogues 51
Rogue Access Points 51
Rogue Clients 51
Interferers 51
Wireless Dashboard 52
AP Performance 52
Client Performance 52
Best Practices 52

CHAPTER 5 **Managing Licenses** 53
Cisco Wireless Controller Licensing 53
Installing a License 54
Installing a License (GUI) 54
Installing a License (CLI) 55
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) 60
Troubleshooting Licensing Issues 60
Activating an AP-Count Evaluation License 60
Information About Activating an AP-Count Evaluation License 60
Activating an AP-Count Evaluation License (GUI) 61
Activating an AP-Count Evaluation License (CLI) 61
Cisco Smart Software Licensing 63
Guidelines and Restrictions for Using Cisco Smart Software Licensing 63
Configuring Cisco Smart Software Licensing (GUI) 65
Configuring the Cisco Smart Software Licensing on Controller (CLI) 65
Updating DNS IP Address for Cisco Smart Software Licensing (CLI) 66
Right to Use Licensing 67

Configuring Right to Use Licensing (GUI) 68
Configuring Right to Use Licensing (CLI) 68
Rehosting Licenses 69
Information About Rehosting Licenses 69
Rehosting a License 69
Rehosting a License (GUI) 69
Rehosting a License (CLI) 71
License Agent 72
Configuring the License Agent (GUI) 72
Configuring the License Agent (CLI) 73
Call-Home 74
Configuring Call-Home (GUI) 75
Configuring Call-Home Parameters (CLI) 76
Retrieving the Unique Device Identifier on Controllers and Access Points 77
Retrieving the Unique Device Identifier on Controllers and Access Points (GUI) 78
Retrieving the Unique Device Identifier on Controllers and Access Points (CLI) 78

CHAPTER 6 **Managing Software** 79
Upgrading the Controller Software 79
Guidelines and Restrictions for Upgrading Controller Software 79
Upgrading Controller Software (GUI) 81
Upgrading Controller Software (CLI) 83
Predownloading an Image to an Access Point 85
Access Point Predownload Process 86
Guidelines and Restrictions for Predownloading an Image to an Access Point 87
Predownloading an Image to Access Points—Global Configuration (GUI) 88
Predownloading an Image to Access Points (CLI) 88
Bootloader and Recovery Image 90
Configuring Boot Order (GUI) 91
Recovering an Access Point Using TFTP 91

CHAPTER 7 **Managing Configuration** 93
Resetting the Controller to Default Settings 93
Resetting the Controller to Default Settings (GUI) 93

Resetting the Controller to Default Settings (CLI) 94
Saving Configurations 94
Editing Configuration Files 94
Clearing the Controller Configuration 96
Restoring Passwords 96
Rebooting the Controller 97
Transferring Files to and from a Controller 97
Backing Up and Restoring Controller Configuration 97
Uploading Configuration Files 98
Downloading Configuration Files 100
Downloading a Login Banner File 102
Downloading a Login Banner File (GUI) 103
Downloading a Login Banner File (CLI) 104
Clearing the Login Banner (GUI) 105
Uploading Diagnostic Support Bundle 105
Uploading Diagnostic Support Bundle (GUI) 105
Uploading Diagnostic Support Bundle (CLI) 106

CHAPTER 8 **Network Time Protocol Setup** 107
Authentication for the Controller and NTP/SNTP Server 107
Guidelines and Restrictions on NTP 107
Configuring the NTP/SNTP Server to Obtain the Date and Time (GUI) 108
Configuring the NTP/SNTP Server to Obtain the Date and Time (CLI) 108
Configuring NTPv4 Keys for Authentication (GUI) 109

CHAPTER 9 **High Availability** 111
Information About High Availability 111
Restrictions for High Availability 115
Configuring High Availability (GUI) 118
Enabling High Availability (CLI) 120
Configuring High Availability Parameters (CLI) 121
Troubleshooting Tips for IPsec Encryption for High Availability 122
vWLC and N+1 High Availability 123
Adding a Hash Key to a Cisco vWLC (GUI) 123

Adding a Hash Key to Cisco vWLC (CLI) 124
Monitoring High Availability Standby Controller 125
Replacing the Primary Controller in an HA Setup 126

CHAPTER 10 Managing Certificates 129
Information about Loading an Externally Generated SSL Certificate 129
Loading an SSL Certificate (GUI) 130
Loading an SSL Certificate (CLI) 130
Downloading Device Certificates 131
Downloading Device Certificates (GUI) 132
Downloading Device Certificates (CLI) 133
Uploading Device Certificates 134
Uploading Device Certificates (GUI) 134
Uploading Device Certificates (CLI) 135
Downloading CA Certificates 136
Download CA Certificates (GUI) 136
Downloading CA Certificates (CLI) 137
Uploading CA Certificates 138
Uploading CA Certificates (GUI) 138
Uploading CA Certificates (CLI) 139
Generating a Certificate Signing Request 140
Generating a Certificate Signing Request using OpenSSL 140
Generating a Certificate Signing Request using Cisco Wireless Controller (GUI) 142
Downloading Third-Party Certificate 143
Downloading Third-Party Certificate (GUI) 143
Downloading Third-Party Certificate (CLI) 144

CHAPTER 11 AAA Administration 145
Setting up RADIUS for Management Users 145
Restrictions on Configuring RADIUS 147
Configuring RADIUS Authentication (GUI) 147
Configuring RADIUS Accounting Servers (GUI) 150
Configuring RADIUS (CLI) 152
RADIUS Authentication Attributes Sent by the Controller 157

Authentication Attributes Honored in Access-Accept Packets (Airespace) 159
RADIUS Accounting Attributes 167
RADIUS VSA 169
Sample RADIUS AVP List XML File 169
Downloading RADIUS AVP List (GUI) 170
Uploading RADIUS AVP List (GUI) 170
Uploading and Downloading RADIUS AVP List (CLI) 171
Custom NAS-ID for RADIUS Accounting Using Downloadable RADIUS AVP 171
Configuring Custom NAS-ID AVP XML File 173
Deleting a NAS-ID AVP (GUI) 174
Viewing Custom NAS-ID Enhancement Configuration (GUI) 174
Viewing Custom NAS-ID Enhancement (CLI) 175
Per-WLAN RADIUS Source Support 175
Prerequisites for Per-WLAN RADIUS Source Support 175
Configuring Per-WLAN RADIUS Source Support (GUI) 176
Configuring Per-WLAN RADIUS Source Support (CLI) 176
Monitoring the Status of Per-WLAN RADIUS Source Support (CLI) 177
RADIUS Realm 177
Disabling Accounting Servers per WLAN (GUI) 180
User Login Policies 181
Configuring User Login Policies (GUI) 181
Configuring User Login Policies (CLI) 181
AAA Override (Identity Networking) 182
RADIUS Attributes Used in Identity Networking 182
Configuring Network Access Identifier (CLI) 185
Setting up TACACS+ 186
TACACS+ VSA 189
Configuring TACACS+ (GUI) 189
Configuring TACACS+ (CLI) 191
Maximum Local Database Entries 193
Configuring Maximum Local Database Entries (GUI) 194
Configuring Maximum Local Database Entries (CLI) 194

CHAPTER 12 **Managing Users** 197

Administrator Usernames and Passwords 197
Restrictions on Managing User Accounts 197
Configuring Usernames and Passwords (GUI) 197
Configuring Usernames and Passwords (CLI) 198
Lobby Ambassador Account 199
Creating a Lobby Ambassador Account (GUI) 199
Creating a Lobby Ambassador Account (CLI) 200
Creating Guest User Accounts as a Lobby Ambassador (GUI) 200
Guest Accounts 201
Viewing the Guest Accounts (GUI) 201
Viewing the Guest Accounts (CLI) 202
Client Whitelisting 202
Restrictions for Client Whitelisting 202
Configuring Lobby Administrator by Global Administrator (GUI) 203
Configuring Lobby Administrator by Global Administrator (CLI) 203
Configuring Client Whitelist by Global Administrator (CLI) 204
Configuring Lobby Administrator Access on WLAN by Global Administrator (GUI) 204
Creating Client Whitelist by Lobby Administrator (GUI) 205
Deleting MAC Address from Whitelist (GUI) 206
Password Policies 207
Configuring Password Policies (GUI) 207
Configuring Password Policies (CLI) 208

CHAPTER 13 **Ports and Interfaces** 211
Ports 211
Distribution System Ports 211
Restrictions for Configuring Distribution System Ports 211
Service Port 212
Configuring Ports (GUI) 212
Configuring Ports (CLI) 214
Link Aggregation 215
Restrictions on Link Aggregation 215
Configuring Link Aggregation (GUI) 217
Configuring Link Aggregation (CLI) 217

Verifying Link Aggregation Settings (CLI) 218
Configuring Neighbor Devices to Support Link Aggregation 218
Choosing Between Link Aggregation and Multiple AP-Manager Interfaces 218
Interfaces 219
Restrictions for Configuring Interfaces 220
Dynamic AP Management 220
WLANs 220
Management Interface 222
Configuring the Management Interface (GUI) 222
Configuring the Management Interface (CLI) 223
Virtual Interface 225
Configuring Virtual Interfaces (GUI) 226
Configuring Virtual Interfaces (CLI) 226
Service-Port Interfaces 227
Configuring Service-Port Interfaces Using IPv4 (GUI) 228
Configuring Service-Port Interfaces Using IPv4 (CLI) 228
Configuring Service-Port Interface Using IPv6 (GUI) 229
Configuring Service-Port Interfaces Using IPv6 (CLI) 229
Dynamic Interface 230
Prerequisites for Configuring Dynamic Interfaces 231
Restrictions on Configuring Dynamic Interfaces 231
Configuring Dynamic Interfaces (GUI) 231
Configuring Dynamic Interfaces (CLI) 233
AP-Manager Interface 234
Restrictions for Configuring AP Manager Interface 234
Configuring the AP-Manager Interface (GUI) 235
Configuring the AP Manager Interface (CLI) 235
Interface Groups 236
Restrictions on Configuring Interface Groups 237
Creating Interface Groups (GUI) 237
Creating Interface Groups (CLI) 238
Adding Interfaces to Interface Groups (GUI) 238
Adding Interfaces to Interface Groups (CLI) 238
Viewing VLANs in Interface Groups (CLI) 239

Adding an Interface Group to a WLAN (GUI) 239
Adding an Interface Group to a WLAN (CLI) 239

CHAPTER 14 IPv6 Clients 241
IPv6 Client Mobility 241
Prerequisites for Configuring IPv6 Mobility 241
Restrictions on Configuring IPv6 Mobility 242
Global IPv6 242
Restrictions on Global IPv6 242
Configuring IPv6 Globally (GUI) 242
Configuring IPv6 Globally (CLI) 243
RA Guard 243
Configuring RA Guard (GUI) 243
Configuring RA Guard (CLI) 244
RA Throttling 244
Configuring RA Throttling (GUI) 244
Configuring the RA Throttle Policy (CLI) 245
IPv6 Neighbor Discovery 245
Configuring Neighbor Binding (GUI) 245
Configuring Neighbor Binding (CLI) 246

CHAPTER 15 Access Control Lists 247
Information about Access Control Lists 247
Guidelines and Restrictions on Access Control Lists 248
Configuring Access Control Lists (GUI) 249
Applying an Access Control List to an Interface (GUI) 251
Applying an Access Control List to the Controller CPU (GUI) 251
Applying an Access Control List to a WLAN (GUI) 252
Applying a Preauthentication Access Control List to a WLAN (GUI) 253
Configuring Access Control Lists (CLI) 253
Applying Access Control Lists (CLI) 254
Layer 2 Access Control Lists 255
Restrictions on Layer 2 Access Control Lists 256
Configuring Layer 2 Access Control Lists (CLI) 257

Configuring Layer 2 Access Control Lists (GUI) 257
Applying a Layer2 Access Control List to a WLAN (GUI) 259
Applying a Layer2 Access Control List to an AP on a WLAN (GUI) 259
DNS-based Access Control Lists 259
Guidelines and Restrictions on DNS-based Access Control Lists 260
Configuring DNS-based Access Control Lists (CLI) 260
Configuring DNS-based Access Control Lists (GUI) 262
URL Filtering 262
Restrictions for URL Filtering 263
Configuring URL Filtering (GUI) 263
Configuring URL Filtering (CLI) 267
CNAME IPv6 Filtering 269
Restrictions for CNAME IPv6 Filtering 269
Configuring CNAME URL ACL (GUI) 270
Configuring Web Authentication for CNAME IPv6 Filtering on a WLAN (GUI) 271
Configuring Web Authentication for CNAME IPv6 Filtering Using External RADIUS Server (GUI) 271
Configuring IPv6 CNAME Filtering (CLI) 271
Domain-based Filtering 272
Restrictions on Domain-based Filtering 272
Configuring Domain-based Filtering (GUI) 273
Configuring Access Control Lists (GUI) 273
Creating a URL ACL List (GUI) 273
Applying a URL Filtering Access Control List Globally (GUI) 274
Applying a URL Filtering Access Control List to an Interface (GUI) 274
Applying a URL Filtering Access Control List for a WLAN (GUI) 275
Mapping the Policy to a WLAN (GUI) 275
Mapping the Policy to an AP Group (GUI) 276
Configuring Domain Based Filtering (CLI) 277
Configuring URL Filtering (CLI) 277
Configuring Access Control List Rules (CLI) 277
Applying Local Policy (CLI) 278
Viewing URL Filtering (CLI) 278
Troubleshooting URL Filtering (CLI) 279

CHAPTER 16 **Multicast/Broadcast Setup** 281

Multicast/Broadcast Mode 281

Restrictions on Configuring Multicast Mode 283

Enabling Multicast Mode (GUI) 285

Enabling Multicast Mode (CLI) 286

Viewing Multicast Groups (GUI) 287

Viewing Multicast Groups (CLI) 287

Viewing an Access Point's Multicast Client Table (CLI) 288

Media Stream 288

Prerequisites for Media Stream 289

Restrictions for Configuring Media Stream 289

Configuring Media Stream (GUI) 289

Configuring Media Stream (CLI) 293

Configuring Media Parameters (GUI) 294

Viewing and Debugging Media Stream 295

Multicast Domain Name System 296

Restrictions for Configuring Multicast DNS 298

Configuring Multicast DNS (GUI) 299

Configuring Multicast DNS (CLI) 300

Bonjour Gateway Based on Access Policy 303

Restrictions on Bonjour Gateway Based on Access Policy 304

Configuring mDNS Service Groups (GUI) 304

Configuring mDNS Service Groups (CLI) 305

CHAPTER 17 **Controller Security** 307

FIPS, CC, and UCAPL 307

FIPS 307

FIPS Self-Tests 307

Information About CC 308

Information About UCAPL 308

Configuring FIPS (CLI) 309

Configuring CC (CLI) 309

Configuring UCAPL (CLI) 310

Preparing Controller in FIPS Mode for Management in Cisco Prime Infrastructure (CLI) 310
Cisco TrustSec 313
Guidelines and Restrictions on Cisco TrustSec 319
Configuring Cisco TrustSec 322
Configuring Cisco TrustSec on Controller (GUI) 322
Configuring Cisco TrustSec on Controller (CLI) 322
Configuring Cisco TrustSec Override for an Access Point (CLI) 322
SXP 322
Cisco TrustSec Credentials 325
Monitoring Environment Data 326
Configuring a Static Security Group Tag on a WLAN 327
Configuring Inline Tagging 328
Verifying SGACL Policy Download 329
Configuring Policy Enforcement 330
Debugging Cisco TrustSec in Controller (CLI) 331
Cisco TrustSec Commands on Lightweight APs 332
IPSec Profile 333
Configuring an IPSec Profile (GUI) 333
Configuring an IPSec Profile (CLI) 334

CHAPTER 18 **Cisco Umbrella WLAN (OpenDNS) 337**
Cisco Umbrella WLAN (OpenDNS) 337
Configuring Cisco Umbrella WLAN (GUI) 338
Configuring Cisco Umbrella WLAN (CLI) 339
Configuring Local Policies for Cisco Umbrella (GUI) 340

CHAPTER 19 **SNMP 343**
Guidelines and Limitations for SNMP 343
Configuring SNMP (CLI) 343
SNMP Community Strings 346
Changing the SNMP Community String Default Values (GUI) 346
Changing the SNMP Community String Default Values (CLI) 346
Configuring Real Time Statistics (CLI) 347
SNMP Trap Enhancements 348

Configuring SNMP Trap Receiver (GUI) 348

PART III **Mobility** 351

CHAPTER 20 **Overview** 353

Information About Mobility 353

Guidelines and Restrictions 356

CHAPTER 21 **Auto-Anchor Mobility** 359

Information about Auto-Anchor Mobility 359

Restrictions for Auto-Anchor Mobility 360

Configuring Auto-Anchor Mobility (GUI) 361

Configuring Auto-Anchor Mobility (CLI) 362

Guest Anchor Priority 364

Configuring Guest Anchor Priority (GUI) 365

Configuring Guest Anchor Priority (CLI) 365

Dynamic Anchoring for Clients with Static IP 366

How Dynamic Anchoring of Static IP Clients Works 366

Restrictions on Dynamic Anchoring for Clients With Static IP Addresses 367

Configuring Dynamic Anchoring of Static IP Clients (GUI) 367

Configuring Dynamic Anchoring of Static IP Clients (CLI) 367

CHAPTER 22 **Mobility Groups** 369

Information About Mobility Groups 369

Prerequisites for Configuring Mobility Groups 372

Configuring Mobility Groups (GUI) 373

Configuring Mobility Groups (CLI) 375

Viewing Mobility Group Statistics (GUI) 377

Viewing Mobility Group Statistics (CLI) 378

CHAPTER 23 **Encrypted Mobility Tunnel** 379

Information about Encrypted Mobility Tunnel 379

Restrictions for Encrypted Mobility Tunnel 379

Configuring Mobility Groups for Inter-Release Controller Mobility (IRCM) (GUI) 380

Configuring Mobility Groups for Inter-Release Controller Mobility (IRCM) (CLI) 381

CHAPTER 24 **Monitoring and Validating Mobility** 383

Mobility Ping Tests 383

Restrictions for Mobility Ping Tests 383

Running Mobility Ping Tests (CLI) 383

WLAN Mobility Security Values 384

PART IV **Wireless** 387

CHAPTER 25 **Country Codes** 389

Information About Configuring Country Codes 389

Restrictions for Configuring Country Codes 390

Configuring Country Codes (GUI) 390

Configuring Country Codes (CLI) 391

CHAPTER 26 **Radio Bands** 395

802.11 Bands 395

Configuring the 802.11 Bands (GUI) 395

Configuring the 802.11 Bands (CLI) 396

802.11n Parameters 399

Configuring the 802.11n Parameters (GUI) 399

Configuring the 802.11n Parameters (CLI) 401

802.11ac Parameters 403

Restrictions for 802.11ac Support 405

Configuring the 802.11ac High-Throughput Parameters (GUI) 406

Configuring the 802.11ac High-Throughput Parameters (CLI) 406

CHAPTER 27 **Radio Resource Management** 409

Information about Radio Resource Management 409

Radio Resource Monitoring 410

Benefits of RRM 410

Information About Configuring RRM 410

Configuring RRM (CLI) 411

Viewing RRM Settings (CLI) 416
RF Groups 416
Information About RF Groups 416
RF Group Leader 417
RF Group Name 420
Controllers and APs in RF Groups 420
Configuring RF Groups 420
Configuring an RF Group Name (GUI) 421
Configuring an RF Group Name (CLI) 421
Configuring the RF Group Mode (GUI) 421
Configuring the RF Group Mode (CLI) 422
Viewing RF Group Status 423
Viewing the RF Group Status (GUI) 423
Viewing the RF Group Status (CLI) 423
Rogue Access Point Detection in RF Groups 424
Enabling Rogue Access Point Detection in RF Groups (GUI) 424
Configuring Rogue Access Point Detection in RF Groups (CLI) 425
Off-Channel Scanning Deferral 426
Configuring Off-Channel Scanning Deferral for WLANs 426
Configuring Off-Channel Scanning Deferral for a WLAN (GUI) 426
Configuring Off Channel Scanning Deferral for a WLAN (CLI) 427
RRM NDP and RF Grouping 427
Configuring RRM NDP (CLI) 428
Channels 428
Dynamic Channel Assignment 428
Configuring Dynamic Channel Assignment (GUI) 430
Configuring RRM Profile Thresholds, Monitoring Channels, and Monitor Intervals (GUI) 434
Overriding RRM 436
Prerequisites for Overriding RRM 436
Statically Assigning Channel and Transmit Power Settings (GUI) 436
Statically Assigning Channel and Transmit Power Settings (CLI) 438
Disabling Dynamic Channel and Power Assignment (CLI) 441
802.11h Parameters 442
Configuring the 802.11h Parameters (GUI) 442

Configuring the 802.11h Parameters (CLI) 442
Transmit Power Control 443
Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings 444
Configuring Transmit Power Control (GUI) 444
Coverage hole detection and correction 446
Configuring Coverage Hole Detection (GUI) 446
RF Profiles 447
Prerequisites for Configuring RF Profiles 450
Restrictions on Configuring RF Profiles 450
Configuring an RF Profile (GUI) 451
Configuring an RF Profile (CLI) 452
Applying an RF Profile to AP Groups (GUI) 454
Applying RF Profiles to AP Groups (CLI) 455
XOR Radios and Flexible Radio Assignment 455
Advantages of Flexible Radio Assignment 456
Additional References 456
Configuring Flexible Radio Assignment-Global (GUI) 457
Configuring Flexible Radio Assignment (CLI) 457
Configuring Flexible Radio Assignment for AP (GUI) 458
Configuring Auto Radio Role of the XOR Radio (CLI) 459
Configuring Manual Radio Role for the AP (CLI) 459
Configuring Radio Band for Client-Serving Radio (CLI) 460
Debug RRM Issues (CLI) 460
CleanAir 461
Role of the Cisco Wireless LAN Controller in a Cisco CleanAir System 461
Interference Types that Cisco CleanAir Can Detect 462
Persistent Devices 463
Persistent Device Detection 463
Persistent Device Propagation 463
Detecting Interferers by an Access Point 463
Detecting Persistent Sources of Interference 464
Prerequisites for CleanAir 464
Restrictions for CleanAir 464
Configuring Cisco CleanAir on the Controller 465

Configuring Cisco CleanAir on Controller (GUI) 465
Configuring Cisco CleanAir on Controller (CLI) 467
Configuring Cisco CleanAir on an Access Point 471
Configuring Cisco CleanAir on an Access Point (GUI) 471
Configuring Cisco CleanAir on an Access Point (CLI) 472
Configuring Spectrum Intelligence 473
Information About Spectrum Intelligence 473
Configuring Spectrum Intelligence – Global (GUI) 474
Configuring Spectrum Intelligence per AP (GUI) 474
Configuring Spectrum Intelligence (CLI) 474
Monitoring Interference Devices 475
Prerequisites for Monitoring the Interference Devices 475
Monitoring the Interference Device (GUI) 475
Monitoring the Interference Device (CLI) 477
Monitoring Persistent Devices (GUI) 478
Monitoring Persistent Devices (CLI) 479
Monitoring the Air Quality of Radio Bands 480

CHAPTER 28 **Wireless Quality of Service** 485
Call Admission Control 485
Voice and Video Parameters 485
Configuring Voice Parameters 485
Configuring Voice Parameters (GUI) 485
Configuring Voice Parameters (CLI) 487
Configuring Video Parameters 488
Configuring Video Parameters (GUI) 488
Configuring Video Parameters (CLI) 489
Viewing Voice and Video Settings 490
Viewing Voice and Video Settings (GUI) 490
Viewing Voice and Video Settings (CLI) 491
Configuring SIP-Based CAC 495
Restrictions for SIP-Based CAC 495
Configuring SIP-Based CAC (GUI) 495
Configuring SIP-Based CAC (CLI) 495

Voice Prioritization Using Preferred Call Numbers 496
Prerequisites for Configuring Voice Prioritization Using Preferred Call Numbers 496
Configuring a Preferred Call Number (GUI) 496
Configuring a Preferred Call Number (CLI) 497
Enhanced Distributed Channel Access Parameters 497
Configuring EDCA Parameters (GUI) 497
Configuring EDCA Parameters (CLI) 498
Key Telephone System-Based CAC 499
Restrictions for Key Telephone System-Based CAC 500
Configuring KTS-based CAC (GUI) 500
Configuring KTS-based CAC (CLI) 501
Application Visibility and Control 502
Restrictions for Application Visibility and Control 504
Configuring Application Visibility and Control (GUI) 505
Configuring Application Visibility and Control (CLI) 506
AVC-based Reanchoring 507
Configuring AVC-based Selective Reanchoring (GUI) 507
Configuring AVC-based Selective Reanchoring (CLI) 508
Application Visibility Control for FlexConnect 509
Configuring Application Visibility and Control for FlexConnect (GUI) 510
Configuring Application Visibility and Control for FlexConnect (CLI) 512
NetFlow 514
Restrictions for Using Netflow 516
Configuring NetFlow (GUI) 516
Configuring NetFlow (CLI) 517
QoS Profiles 517
Configuring QoS Profiles (GUI) 518
Configuring QoS Profiles (CLI) 520
Assigning a QoS Profile to a WLAN (GUI) 522
Assigning a QoS Profile to a WLAN (CLI) 523
Cisco Air Time Fairness 524
Configuring Cisco Air Time Fairness (GUI) 527
Configuring Cisco Air Tme Fairness (CLI) 529

CHAPTER 29 **Location Services** 531

Cisco Hyperlocation 531

Cisco Hyperlocation in a High Availability Environment 532

Cisco Hyperlocation Client Debug Tracing 532

Configuring Cisco Hyperlocation 533

FastLocate for Cisco Wave 2 Access Points 535

Configuring FastLocate on Cisco Wave 2 APs (GUI) 536

Optimizing RFID Tracking on Access Points 536

Optimizing RFID Tracking on Access Points (GUI) 537

Optimizing RFID Tracking on Access Points (CLI) 537

Location Settings 538

Configuring Location Settings (CLI) 538

Viewing Location Settings (CLI) 541

Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues (CLI) 541

Viewing NMSP Settings (CLI) 542

Debugging NMSP Issues 543

Probe Request Forwarding 543

Configuring Probe Request Forwarding (CLI) 544

CCX Radio Management 544

Radio Measurement Requests 545

Location Calibration 545

Configuring CCX Radio Management 546

Configuring CCX Radio Management (GUI) 546

Configuring CCX Radio Management (CLI) 546

Viewing CCX Radio Management Information (CLI) 547

Debugging CCX Radio Management Issues (CLI) 548

Mobile Concierge 548

Configuring Mobile Concierge (802.11u) (GUI) 549

Configuring Mobile Concierge (802.11u) (CLI) 550

Online Sign Up 551

802.11u MSAP 553

Configuring 802.11u MSAP (GUI) 553

Configuring MSAP (CLI) 554

Configuring 802.11u HotSpot 554
Information About 802.11u HotSpot 554
Configuring 802.11u HotSpot (GUI) 554
Configuring HotSpot 2.0 (CLI) 555
Configuring Access Points for HotSpot2 (GUI) 556
Configuring Access Points for HotSpot2 (CLI) 557
Downloading the Icon File (CLI) 560
Configuring ICONs 561
Configuring OSEN Support (CLI) 562
Configuring OSU (CLI) 563
Configuring WAN Metrics 565
CMX Cloud Connector 565
Prerequisites for CMX Cloud Connector 566
Restrictions for CMX Cloud Connector 567
Configuring CMX Cloud Connector (GUI) 567
Configuring CMX Cloud Connector (CLI) 567
Installing CMX-Serv CA Certificate on a Controller (CLI) 568
NMSP by AP Groups with Subscription List from CMX 569
Guidelines and Restrictions for NMSP by AP Groups with Subscription List from CMX 569
Monitoring NMSP by AP Groups with Subscription List from CMX (GUI) 570
Monitoring NMSP by AP Groups with Subscription List from CMX (CLI) 570

CHAPTER 30 **Wireless Intrusion Detection System** 573
Protected Management Frames (Management Frame Protection) 573
Configuring Infrastructure MFP (GUI) 574
Viewing the Management Frame Protection Settings (GUI) 575
Configuring Infrastructure MFP (CLI) 575
Viewing the Management Frame Protection Settings (CLI) 576
Debugging Management Frame Protection Issues (CLI) 576
Rogue Management 576
Configuring Rogue Detection (GUI) 577
Configuring Rogue Detection (CLI) 579
Rogue Access Point Classification 582
Guidelines and Restrictions for Classifying Rogue Access Points 585

Configuring Rogue Classification Rules (GUI) 586
Viewing and Classifying Rogue Devices (GUI) 589
Configuring Rogue Classification Rules (CLI) 592
Viewing and Classifying Rogue Devices (CLI) 595
Intrusion Detection System Signatures 597
Uploading or Downloading IDS Signatures 599
Configuring IDS Signatures (GUI) 601
Viewing IDS Signature Events (GUI) 602
Configuring IDS Signatures (CLI) 603
Viewing IDS Signature Events (CLI) 605
Cisco Intrusion Detection System 605
Shunned Clients 606
Configuring IDS Sensors (GUI) 606
Viewing Shunned Clients (GUI) 607
Configuring IDS Sensors (CLI) 607
Viewing Shunned Clients (CLI) 609
Wireless Intrusion Prevention System 609
Restrictions for wIPS 615
Configuring wIPS on an Access Point (GUI) 615
Configuring wIPS on an Access Point (CLI) 615
Viewing wIPS Information (CLI) 616
Cisco Adaptive wIPS Alarms 617

CHAPTER 31 **Advanced Wireless Tuning** 619
Aggressive Load Balancing 619
Configuring Aggressive Load Balancing (GUI) 620
Configuring Aggressive Load Balancing (CLI) 621
Reanchoring of Roaming Voice Clients 621
Restrictions for Configuring Reanchoring of Roaming Voice Clients 622
Configuring Reanchoring of Roaming Voice Clients (GUI) 622
Configuring Reanchoring of Roaming Voice Clients (CLI) 622
SpectraLink NetLink Telephones 623
Enabling Long Preambles (GUI) 623
Enabling Long Preambles (CLI) 624

Receiver Start of Packet Detection Threshold 624
Guidelines and Restrictions for RxSOP 625
Configuring Rx SOP (GUI) 625
Configuring RxSOP (CLI) 626

CHAPTER 32 **Timers** 627
Information about Wireless Timers 627
Restrictions for Wireless Timers 627
Configuring Wireless Timers (GUI) 627
Configuring Wireless Timers (CLI) 628

PART V **Access Points** 629

CHAPTER 33 **AP Power and Uplink LAN Connections** 631
Power over Ethernet 631
Configuring Power over Ethernet (GUI) 631
Configuring Power over Ethernet (CLI) 632
Cisco Discovery Protocol 634
Restrictions for Cisco Discovery Protocol 634
Configuring the Cisco Discovery Protocol 635
Configuring the Cisco Discovery Protocol (GUI) 635
Configuring the Cisco Discovery Protocol (CLI) 637
Viewing Cisco Discovery Protocol Information 638
Viewing Cisco Discovery Protocol Information (GUI) 638
Viewing Cisco Discovery Protocol Information (CLI) 640
Getting CDP Debug Information 641
Cisco Wave 2 AP's USB Port as Power Source 641
Configuring Cisco Aironet AP's USB Port as Power Source (GUI) 642
Configuring a Cisco AP Group to Use the Cisco AP's USB Port as Power Source (GUI) 642
Configuring Cisco Aironet APs USB Port as Power Source (Controller CLI) 643
Viewing Cisco Aironet APs USB Port as Power Source (AP-CLI) 643
Viewing AP Serviceability (AP CLI) 643
Cisco 700 Series Access Points 644
Configuring Cisco 700 Series Access Points 644

Enabling the LAN Ports (CLI) 644
Remote LAN Support for Wired Ports on Cisco Aironet 702W APs 645
IEEE 802.1X Authentication Modes 645
Configuring Preauthentication Open (CLI) 646
Configuring IEEE 802.1X Authentication Modes (CLI) 646
Enabling IEEE 802.1X Authentication in Controller (GUI) 647
Enabling IEEE 802.1X Authentication (CLI) 648
Mapping an RLAN to an AP Port in Controller (GUI) 648
Mapping an RLAN to an AP Port in Controller (CLI) 649
Mapping an RLAN to an AP Port in Controller per AP (GUI) 649
Mapping a RLAN to an AP External Port in Controller (GUI) 650
Mapping a RLAN to an AP External Port in Controller (CLI) 650
MAB Authentication Support for AP Port LAN Client in Cisco Aironet 702w Access Points 651
Converting Cisco Wave 2 AP AUX Port to Downlink LAN (RLAN) Port (CLI) 651
Re-enabling LAG Mode on Cisco Wave 2 APs (CLI) 653

CHAPTER 34 **AP Connectivity to Controller** 655
CAPWAP 655
Restrictions for Access Point Communication Protocols 656
Viewing CAPWAP Maximum Transmission Unit Information 656
Debugging CAPWAP 657
Link Latency 657
Restrictions for Link Latency 658
Configuring Link Latency (GUI) 658
Configuring Link Latency (CLI) 659
Preferred Mode 660
Guidelines for Configuring Preferred Mode 660
Configuring CAPWAP Preferred Mode (GUI) 660
Configuring CAPWAP Preferred Mode (CLI) 661
IPv6 CAPWAP UDP Lite 662
Configuring UDP Lite Globally (GUI) 663
Configuring UDP Lite on AP (GUI) 663
Configuring the UDP Lite (CLI) 663
Data Encryption 664

Restrictions on Data Encryption 666
Configuring Data Encryption (GUI) 666
Configuring Data Encryption (CLI) 667
VLAN Tagging for CAPWAP Frames from Access Points 668
Configuring VLAN Tagging for CAPWAP Frames from Access Points (GUI) 668
Configuring VLAN Tagging for CAPWAP Frames from Access Points (CLI) 669
Discovering and Joining Controllers 669
Controller Discovery Process 669
Guidelines and Restrictions on Controller Discovery Process 670
Using DHCP Option 43 and DHCP Option 60 671
Backup Controllers 671
Restrictions for Configuring Backup Controllers 672
Configuring Backup Controllers (GUI) 672
Configuring Backup Controllers (CLI) 673
Failover Priority for Access Points 676
Configuring Failover Priority for Access Points (GUI) 677
Configuring Failover Priority for Access Points (CLI) 677
Viewing Failover Priority Settings (CLI) 678
AP Retransmission Interval and Retry Count 678
Restrictions for Access Point Retransmission Interval and Retry Count 678
Configuring the AP Retransmission Interval and Retry Count (GUI) 679
Configuring the Access Point Retransmission Interval and Retry Count (CLI) 679
Authorizing Access Points 680
Authorizing Access Points Using SSCs 681
Authorizing Access Points for Virtual Controllers Using SSC 681
Authorizing Access Points Using MICs 682
Authorizing Access Points Using LSCs 682
Configuring Locally Significant Certificates (GUI) 683
Configuring Locally Significant Certificates (CLI) 684
Authorizing Access Points (GUI) 686
Authorizing Access Points (CLI) 687
Plug and Play (PnP) 687
AP Wired 802.1X Supplicant 688
Prerequisites for Configuring Wired 802.1X Authentication for Access Points 690

Restrictions for Authenticating Access Points 690
Configuring 802.1X Authentication Protocols for All Access Points (GUI) 691
Configuring 802.1X Authentication Protocols for All Access Points (CLI) 692
Configuring 802.1X Authentication Protocols for An Access Point (GUI) 693
Configuring 802.1X Authentication Protocols for An Access Point (CLI) 693
Configuring LSC Authentication State (GUI) 695
Configuring LSC Authentication State (CLI) 695
Adding AP to an LSC Provisioned Network 695
Configuring the Switch for Authentication 696
Configuring a Static IP Address on a Lightweight Access Point 696
Configuring a Static IP Address (GUI) 697
Configuring a Static IP Address (CLI) 697
Troubleshooting the Access Point Join Process 699
Configuring the Syslog Server for Access Points (CLI) 701
Viewing Access Point Join Information 701
Viewing Access Point Join Information (GUI) 702
Viewing Access Point Join Information (CLI) 703

CHAPTER 35 **Managing APs** 705
Access Point Modes 705
Global Credentials for Access Points 706
Restrictions for Global Credentials for Access Points 707
Configuring Global Credentials for Access Points 707
Configuring Global Credentials for Access Points (GUI) 707
Configuring Global Credentials for Access Points (CLI) 708
Configuring Telnet and SSH for Access Points 709
Configuring Telnet and SSH for APs (GUI) 709
Configuring Telnet and SSH for APs (CLI) 710
Spectrum Expert Connection 710
Guidelines and Limitations for Spectrum Expert Connection 710
Configuring Spectrum Expert (GUI) 710
Cisco Universal Small Cell 8x18 Dual-Mode Module 713
Configuring Cisco Universal Small Cell 8x18 Dual-Mode Module 714
Configuring USC8x18 Dual-Mode Module in Different Scenarios 715

LED States for Access Points 717
Configuring the LED State for Access Points in a Network Globally (GUI) 717
Configuring the LED State for Access Point in a Network Globally (CLI) 717
Configuring LED State on a Specific Access Point (GUI) 718
Configuring LED State on a Specific Access Point (CLI) 718
Configuring Flashing LEDs 718
Information About Configuring Flashing LEDs 718
Configuring Flashing LEDs (CLI) 718
Configuring LED Flash State on a Specific Access Point (GUI) 719
Access Points with Dual-Band Radios 719
Configuring Access Points with Dual-Band Radios (GUI) 720
Configuring Access Points with Dual-Band Radios (CLI) 720

PART VI **Mesh Access Points** 721

CHAPTER 36 **Connecting Mesh Access Points to the Network** 723
Overview 723
Adding Mesh Access Points to the Mesh Network 724
Adding MAC Addresses of Mesh Access Points to MAC Filter 725
Adding the MAC Address of the Mesh Access Point to the Controller Filter List (CLI) 726
Defining Mesh Access Point Role 726
Configuring the AP Role (CLI) 726
Configuring Multiple Controllers Using DHCP 43 and DHCP 60 726
Configuring External Authentication and Authorization Using a RADIUS Server 727
Configuring RADIUS Servers 728
Enable External Authentication of Mesh Access Points (CLI) 729
View Security Statistics (CLI) 729
Mesh PSK Key Provisioning 729
CLI Commands for PSK Provisioning 730
Configuring Global Mesh Parameters 731
Configuring Global Mesh Parameters (CLI) 731
Viewing Global Mesh Parameter Settings (CLI) 732
Backhaul Client Access 733
Configuring Backhaul Client Access (GUI) 734

Configuring Backhaul Client Access (CLI) 734
Configuring Local Mesh Parameters 735
Configuring Wireless Backhaul Data Rate 735
Configuring Ethernet Bridging 737
Configuring Native VLAN (CLI) 738
Configuring Bridge Group Names 739
Configuring Bridge Group Names (CLI) 739
Configuring Antenna Gain 739
Configuring Antenna Gain (CLI) 740
Configuring Mesh Leaf Node 740
Configuring Advanced Features 741
Configuring Ethernet VLAN Tagging 741
Ethernet Port Notes 742
VLAN Registration 743
Configuring Ethernet VLAN Tagging (CLI) 745
Viewing Ethernet VLAN Tagging Configuration Details (CLI) 746
Workgroup Bridge Interoperability with Mesh Infrastructure 746
Configuring Workgroup Bridges 748
Guidelines for Configuration 751
Configuration Example 752
WGB Association Check 753
Link Test Result 755
WGB Wired/Wireless Client 756
Client Roaming 757
WGB Roaming Guidelines 757
Configuration Example 758
Troubleshooting Tips 758
Configuring Voice Parameters in Indoor Mesh Networks 758
Call Admission Control 759
Quality of Service and Differentiated Services Code Point Marking 759
Guidelines For Using Voice on the Mesh Network 764
Voice Call Support in a Mesh Network 765
Enabling Mesh Multicast Containment for Video 766
Viewing the Voice Details for Mesh Networks (CLI) 767

Enabling Multicast on the Mesh Network (CLI) 771
IGMP Snooping 771
Locally Significant Certificates for Mesh APs 772
Guidelines for Configuration 773
Differences Between LSCs for Mesh APs and Normal APs 773
Certificate Verification Process in LSC AP 773
Getting Certificates for LSC Feature 774
Configuring a Locally Significant Certificate (CLI) 775
LSC only MAP Authentication using wild card MAC 776
LSC-Related Commands 777
Controller GUI Security Settings 779
Deployment Guidelines 780
Configuring Antenna Band Mode 780
Information About Configuring Antenna Band Modes 780
Configuring Antenna Band Mode (CLI) 781
Configuring Daisy Chaining on Cisco Aironet 1530 Series Access Points 781
Information About Daisy Chaining the Cisco Aironet 1530 Series Access Points 781
Configuring Daisy Chaining (CLI) 785
Configuring a Daisy-Chain 786
Configuring Mesh Convergence 788
Information About Mesh Convergence 788
Restrictions on Mesh Convergence 788
Configuring Mesh Convergence (CLI) 789
Switching Between LWAPP and Autonomous Images (AP CLI) 789
Information About DHCP on RAP 789
Restrictions on DHCP on RAP 790
Configuring DHCP on RAP on a Controller (CLI) 790
Configuring DHCP on RAP on a Mesh AP (CLI) 790
Information About NAT-PAT on RAP 791
Restrictions on NAT-PAT on RAP 791
Viewing NAT-PAT on RAP on a Mesh AP (CLI) 791
Configuring Mesh Leaf Node 792

CHAPTER 37 **Checking the Health of the Network** 795

Show Mesh Commands 795
Viewing General Mesh Network Details 795
Viewing Mesh Access Point Details 797
Viewing Global Mesh Parameter Settings 798
Viewing Bridge Group Settings 799
Viewing VLAN Tagging Settings 799
Viewing DFS Details 799
Viewing Security Settings and Statistics 800
Viewing GPS Status 800
Viewing Mesh Statistics for a Mesh Access Point 801
Viewing Mesh Statistics for a Mesh Access Point (GUI) 801
Viewing Mesh Statistics for a Mesh Access Point (CLI) 804
Viewing Neighbor Statistics for a Mesh Access Point 805
Viewing Neighbor Statistics for a Mesh Access Point (GUI) 805
Viewing the Neighbor Statistics for a Mesh Access Point (CLI) 806

CHAPTER 38 **Troubleshooting Mesh Access Points** 809
Installation and Connections 809
Debug Commands 810
Remote Debug Commands 810
AP Console Access 811
Cable Modem Serial Port Access from an AP 811
Configuration 812
Mesh Access Point CLI Commands 814
Mesh Access Point Debug Commands 817
Defining Mesh Access Point Roles 817
Backhaul Algorithm 817
Passive Beaconing (Anti-Stranding) 818
Dynamic Frequency Selection 819
DFS in RAP 820
DFS in MAP 820
Preparation in a DFS Environment 821
Monitoring DFS 823
Frequency Planning 823

Good Signal-to-Noise Ratios 824
Access Point Placement 824
Bridge Group Name Misconfiguration 824
Misconfiguration of the Mesh Access Point IP Address 825
Misconfiguration of DHCP 826
Identifying the Node Exclusion Algorithm 826
Throughput Analysis 828

PART VII **Client Network** 831

CHAPTER 39 **Client Traffic Forwarding Configurations** 833
802.3 Bridging 833
Restrictions on 802.3 Bridging 833
Configuring 802.3 Bridging (GUI) 833
Configuring 802.3 Bridging (CLI) 834
Enabling 802.3X Flow Control 834
Bridging Link Local Traffic 834
Configuring Bridging of Link Local Traffic (GUI) 834
Configuring Bridging of Link Local Traffic (CLI) 835
IP-MAC Address Binding 835
Configuring IP-MAC Address Binding (CLI) 835
TCP Adjust MSS 836
Configuring TCP Adjust MSS (GUI) 836
Configuring TCP Adjust MSS (CLI) 837
Passive Clients 837
Restrictions for Passive Clients 838
Configuring Passive Clients (GUI) 838
Configuring Passive Clients (CLI) 839
Enabling the Multicast-Multicast Mode (GUI) 840
Enabling the Global Multicast Mode on Controllers (GUI) 841
Enabling the Passive Client Feature on the Controller (GUI) 841
Multicast-to-Unicast Support for Passive Client ARPs 841
Configuring Unicast Mode (GUI) 842
Configuring Unicast mode on Controller (CLI) 842

CHAPTER 40

Quality of Service 843

Quality of Service 843

QoS Profiles 844

Configuring QoS Profiles (GUI) 845

Configuring QoS Profiles (CLI) 847

Assigning a QoS Profile to a WLAN (GUI) 848

Assigning a QoS Profile to a WLAN (CLI) 850

Quality of Service Roles 850

Configuring QoS Roles (GUI) 851

Configuring QoS Roles (CLI) 852

QoS Map 853

Guidelines and Restrictions for QoS Map 854

Configuring QoS Map (GUI) 854

Configuring QoS Map (CLI) 855

FastLane QoS 856

Configuring Fastlane QoS (CLI) 856

Configuring Fastlane QoS (GUI) 864

Disabling Fastlane QoS Globally (GUI) 864

SIP (Media Session) Snooping, CAC, and Reporting 865

Restrictions for SIP (Media Session) Snooping, CAC, and Reporting 865

Configuring Media Session Snooping (GUI) 865

Configuring Media Session Snooping (CLI) 866

Voice and Video Parameters 869

Call Admission Control 869

Static CAC 870

Load-Based CAC 870

Expedited Bandwidth Requests 870

U-APSD 871

Traffic Stream Metrics 872

Configuring Voice Parameters 872

Configuring Voice Parameters (GUI) 872

Configuring Voice Parameters (CLI) 874

Configuring Video Parameters 875

Configuring Video Parameters (GUI) 875
Configuring Video Parameters (CLI) 876
Viewing Voice and Video Settings 877
Viewing Voice and Video Settings (GUI) 877
Viewing Voice and Video Settings (CLI) 878
SIP-based CAC 881
Restrictions for SIP-Based CAC 882
Configuring SIP-Based CAC (GUI) 882
Configuring SIP-Based CAC (CLI) 882
Enhanced Distributed Channel Access Parameters 883
Configuring EDCA Parameters (GUI) 883
Configuring EDCA Parameters (CLI) 884

CHAPTER 41 WLANs 887
Information About WLANs 887
Prerequisites for WLANs 887
Restrictions for WLANs 888
Creating and Removing WLANs (GUI) 888
Enabling and Disabling WLANs (GUI) 890
Editing WLAN SSID or Profile Name for WLANs (GUI) 890
Creating and Deleting WLANs (CLI) 890
Enabling and Disabling WLANs (CLI) 891
Editing WLAN SSID or Profile Name for WLANs (CLI) 892
Viewing WLANs (CLI) 892
Searching WLANs (GUI) 892
Assigning WLANs to Interfaces 893

CHAPTER 42 Per-WLAN Wireless Settings 895
DTIM Period 895
Configuring the DTIM Period (GUI) 896
Configuring the DTIM Period (CLI) 896
Cisco Client Extensions 897
Prerequisites for Configuring Cisco Client Extensions 897
Configuring CCX Aironet IEs (GUI) 897

Viewing a Client's CCX Version (GUI) 897
Configuring CCX Aironet IEs (CLI) 898
Viewing a Client's CCX Version (CLI) 898
Client Profiling 898
Prerequisites for Configuring Client Profiling 899
Restrictions for Configuring Client Profiling 900
Configuring Client Profiling (GUI) 900
Configuring Client Profiling (CLI) 901
Configuring Custom HTTP Port for Profiling (GUI) 901
Configuring Custom HTTP Port for Profiling (CLI) 902
Client Count per WLAN 902
Restrictions for Setting Client Count for WLANs 902
Configuring the Client Count per WLAN (GUI) 903
Configuring the Maximum Number of Clients per WLAN (CLI) 903
Configuring the Maximum Number of Clients for each AP Radio per WLAN (GUI) 903
Configuring the Maximum Number of Clients for each AP Radio per WLAN (CLI) 904
Limit Clients per WLAN per AP Radio 904
Limit Clients per WLAN per AP Radio (GUI) 904
Limit Clients per WLAN per AP Radio (CLI) 905
Disabling Coverage Hole Detection per WLAN 905
Disabling Coverage Hole Detection on a WLAN (GUI) 906
Disabling Coverage Hole Detection on a WLAN (CLI) 906

CHAPTER 43 **WLAN Interfaces** 907
Multicast VLAN 907
Configuring a Multicast VLAN (GUI) 908
Configuring a Multicast VLAN (CLI) 908

CHAPTER 44 **WLAN Timeouts** 909
Client Exclusion Timeout 909
Configuring Client Exclusion Timeout (CLI) 909
Session Timeouts 909
Configuring a Session Timeout (GUI) 910
Configuring a Session Timeout (CLI) 910

User Idle Timeout 911
Configuring User Idle Timeout (GUI) 911
Configuring User Idle Timeout (CLI) 911
User Idle Timeout per WLAN 912
Configuring Per-WLAN User Idle Timeout (GUI) 912
Configuring Per-WLAN User Idle Timeout (CLI) 912
Address Resolution Protocol Timeout 913
Configuring ARP Timeout (GUI) 913
Configuring ARP Timeout (CLI) 913

CHAPTER 45 WLAN Security 915
Layer 2 Security 915
Prerequisites for Layer 2 Security 915
MAC Filtering of WLANs 916
Restrictions for MAC Filtering 916
Enabling MAC Filtering 916
Local MAC Filters 917
Prerequisites for Configuring Local MAC Filters 917
Configuring Local MAC Filters (CLI) 917
Protected Management Frames (802.11w) 918
Restrictions for Protected Management Frames (802.11w) 918
Configuring Protected Management Frames (802.11w) (GUI) 919
Configuring Protected Management Frames (802.11w) 802.11w (CLI) 919
Fast Secure Roaming 920
802.11r Fast Transition 920
802.11i Sticky Key Caching 926
Cisco Centralized Key Management (CCKM) 927
Wi-Fi Protected Areas (WPA) 928
WPA1 and WPA2 928
Wireless Encryption Protocol (WEP) 932
WLAN for Static WEP 932
Configuring Dynamic WEP (CLI) 932
MAC Authentication Failover to 802.1X Authentication 933
Identity PSK 934

Prerequisites for Identity PSK 934
Configuring Identity PSK (GUI) 934
Configuring Identity PSK (CLI) 935
Layer 3 Security 935
Information About Web Authentication 936
Prerequisites for Configuring Web Authentication on a WLAN 936
Restrictions for Configuring Web Authentication on a WLAN 937
Default Web Authentication Login Page 937
Using a Customized Web Authentication Login Page from an External Web Server 941
Downloading a Customized Web Authentication Login Page 945
Assigning Login, Login Failure, and Logout Pages per WLAN 948
Captive Network Assistant Bypass 951
Configuring Captive Bypassing (CLI) 951
Configuring Captive Network Assistant Bypass per WLAN (GUI) 952
Configuring Captive Network Assistant Bypass per WLAN (CLI) 952
Fallback Policy with MAC Filtering and Web Authentication 952
Configuring a Fallback Policy with MAC Filtering and Web Authentication (GUI) 953
Configuring a Fallback Policy with MAC Filtering and Web Authentication (CLI) 953
Central Web Authentication 954
Authentication of Sleeping Clients 955
Restrictions for Authenticating Sleeping Clients 956
Configuring Authentication for Sleeping Clients (GUI) 957
Configuring Authentication for Sleeping Clients (CLI) 957
Authenticating Sleeping Clients on L2+L3 Enabled WLANs 957
Configuring Sleeping Client Authentication on L2+L3 Enabled WLANs (GUI) 958
Configuring Sleeping Client Authentication on L2+L3 Enabled WLANs (CLI) 958
Web Redirect with 802.1X Authentication 958
Conditional Web Redirect 958
Splash Page Web Redirect 959
Configuring the RADIUS Server (GUI) 959
Configuring Web Redirect 960
Web Authentication Proxy 961
Configuring Web Authentication Proxy (GUI) 963
Configuring Web Authentication Proxy (CLI) 963

Supporting IPv6 Client Guest Access 964
EAP and AAA Servers 964
802.1X and Extensible Authentication Protocol 964
LDAP 966
Configuring LDAP (GUI) 966
Configuring LDAP (CLI) 968
Local EAP 971
Restrictions for Local EAP 971
Configuring Local EAP (GUI) 971
Configuring Local EAP (CLI) 975
Local Network Users on Controller 981
Uploading PACs for EAP-FAST 983
Uploading PACs (GUI) 983
Uploading PACs (CLI) 984
Advanced WLAN Security 985
AAA Override 985
Restrictions for AAA Override 985
Updating the RADIUS Server Dictionary File for Proper QoS Values 986
Configuring AAA Override (GUI) 987
Configuring AAA Override (CLI) 988
ISE NAC Support 988
Device Registration 988
Central Web Authentication 988
Local Web Authentication 989
Guidelines and Restrictions on ISE NAC Support 990
Configuring ISE NAC Support (GUI) 991
Configuring ISE NAC Support (CLI) 992
Enabling ISE NAC on a WPA/WPA2-PSK WLAN 992
Client Exclusion Policies 994
Configuring Client Exclusion Policies (GUI) 994
Configuring Client Exclusion Policies (CLI) 995
Configuring Client Exclusion Policies for a WLAN (GUI) 996
Configuring Client Exclusion Policies for a WLAN (CLI) 997
Wi-Fi Direct Client Policy 997

Restrictions for the Wi-Fi Direct Client Policy 997
Configuring the Wi-Fi Direct Client Policy (GUI) 998
Configuring the Wi-Fi Direct Client Policy (CLI) 998
Monitoring and Troubleshooting the Wi-Fi Direct Client Policy (CLI) 999
Peer-to-Peer Blocking 999
Restrictions on Peer-to-Peer Blocking 999
Configuring Peer-to-Peer Blocking (GUI) 1000
Configuring Peer-to-Peer Blocking (CLI) 1000
Peer-to-Peer Blocking Using IPSK Tags 1001
Local Policies 1002
Guidelines and Restrictions for Local Policy Classification 1003
Local Policy—Best Practices 1004
Configuring Local Policies (GUI) 1005
Configuring Local Policies (CLI) 1006
Updating Organizationally Unique Identifier List 1008
Updating Device Profile List 1009
Wired Guest Access 1010
Prerequisites for Configuring Wired Guest Access 1010
Restrictions for Configuring Wired Guest Access 1011
Configuring Wired Guest Access (GUI) 1011
Configuring Wired Guest Access (CLI) 1013

CHAPTER 46 **Client Roaming** 1017
Fast SSID Changing 1017
Configuring Fast SSID Changing (GUI) 1017
Configuring Fast SSID Changing (CLI) 1018
802.11k Neighbor List and Assisted Roaming 1018
Restrictions for Assisted Roaming 1019
Configuring Assisted Roaming (GUI) 1019
Configuring Assisted Roaming (CLI) 1019
802.11v 1020
Prerequisites for Configuring 802.11v 1022
Configuring 802.11v Network Assisted Power Savings (CLI) 1022
Monitoring 802.11v Network Assisted Power Savings (CLI) 1022

Configuration Examples for 802.11v Network Assisted Power Savings 1023
Enabling 802.11v BSS Transition Management 1023
Optimized Roaming 1024
Restrictions for Optimized Roaming 1024
Configuring Optimized Roaming (GUI) 1024
Configuring Optimized Roaming (CLI) 1025
Band Select 1026
Band Select Algorithm 1026
Restrictions for Band Selection 1027
Configuring Band Selection (GUI) 1028
Configuring Band Selection (CLI) 1028

CHAPTER 47 DHCP 1031
Information About Dynamic Host Configuration Protocol 1031
Internal DHCP Servers 1031
External DHCP Servers 1032
DHCP Assignments 1032
DHCP Proxy Mode versus DHCP Bridging Mode 1033
DHCP Proxy Mode 1033
Restrictions on Using DHCP Proxy 1034
Configuring DHCP Proxy (GUI) 1034
Configuring DHCP Proxy (CLI) 1035
Configuring a DHCP Timeout (GUI) 1036
Configuring a DHCP Timeout (CLI) 1037
DHCP Option 82 1037
Restrictions on DHCP Option 82 1037
Configuring DHCP Option 82 (GUI) 1038
Configuring DHCP Option 82 (CLI) 1038
Configuring DHCP Option 82 Insertion in Bridge Mode (CLI) 1039
DHCP Option 82 Link Select and VPN Select Suboptions 1039
DHCP Link Select 1040
DHCP VPN Select 1040
Mobility Considerations 1040
Prerequisites for DHCP Option 82 Link Select and VPN Select 1041

Configuring DHCP Option 82 Link Select and VPN Select (GUI) 1041
Configuring DHCP Option 82 Link Select and VPN Select (CLI) 1042
Internal DHCP Server 1043
Restrictions for Configuring Internal DHCP Server 1043
Configuring DHCP Scopes (GUI) 1044
Configuring DHCP Scopes (CLI) 1045
Configuring DHCP Per WLAN (GUI) 1046
Configuring DHCP Per WLAN (CLI) 1047
Debugging DHCP (CLI) 1048

CHAPTER 48 **Client Data Tunneling** 1051
Ethernet over GRE Tunnels 1051
Restrictions for EoGRE Tunneling 1055
Configuring EoGRE on the Controller (GUI) 1056
Configuring EoGRE on the Controller (CLI) 1058
Configuring EoGRE for FlexConnect APs (GUI) 1060
Configuring EoGRE for FlexConnect APs (CLI) 1060
One-to-One Mapping of WLAN with EoGRE VLAN (GUI) 1061
One-to-One Mapping of WLAN with EoGRE VLAN (CLI) 1061
Proxy Mobile IPv6 1062
Restrictions on Proxy Mobile IPv6 1064
Configuring Proxy Mobile IPv6 (GUI) 1065
Configuring Proxy Mobile IPv6 (CLI) 1067

CHAPTER 49 **AP Groups** 1071
Access Point Groups 1071
Restrictions for Configuring Access Point Groups 1072
Configuring Access Point Groups 1072
Creating Access Point Groups (GUI) 1073
Creating Access Point Groups (CLI) 1075
Viewing Access Point Groups (CLI) 1077
802.1Q-in-Q VLAN Tagging 1077
Restrictions for 802.1Q-in-Q VLAN Tagging 1077
Configuring 802.1Q-in-Q VLAN Tagging (GUI) 1078

Configuring 802.1Q-in-Q VLAN Tagging (CLI) 1078
Captive Portal Configuration for AP Groups 1079
Restrictions for Captive Portal Configuration for AP Groups 1080
Configuring Captive Portal for an AP Group (GUI) 1080
Configuring Captive Portal for an AP Group (CLI) 1080

CHAPTER 50 **Workgroup Bridges** 1081
Cisco Workgroup Bridges 1081
Guidelines and Restrictions for Cisco Workgroup Bridges 1082
Workgroup Bridge (WGB) Downstream Broadcast On Multiple VLANs 1083
Reliable WGB Downstream Broadcast for Multiple VLANs 1086
Controller Configuration 1088
WGB Configuration 1089
Troubleshooting Reliable Broadcast 1089
Parallel Redundancy Protocol Enhancement on AP and WGB 1092
Verifying the PRP Configurations 1099
Dual Radio Parallel Redundancy Protocol Enhancement on WGB 1101
Sample Network Configuration 1101
Configuration of Roaming Coordination on a Single WGB 1102
Controller Configurations 1102
WGB Configurations 1103
Aggregated Switch Configuration 1106
PRP Switch Configuration 1106
Verifying the Configuration 1107
Debug Commands 1108
DLEP Client Support on WGB 1108
Configuring the Physical Interface 1109
Configuring DLEP Local TCP Port and Server Address 1109
Configuring Optional DLEP Timers 1109
Configuring DLEP Neighbors 1110
Verifying DLEP Configuration 1111
Debug Commands 1113
Configuration Example 1113
Viewing the Status of Workgroup Bridges (GUI) 1126

Viewing the Status of Workgroup Bridges (CLI) 1127
Debugging WGB Issues (CLI) 1127
Non-Cisco Workgroup Bridges 1128
Restrictions for Non-Cisco Workgroup Bridges 1129
Cisco Wave 2 Access Points as Workgroup Bridges 1129
Guidelines and Restrictions on Cisco Wave 2 Access Points as Workgroup Bridges 1129
Configuring Cisco Wave 2 Access Points Image (CLI) 1130
Configuring Cisco Wave 2 Access Points as Workgroup Bridge (CLI) 1131
Configuring a Dot1X Credential (CLI) 1131
Configuring an EAP Profile (CLI) 1132
Configuring Manual-Enrollment of a Trustpoint for Workgroup Bridge (CLI) 1132
Configuring an SSID Profile (CLI) 1133
Configuring Radio Interface for Workgroup Bridges (CLI) 1134
Configuring Workgroup Bridge Timeouts (CLI) 1135
Configuring Bridge Forwarding for Workgroup Bridge (CLI) 1136

CHAPTER 51 **Software-Defined Access Wireless** 1139
Introduction to Software-Defined Access Wireless 1139
AP Bring-up Process 1141
Onboarding the Wireless Clients 1141
Platform Support 1142
Migration From Converged Access 1144
Restrictions 1145
Additional References 1145
Configuring SD-Access Wireless (CLI) 1145
Enabling SD-Access Wireless (GUI) 1146
Configuring SD-Access Wireless VNID (GUI) 1147
Configuring SD-Access Wireless WLAN (GUI) 1147
Configuring DNS Access Control List on SD-Access (GUI) 1148
Configuring Access Control List Templates (GUI) 1148

PART VIII **FlexConnect** 1151

CHAPTER 52 **FlexConnect** 1153

FlexConnect Overview 1153
FlexConnect Authentication Process 1155
FlexConnect Switching Modes 1158
FlexConnect Operation Modes 1158
FlexConnect VLANs and ACLs 1159
Central DHCP Server for FlexConnect 1159
Guidelines and Restrictions on FlexConnect 1159
Configuring FlexConnect 1161
Configuring the Switch at a Remote Site 1161
Configuring the Controller for FlexConnect 1162
Configuring the Controller for FlexConnect for a Centrally Switched WLAN Used for Guest Access 1163
Configuring the Controller for FlexConnect (GUI) 1163
Configuring the Controller for FlexConnect (CLI) 1166
Configuring an Access Point for FlexConnect 1167
Configuring an Access Point for FlexConnect (GUI) 1167
Configuring an Access Point for FlexConnect (CLI) 1170
Configuring an Access Point for Local Authentication on a WLAN (GUI) 1172
Configuring an Access Point for Local Authentication on a WLAN (CLI) 1172
Configuring FlexConnect Ethernet Fallback 1173
Information About FlexConnect Ethernet Fallback 1173
Restrictions for FlexConnect Ethernet Fallback 1173
Configuring FlexConnect Ethernet Fallback (GUI) 1173
Configuring FlexConnect Ethernet Fallback (CLI) 1174
VideoStream for FlexConnect 1174
Information About VideoStream for FlexConnect 1174
Configuring VideoStream for FlexConnect (GUI) 1175
Configuring VideoStream for FlexConnect (CLI) 1176
FlexConnect+Bridge Mode 1178
Information about Flex+Bridge Mode 1178
Configuring Flex+Bridge Mode (GUI) 1180
Configuring Flex+Bridge Mode (CLI) 1180

CHAPTER 53 **FlexConnect Groups** 1183

Information About FlexConnect Groups 1183
FlexConnect Groups and VLAN Support 1184
IP-MAC Context Distribution for FlexConnect Local Switching Clients 1184
Guidelines and Restrictions for IP-MAC Context Distribution for FlexConnect Local Switching Clients 1185
Configuring IP-MAC Context Distribution For FlexConnect Local Switching Clients (GUI) 1185
Configuring IP-MAC Context Distribution For FlexConnect Local Switching Clients (CLI) 1185
FlexConnect Groups and Backup RADIUS Servers 1186
FlexConnect Groups and Fast Secure Roaming 1186
FlexConnect Groups and Local Authentication Server 1186
Default FlexGroup 1187
Restrictions for FlexConnect Groups 1189
Configuring FlexConnect Groups (GUI) 1189
Configuring FlexConnect Groups (CLI) 1193
Moving APs from a Default FlexConnect Group to Another FlexConnect Group (GUI) 1195
Viewing APs in a Default FlexGroup (GUI) 1196
Viewing Default FlexGroup Details (CLI) 1196
VLAN-ACL Mapping 1199
Configuring VLAN-ACL Mapping on FlexConnect Groups (GUI) 1199
Configuring VLAN-ACL Mapping on FlexConnect Groups (CLI) 1200
Viewing VLAN-ACL Mappings (CLI) 1200
WLAN-VLAN Mapping 1200
Configuring WLAN-VLAN Mapping on FlexConnect Groups (GUI) 1200
Configuring WLAN-VLAN Mapping on FlexConnect Groups (CLI) 1201
OfficeExtend Access Points 1202
Implementing Security 1203
Configuring OfficeExtend Access Points 1203
Configuring OfficeExtend Access Points (GUI) 1203
Configuring OfficeExtend Access Points (CLI) 1205
Configuring a Personal SSID on an OfficeExtend Access Point 1208
Viewing OfficeExtend Access Point Statistics 1209
Viewing Voice Metrics on OfficeExtend Access Points 1209
Network Diagnostics 1210
Running Network Diagnostics (GUI) 1211

Running Network Diagnostics (CLI) 1211
Remote LANs 1211
Configuring a Remote LAN (GUI) 1212
Configuring a Remote LAN (CLI) 1212
FlexConnect AP Image Upgrades 1213
Restrictions on FlexConnect AP Image Upgrades 1213
Configuring FlexConnect AP Upgrades (GUI) 1214
Configuring FlexConnect AP Upgrades (CLI) 1215
FlexConnect AP Easy Admin 1215
Configuring FlexConnect AP Easy Admin on the Controller (GUI) 1215
Configuring FlexConnect AP Easy Admin on the Controller (CLI) 1216
WeChat Client Authentication 1216
Restrictions on WeChat Client Authentication 1216
Configuring WeChat Client Authentication on Controller (GUI) 1216
Configuring WeChat Client Authentication on Controller (CLI) 1218
Authenticating Client Using WeChat App for Mobile Internet Access (GUI) 1219
Authenticating Client Using WeChat App for PC Internet Access (GUI) 1219
Lawful Interception of Traffic 1220
Restrictions on Lawful Interception of Traffic 1220
Configuring Lawful Interception of Traffic on a Cisco Controller (CLI) 1220
Viewing and Debugging Lawful Interception of Traffic on a Cisco Access Point (CLI) 1220

CHAPTER 54 **FlexConnect Security** 1223
FlexConnect Access Control Lists 1223
Restrictions for FlexConnect Access Control Lists 1223
Configuring FlexConnect Access Control Lists (GUI) 1225
Configuring FlexConnect Access Control Lists (CLI) 1228
Viewing and Debugging FlexConnect Access Control Lists (CLI) 1229
Configuring CAPWAP Message Aggregation (CLI) 1230
Authentication, Authorization, Accounting Overrides 1230
Restrictions on AAA Overrides for FlexConnect 1232
Configuring AAA Overrides for FlexConnect on an Access Point (GUI) 1233
Configuring VLAN Overrides for FlexConnect on an Access Point (CLI) 1234
Software Defined Access and FlexConnect Post Authentication IPv6 ACL Support 1234

Applying FlexConnect Access Control Lists (GUI) 1234
Applying FlexConnect Access Control Lists (CLI) 1236

CHAPTER 55 OfficeExtend Access Points 1239
OfficeExtend Access Points 1239
Implementing Security 1240
Configuring OfficeExtend Access Points 1241
Configuring OfficeExtend Access Points (GUI) 1241
Configuring OfficeExtend Access Points (CLI) 1243
Configuring a Personal SSID on an OfficeExtend Access Point 1246
Viewing OfficeExtend Access Point Statistics 1247
Viewing Voice Metrics on OfficeExtend Access Points 1247
Network Diagnostics 1248
Running Network Diagnostics (GUI) 1248
Running Network Diagnostics (CLI) 1249
Remote LANs 1249
Configuring a Remote LAN (GUI) 1249
Configuring a Remote LAN (CLI) 1250

CHAPTER 56 FlexConnect AP Image Upgrades 1253
FlexConnect AP Image Upgrades 1253
Restrictions on FlexConnect AP Image Upgrades 1253
Configuring FlexConnect AP Upgrades (GUI) 1254
Configuring FlexConnect AP Upgrades (CLI) 1255

CHAPTER 57 FlexConnect AP Easy Admin 1257
FlexConnect AP Easy Admin 1257
Configuring FlexConnect AP Easy Admin on the Controller (GUI) 1257
Configuring FlexConnect AP Easy Admin on the Controller (CLI) 1258

CHAPTER 58 WeChat Authentication Based Internet Access 1259
WeChat Client Authentication 1259
Restrictions on WeChat Client Authentication 1259
Configuring WeChat Client Authentication on Controller (GUI) 1259

Configuring WeChat Client Authentication on Controller (CLI) 1261
Authenticating Client Using WeChat App for Mobile Internet Access (GUI) 1262
Authenticating Client Using WeChat App for PC Internet Access (GUI) 1262

CHAPTER 59 Lawful Interception of Traffic 1265
Lawful Interception of Traffic 1265
Restrictions on Lawful Interception of Traffic 1265
Configuring Lawful Interception of Traffic on a Cisco Controller (CLI) 1265
Viewing and Debugging Lawful Interception of Traffic on a Cisco Access Point (CLI) 1266

PART IX Monitoring the Network 1267

CHAPTER 60 Monitoring the Controller 1269
Viewing System Resources 1269
Viewing System Resources (GUI) 1269
Viewing System Resources (CLI) 1270

CHAPTER 61 System and Message Logging 1273
System and Message Logging 1273
Configuring System and Message Logging (GUI) 1273
Viewing Message Logs (GUI) 1276
Configuring System and Message Logging (CLI) 1276
Viewing System and Message Logs (CLI) 1281
Viewing Access Point Event Logs 1281
Information About Access Point Event Logs 1281
Viewing Access Point Event Logs (CLI) 1281

PART X Troubleshooting 1283

CHAPTER 62 Debugging on Cisco Wireless Controllers 1285
Troubleshooting AAA RADIUS Interactions for WLAN Authentication 1285
Understanding Debug Client on Wireless Controllers 1293
Deauthenticating Clients 1293
Deauthenticating Clients (GUI) 1293

Deauthenticating Clients (CLI) 1294
Using the CLI to Troubleshoot Problems 1294
Potential Reasons for Controller Reset 1296

CHAPTER 63 Controller Unresponsiveness 1299
Upload Logs and Crash Files 1299
Uploading Logs and Crash Files (GUI) 1299
Uploading Logs and Crash Files (CLI) 1300
Uploading Core Dumps from the Controller 1301
Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (GUI) 1301
Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (CLI) 1302
Uploading Core Dumps from Controller to a Server (CLI) 1303
Uploading Crash Packet Capture Files 1304
Restrictions for Uploading Crash Packet Capture Files 1305
Uploading Crash Packet Capture Files (GUI) 1305
Uploading Crash Packet Capture Files (CLI) 1306
Monitoring Memory Leaks 1307
Monitoring Memory Leaks (CLI) 1307
Troubleshooting Memory Leaks 1308

CHAPTER 64 Debugging on Cisco Access Points 1311
Troubleshooting Access Points Using Telnet or SSH 1311
Troubleshooting Access Points Using Telnet or SSH (GUI) 1312
Troubleshooting Access Points Using Telnet or SSH (CLI) 1312
Debugging the Access Point Monitor Service 1313
Debugging Access Point Monitor Service Issues (CLI) 1313
Sending Commands to Access Points 1313
Understanding How Access Points Send Crash Information to the Controller 1314
Understanding How Access Points Send Radio Core Dumps to the Controller 1314
Retrieving Radio Core Dumps (CLI) 1314
Uploading Radio Core Dumps (GUI) 1315
Uploading Radio Core Dumps (CLI) 1316
Viewing the AP Crash Log Information 1316
Viewing the AP Crash Log information (GUI) 1317

Viewing the AP Crash Log information (CLI) 1317
Viewing MAC Addresses of Access Points 1317
Disabling the Reset Button on Access Points to Lightweight Mode 1318
Viewing Access Point Event Logs 1318
Information About Access Point Event Logs 1318
Viewing Access Point Event Logs (CLI) 1318
Troubleshooting Clients on FlexConnect Access Points 1319
Troubleshooting OfficeExtend Access Points 1320
Troubleshooting Common Problems with OfficeExtend Access Points 1320
Link Test 1321
Performing a Link Test (GUI) 1322
Performing a Link Test (CLI) 1323

CHAPTER 65 **Packet Capture** 1325
Using the Debug Packet Logging Facility 1325
Configuring the Debug Facility (CLI) 1326
Wireless Sniffing 1330
Prerequisites for Wireless Sniffing 1330
Restrictions on Wireless Sniffing 1331
Configuring Sniffing on an Access Point (GUI) 1331
Configuring Sniffing on an Access Point (CLI) 1332

Preface

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

This preface includes the following sections:

- Audience, on page liii
- Conventions, on page liii
- Related Documentation, on page liv
- Communications, services, and additional information, on page lv

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.

Convention	Indication
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

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

- Feature Matrix for Wave 2 and 802.11ax (Wi-Fi 6) Access Points

  https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-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

- Cisco Mobility Express for Aironet Access Points

  https://www.cisco.com/c/en/us/support/wireless/mobility-express/series.html

Communications, services, and additional information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

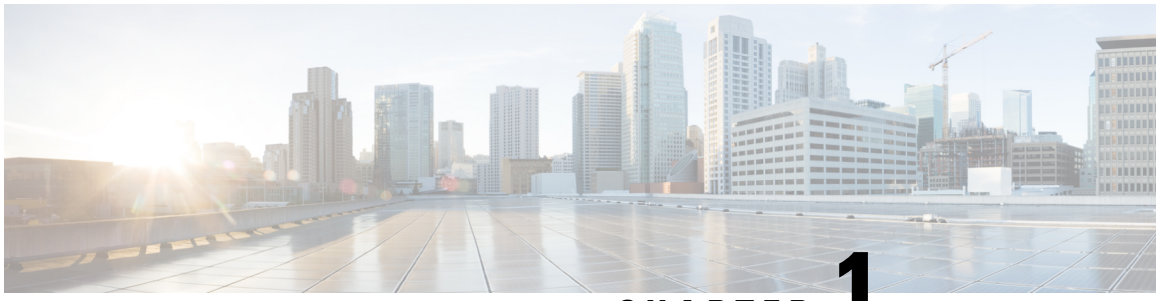
Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

PART I

Overview

- Cisco Wireless Solution Overview, on page 1
- Initial Setup, on page 5



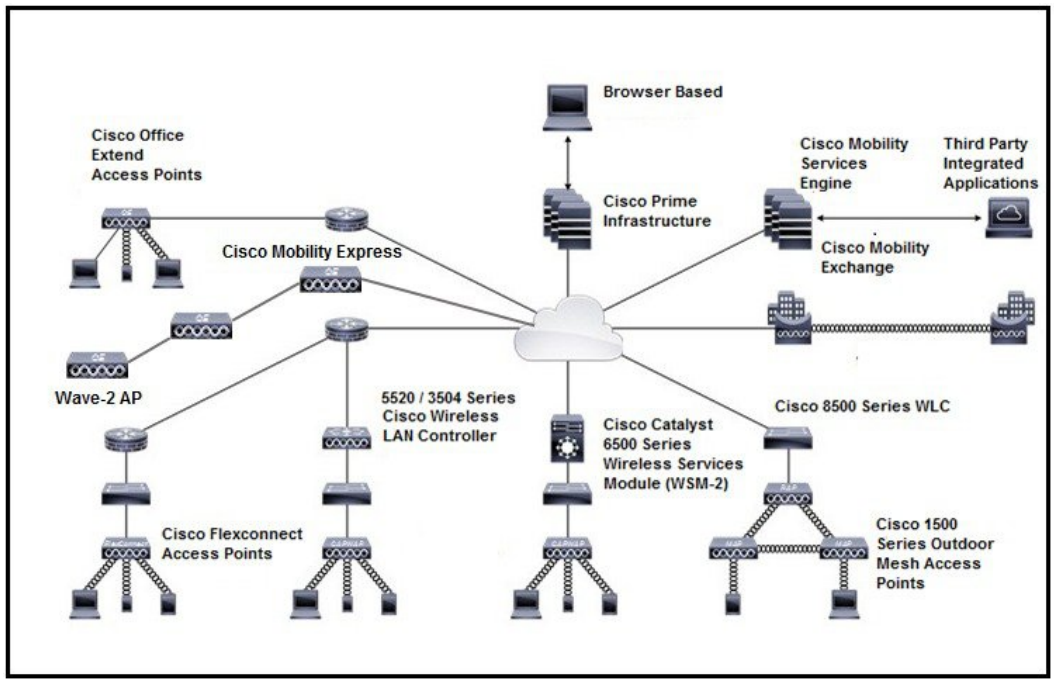
CHAPTER 1

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 the following:

- Client devices
- Access points (APs)

- Network unification through Cisco Wireless Controllers (controllers)
- 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 wireless LAN (WLAN) solution.

- Core Components, on page 2

Core Components

A Cisco Wireless network consists of the following core components:

- Cisco Wireless Controllers: 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 AireOS 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 radio frequency (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 3504 Wireless Controller
  - Cisco 5520 Wireless Controller
  - Cisco 8540 Wireless Controller
  - Cisco Virtual Wireless Controller

Note The Cisco Wireless Controllers do not support 10 G-based CISCO-AMPHENOL SFP. However, you may use an alternate vendor SFP.

- Cisco Access Points: Cisco access points (APs) 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 https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/series.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/series.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 Cisco Wave 2 AP with an in-built software-based wireless controller managing other Cisco APs in the network.

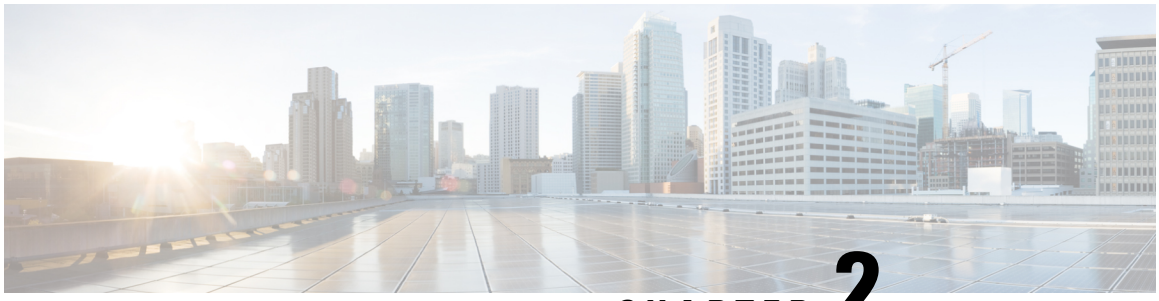
The AP acting as the controller is referred to as the primary AP while the other APs in the Cisco Mobility Express network, which are managed by this primary AP, are referred to as subordinate APs.

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

Cisco Mobility Express provides most features of a controller and can 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



CHAPTER 2

Initial Setup

- Cisco WLAN Express Setup, on page 5
- Configuring the Controller Using the Configuration Wizard, on page 11
- Using the AutoInstall Feature for Controllers Without a Configuration, on page 25
- Managing the Controller System Date and Time, on page 26

Cisco WLAN Express Setup

Cisco WLAN Express Setup is a simplified, out-of-the-box installation and configuration interface for Cisco Wireless Controllers. This section provides instructions to set up a controller to operate in a small, medium, or large network wireless environment, where access points can join and together as a simple solution provide various services such as corporate employee or guest wireless access on the network.

There are two methods:

- Wired method
- Wireless method

With this, there are three ways to set up a controller:

- Cisco WLAN Express Setup
- Traditional command line interface (CLI) through serial console
- Updated method using network connection directly to the controller GUI setup wizard

Note Cisco WLAN Express Setup can be used only for the first time in out-of-the-box installations or when controller configuration is reset to factory defaults.

Feature History

- Release 7.6.120.0: This feature was introduced and supported only on Cisco 2500 Series Wireless Controller. It includes an easy-to-use GUI Configuration Wizard, an intuitive monitoring dashboard and several Cisco Wireless LAN best practices enabled by default.
- Release 8.0.110.0: The following enhancements were made:

- Connect to any port: You can connect a client device to any port on the Cisco 2500 Series Wireless Controller and access the GUI configuration wizard to run Cisco WLAN Express. Previously, you were required to connect the client device to only port 2.
- Wireless Support to run Cisco WLAN Express: You can connect an AP to any of the ports on the Cisco 2500 Series Wireless Controller, associate a client device with the AP, and run Cisco WLAN Express. When the AP is associated with the Cisco 2500 Series Wireless Controller, only 802.11b and 802.11g radios are enabled; the 802.11a radio is disabled. The AP broadcasts an SSID named *CiscoAirProvision*, which is of WPA2-PSK type with the key being *password*. After a client device associates with this SSID, the client device automatically gets an IP address in the 192.168.x.x range. On the web browser of the client device, go to http://192.168.1.1 to open the GUI configuration wizard.

Note This feature is not supported on mobile devices such as smartphones and tablet computers.

- Release 8.1: The following enhancements are made:
  - Added support for the Cisco WLAN Express using the wired method to Cisco 5500, Flex 7500, 8500 Series Wireless Controllers and Cisco Virtual Wireless Controller.
  - Introduced the Main Dashboard view and compliance assessment and best practices. For more details, see the controller Online Help.

Configuration Checklist

The following checklist is for your reference to make the installation process easy. Ensure that you have these requirements ready before you proceed:

1. Network switch requirements:
   a. Controller switch port number assigned
   b. Controller assigned switch port
   c. Is the switch port configured as trunk or access?
   d. Is there a management VLAN? If yes, Management VLAN ID
   e. Is there a guest VLAN? If yes, Guest VLAN ID
2. Controller Settings:
   a. New admin account name
   b. Admin account password
   c. System name for the controller
   d. Current time zone
   e. Is there an NTP server available? If yes, NTP server IP address

Note We recommend using a reachable NTP server IP address. APs do not support FQDN in a day0 scenario.

   f. Controller Management Interface:
      1. IP address
      2. Subnet Mask
      3. Default gateway
   g. Management VLAN ID

3. Corporate wireless network
4. Corporate wireless name or SSID
5. Is a RADIUS server required?
6. Security authentication option to select:
   a. WPA/WPA2 Personal
   b. Corporate passphrase (PSK)
   c. WPA/WPA2 (Enterprise)
   d. RADIUS server IP address and shared secret
7. Is a DHCP server known? If yes, DHCP server IP address
8. Guest Wireless Network (optional)
   a. Guest wireless name/SSID
   b. Is a password required for guest?
   c. Guest passphrase (PSK)
   d. Guest VLAN ID
   e. Guest networking
      1. IP address
      2. Subnet Mask
      3. Default gateway
9. Advanced option: Configure RF Parameters for Client Density as Low, Medium, or High.

Preparing for Setup Using Cisco WLAN Express

- Do not auto-configure the controller or use the wizard for configuration.
- Do not use console interface; the only connection to the controller should be client connected to service port.

- Configure DHCP or assign static IP 192.168.1.X to laptop interface connected to service port.

For more information about Cisco WLAN Express, see WLAN Express Setup and Best Practices Deployment Guide.

This section contains the following subsections:

Setting up Cisco Wireless Controller using Cisco WLAN Express (Wired Method)

Procedure

Step 1 Connect a laptop's wired Ethernet port directly to the Service port of the controller. The port LEDs blink to indicate that both the machines are properly connected.

Note
It may take several minutes for the controller to fully power on to make the GUI available to the PC. Do not auto-configure the controller.

The LEDs on the front panel provide the system status:

- If the LED is off, it means that the controller is not ready.
- If the LED is solid green, it means that the controller is ready.

Step 2 Configure DHCP option on the laptop that you have connected to the Service port. This assigns an IP address to the laptop from the controller Service port 192.168.1.X, or you can assign a static IP address 192.168.1.X to the laptop to access the controller GUI; both options are supported.

Step 3 Open any one of the following supported web browsers and type http://192.168.1.1 in the address bar.

- Mozilla Firefox version 32 or later (Windows, Mac)
- Microsoft Internet Explorer version 10 or later (Windows)
- Apple Safari version 7 or later (Mac)

Note
This feature is not supported on mobile devices such as smartphones and tablet computers.

Step 4 Create an administrator account by providing the name and password. Click **Start** to continue.

Step 5 In the **Set Up Your Controller** box, enter the following details:

a. System Name for the controller

b. Current time zone

c. NTP Server (optional)

Note
We recommend using a reachable NTP server IP address. APs do not support FQDN in a day0 scenario.

d. Management IP Address

e. Subnet Mask

f. Default Gateway

g. Management VLAN ID—If left unchanged or set to 0, the network switch port must be configured with a native VLAN 'X0'

Note
The setup attempts to import the clock information (date and time) from the computer via JavaScript. We recommend that you confirm this before continuing. Access points rely on correct clock settings to be able to join the controller.

Step 6 In the **Create Your Wireless Networks** box, in the **Employee Network** area, use the checklist to enter the following data:

a) Network name/SSID
b) Security
c) Pass Phrase, if Security is set to WPA/WPA2 Personal
d) DHCP Server IP Address: If left empty, the DHCP processing is bridged to the management interface
e) (Optional) Enable **Apply Cisco ISE default settings** to automatically set the following parameters:

- CoA is enabled by default
- The same Authentication server details (IP and shared-secret) are applied to the Accounting server
- When you add the Authentication server for a WLAN, the Authentication server details are also applied to the Accounting server for the WLAN
- AAA override is enabled by default
- Set the NAC State to ISE NAC by default
- RADIUS client profiling: DHCP profiling and HTTP profiling are enabled by default
- Captive bypass mode is enabled by default
- The Layer 2 security of the WLAN is set to WPA+WPA2
- 802.1X is the default AKM.
- MAC filtering is enabled if the Layer 2 security is set to None.

The Layer 2 security is either WPA+WPA2 with 802.1X or None with MAC filtering. You can change these default settings if required.

Step 7 (Optional) In the **Create Your Wireless Networks** box, in the **Guest Network** area, use the checklist to enter the following data:

a) Network name/SSID
b) Security
c) VLAN IP Address, VLAN Subnet Mask, VLAN Default Gateway, VLAN ID
d) DHCP Server IP Address: If left empty, the DHCP processing is bridged to the management interface

Step 8 In the **Advanced Setting** box, in the **RF Parameter Optimization** area, do the following:

a) Select the client density as Low, Typical, or High.
b) Configure the RF parameters for RF Traffic Type, such as Data and Voice.
c) Change the Service port IP address and subnet mask, if necessary.

Step 9 Click **Next**.

Step 10 Review your settings and then click **Apply** to confirm.

The controller reboots automatically. You will be prompted that the controller is fully configured and will be restarted. Sometimes, you might not be prompted with this message. In this scenario, do the following:

a) Disconnect the laptop from the controller service port and connect it to the Switch port.
b) Connect the controller port 1 to the switch configured trunk port.
c) Connect access points to the switch if not already connected.
d) Wait until the access points join the controller.

RF Profile Configurations

Procedure

Step 1 After a successful login as an administrator, choose **Wireless** > **RF Profiles** to verify whether the Cisco WLAN Express features are enabled by checking that the predefined RF profiles are created on this page.

You can define AP Groups and apply appropriate profile to a set of APs.

Step 2 Choose **Wireless** > **Advanced** > **Network Profile**, verify the client density and traffic type details.

Note
We recommend that you use **RF and Network profiles** configuration even if Cisco WLAN Express was not used initially or if the controller was upgraded from a release that is earlier than Release 8.1.

Default Configurations

When you configure your Cisco Wireless Controller, the following parameters are enabled or disabled. These settings are different from the default settings obtained when you configure the controller using the CLI wizard.

Parameters in New Interface	Default Setting
Aironet IE	Disabled
DHCP Address Assignment (Guest SSID)	Enabled
Client Band Select	Enabled
Local HTTP and DHCP Profiling	Enabled
Guest ACL	Applied. **Note** Guest ACL denies traffic to the management subnet.
CleanAir	Enabled
EDRRM	Enabled

Parameters in New Interface	Default Setting
EDRRM Sensitivity Threshold	• Low sensitivity for 2.4 GHz. • Medium sensitivity for 5 GHz.
Channel Bonding (5 GHz)	Enabled
DCA Channel Width	40 MHz
mDNS Global Snooping	Enabled
Default mDNS profile	Two new services added: • Better printer support • HTTP
AVC (only AV)	Enabled only with following prerequisites: • Bootloader version—1.0.18 Or • Field Upgradable Software version—1.8.0.0 and above
Management	• Via Wireless Clients—Enabled • HTTP/HTTPS Access—Enabled • WebAuth Secure Web—Enabled
Virtual IP Address	192.0.2.1
Multicast Address	Not configured
Mobility Domain Name	Name of employee SSID
RF Group Name	Default

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.

Configuring the Controller (GUI)

Procedure

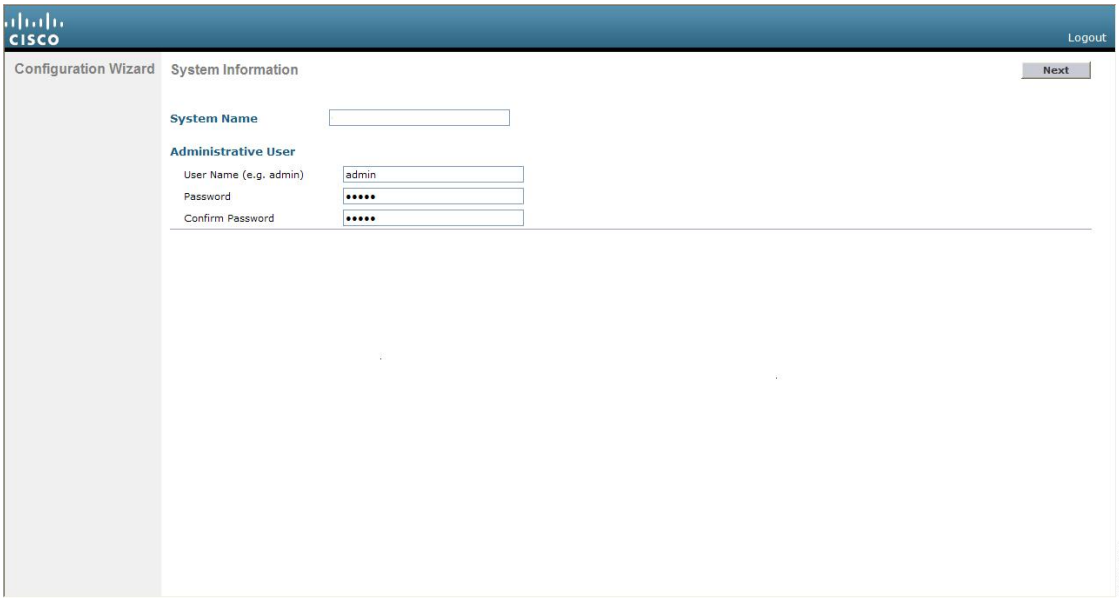
Step 1 Connect your PC to the service port and configure it to use the same subnet as the controller.

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

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.

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

Figure 2: Configuration Wizard — System Information Page



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

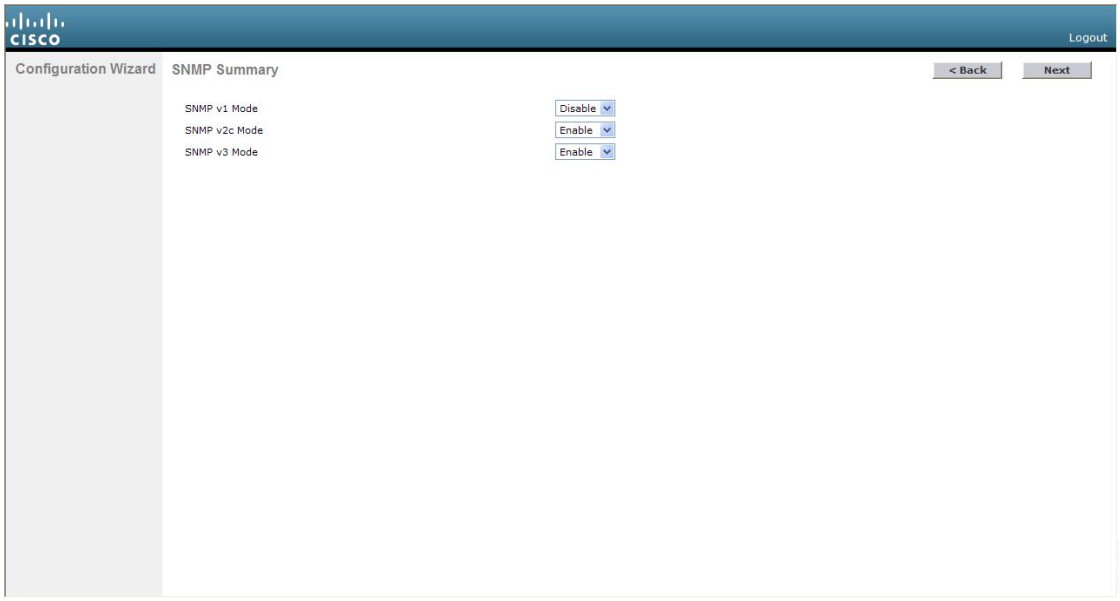
Step 4 In the **User Name** field, enter the administrative username to be assigned to this controller. You can enter up to 24 ASCII characters. The default username is *admin*.

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*.

- 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 3: 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.

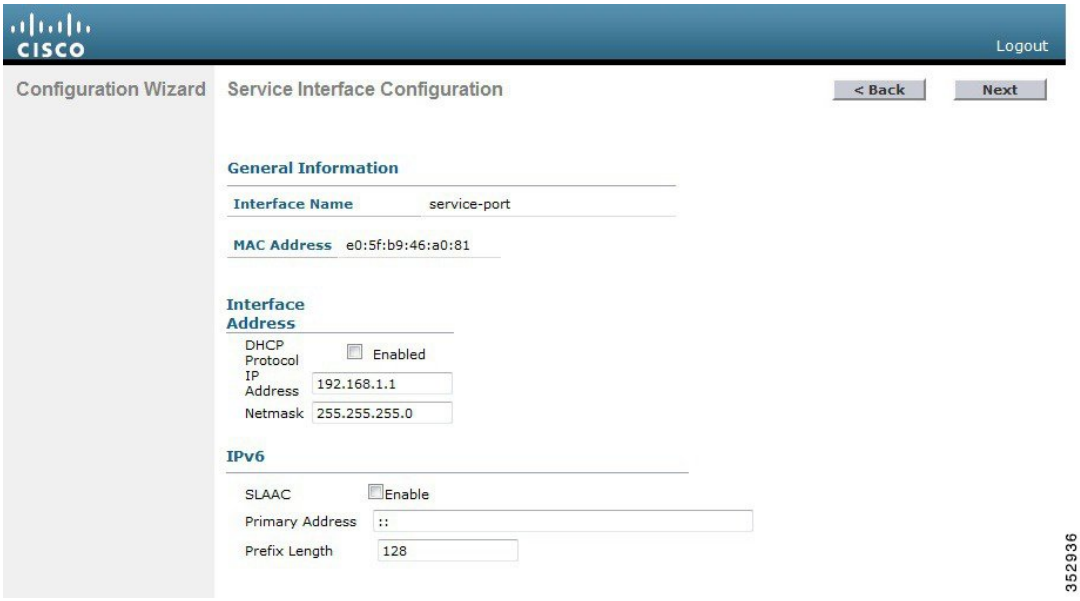
Step 10 Click **Next**.

Step 11 When the following message is displayed, 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 4: 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.

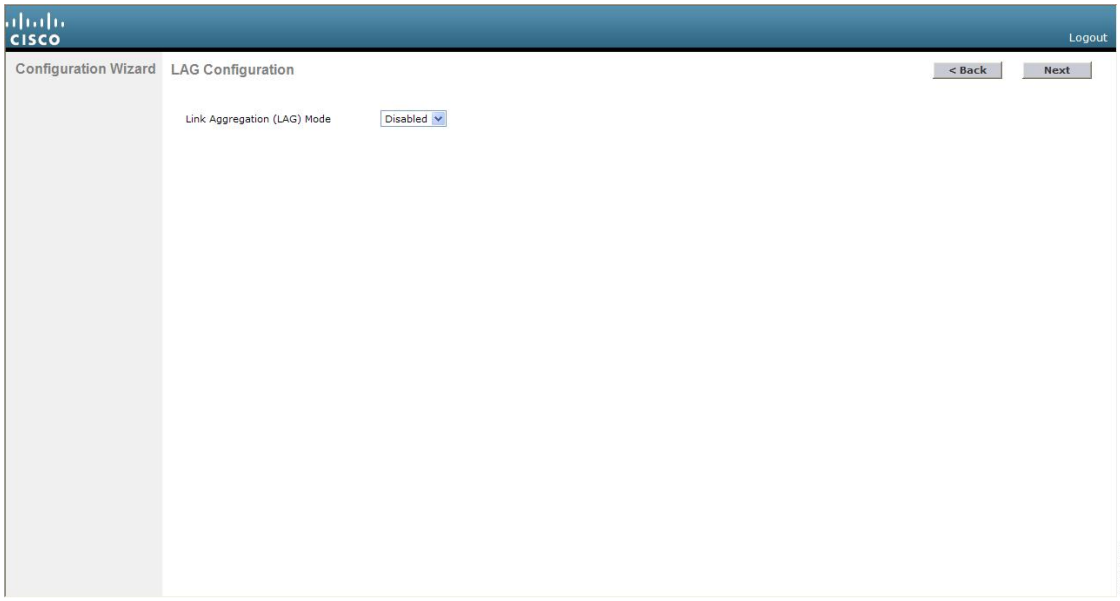
Step 13 Perform one of the following:

- 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.

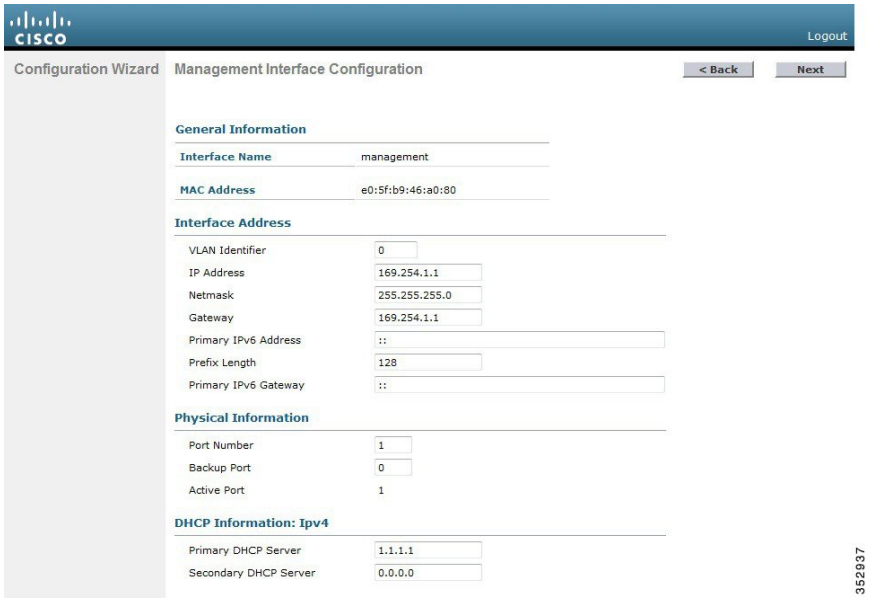
Figure 5: Configuration Wizard—LAG Configuration Page



Step 15 To enable link aggregation (LAG), choose **Enabled** from the Link Aggregation (LAG) Mode drop-down list. To disable LAG, leave this field 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** field, 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** field, enter the IP address of the management interface.

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

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

Step 21 In the **Port Number** field, 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** field, 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** field, 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.

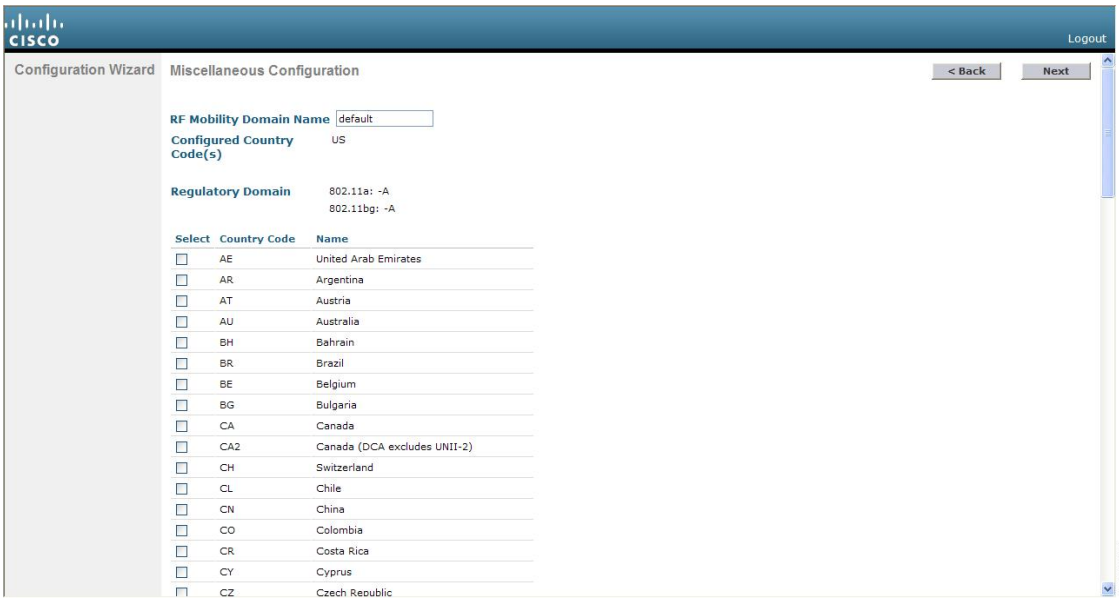
Step 24 In the **Secondary DHCP Server** field, enter the IP address of an optional secondary DHCP server that will supply IP addresses to clients, the controller's management interface, and optionally, the service port interface.

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

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

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

Figure 6: Configuration Wizard—Miscellaneous Configuration Page



Step 28 In the **RF Mobility Domain Name** field, 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)** field 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.

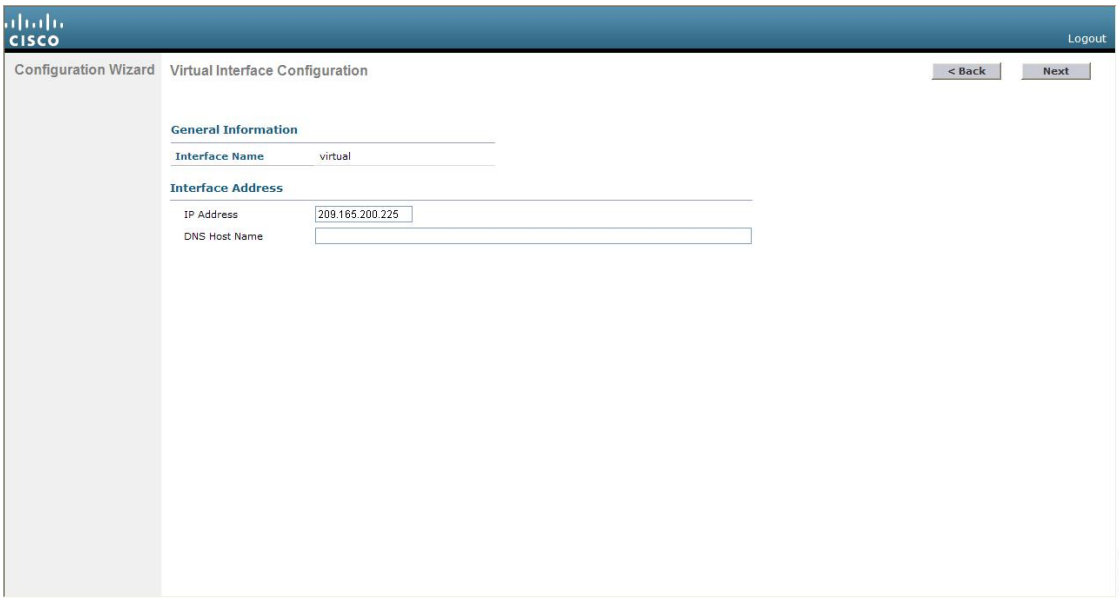
Step 30 Click **Next**.

Step 31 When the following message is displayed, 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 7: Configuration Wizard — Virtual Interface Configuration Page



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

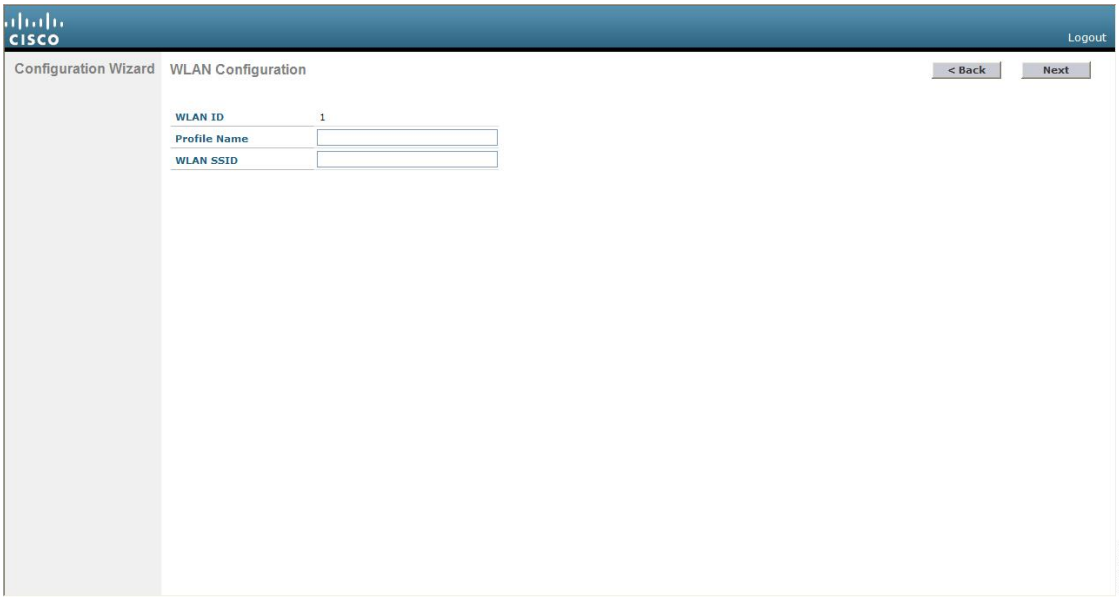
Note
The virtual interface is used to support mobility management, DHCP relay, and embedded Layer 3 security such as guest web authentication and VPN termination. All controllers within a mobility group must be configured with the same virtual interface IP address.

Step 33 In the **DNS Host Name** field, 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 8: Configuration Wizard — WLAN Configuration Page



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

Step 36 In the **WLAN SSID** field, 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.

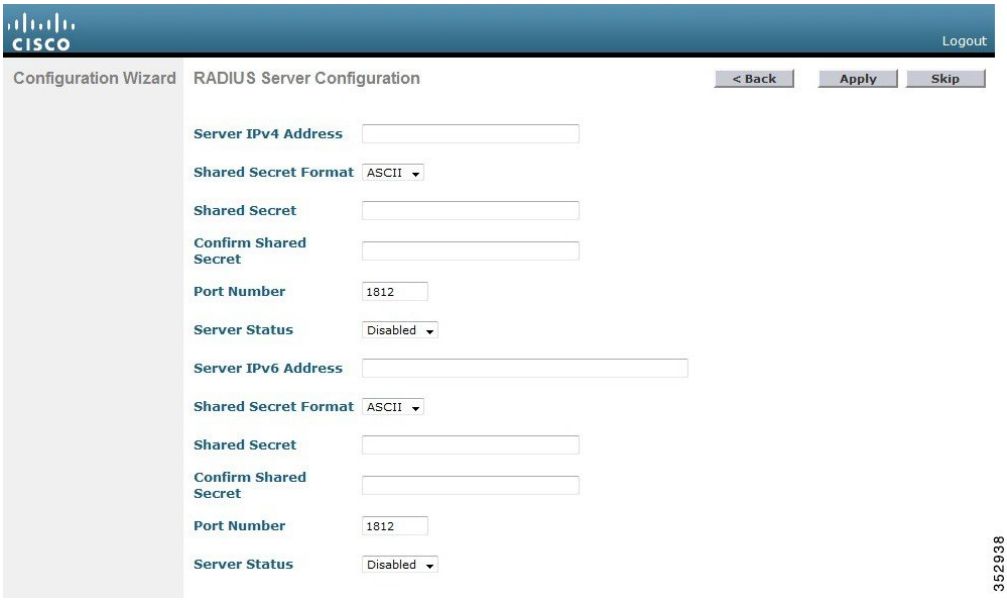
Step 37 Click **Next**.

Step 38 When the following message is displayed, 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 9: Configuration Wizard-RADIUS Server Configuration Page



Step 39 In the **Server IP Address** field, 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.

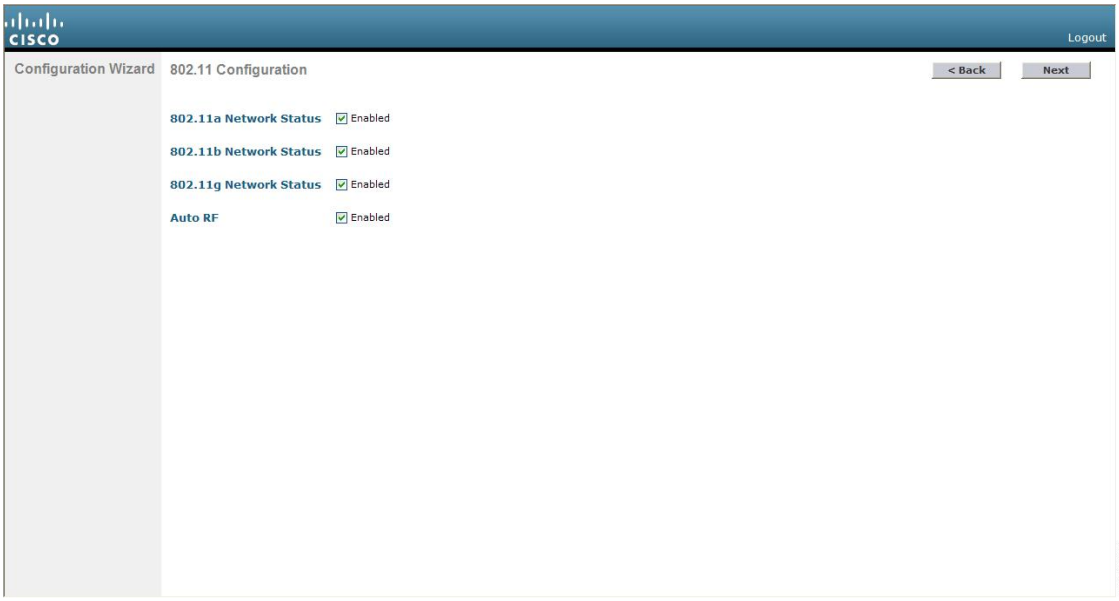
Step 41 In the **Shared Secret** and **Confirm Shared Secret** boxes, enter the secret key used by the RADIUS server.

Step 42 In the **Port Number** field, 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 field set to **Disabled**.

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

Figure 10: Configuration Wizard—802.11 Configuration Page



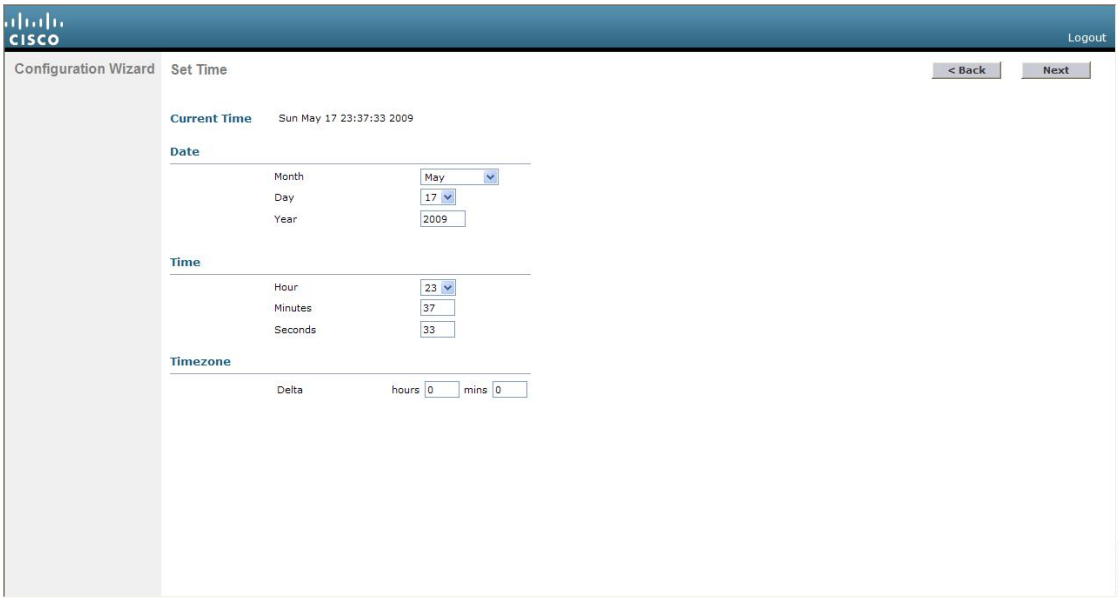
Step 45 To enable the 802.11a, 802.11b, and 802.11g lightweight access point networks, leave the **802.11a Network Status**, **802.11b Network Status**, and **802.11g Network Status** check boxes checked. To disable support for any of these networks, uncheck the check boxes.

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 11: Configuration Wizard — Set Time Screen



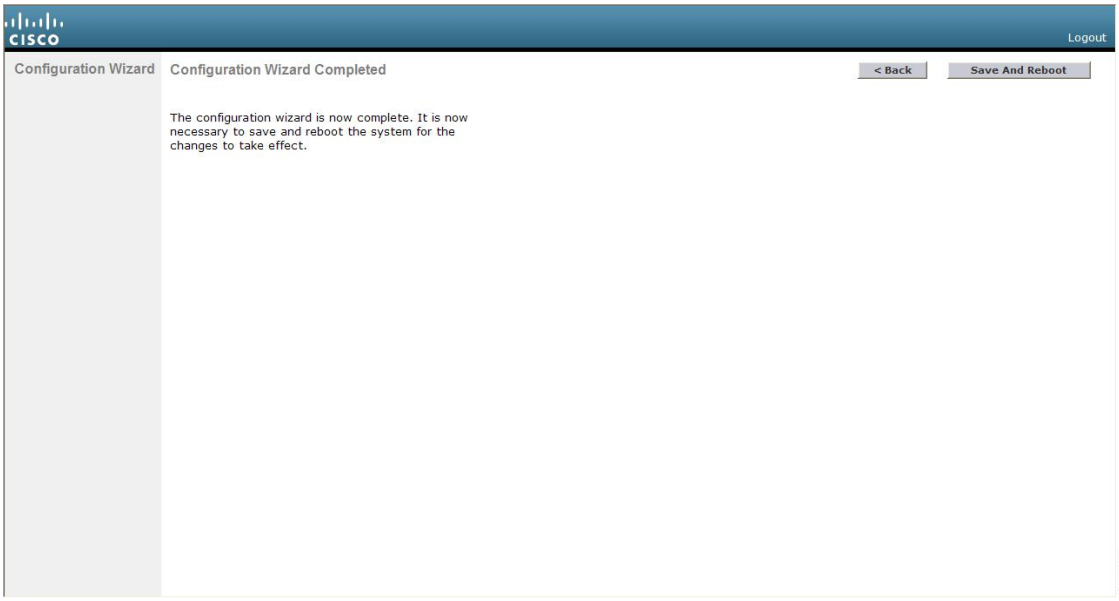
Step 48 To manually configure the system time on your controller, enter the current date in Month/DD/YYYY format and the current time in HH:MM:SS format.

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** field and the local minute difference from GMT in the **Delta Mins** field.

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 12: 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 is displayed, 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 are displayed in brackets after each configuration parameter. The default value is displayed in all uppercase letters.
- If you enter an incorrect response, an appropriate error message is displayed, 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.

Procedure

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.

- 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.

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 is displayed: `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.

After you have completed *step 22*, the wizard prompts you to configure IPv6 parameters. Enter **YES** to proceed.

Step 23 Enter the service port interface IPv6 address configuration. You can enter either **static** or **SLAAC**.

- If you entered, **SLAAC**, then IPv6 address is autoconfigured.
- If you entered, **static**, you must enter the IPv6 address and its prefix length of the service interface.

Step 24 Enter the IPv6 address of the management interface.

Step 25 Enter the IPv6 address prefix length of the management interface.

Step 26 Enter the gateway IPv6 address of the management interface .

After the management interface configuration is complete, the wizard prompts to configure IPv6 parameters for RADIUS server. Enter **yes**.

Step 27 Enter the IPv6 address of the RADIUS server.

Step 28 Enter the communication port number of the RADIUS server. The default value is 1812.

Step 29 Enter the secret key for IPv6 address of the RADIUS server.

Once the RADIUS server configuration is complete, the wizard prompts to configure IPv6 NTP server. Enter **yes**.

Step 30 Enter the IPv6 address of the NTP server.

Step 31 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 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.

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.

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.
- Notifications for certificates expiring after the year 2049 are not triggered. This is due to the change in the date format to Generalized time format from the year 2050. Currently UTC time format is used to validate the certificate.

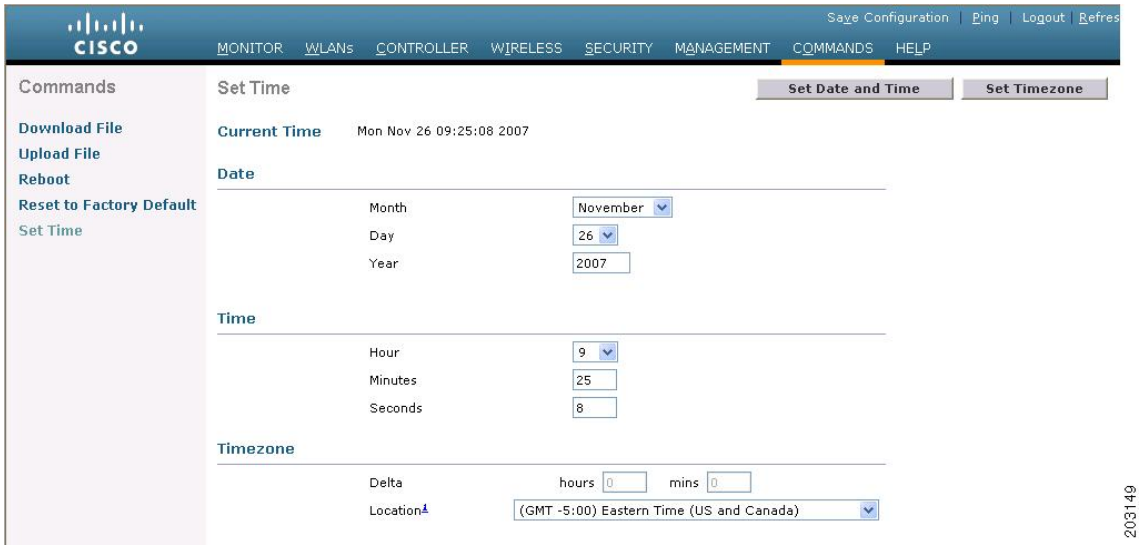
  For more information, see section 4.1.2.5 of the RFC 5280 document at https://tools.ietf.org/html/rfc5280.

Configuring the Date and Time (GUI)

Procedure

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

Figure 13: 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)

Procedure

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 is displayed:

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

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

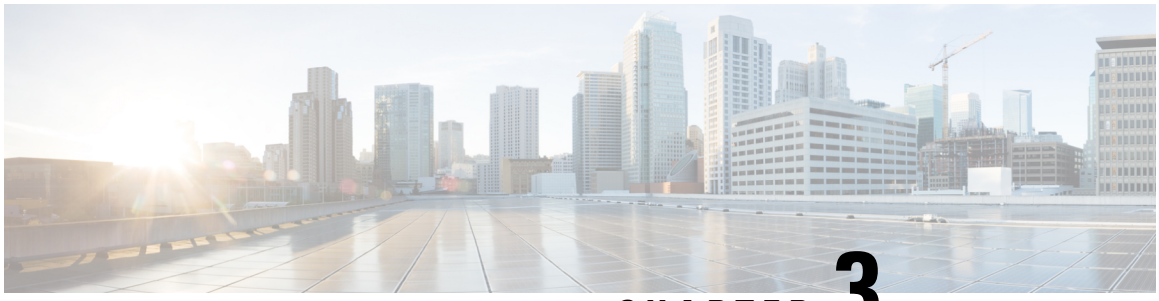
```
 Index     NTP Key Index     NTP Server    NTP Msg Auth Status
-------  ---------------------------------------------------------
   1              1        209.165.200.225     AUTH SUCCESS
```

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.

PART II

Management of Controllers

- Administration of Controller, on page 33
- Monitoring Dashboard, on page 47
- Managing Licenses, on page 53
- Managing Software, on page 79
- Managing Configuration, on page 93
- Network Time Protocol Setup, on page 107
- High Availability, on page 111
- Managing Certificates, on page 129
- AAA Administration, on page 145
- Managing Users, on page 197
- Ports and Interfaces, on page 211
- IPv6 Clients, on page 241
- Access Control Lists, on page 247
- Multicast/Broadcast Setup, on page 281
- Controller Security, on page 307
- Cisco Umbrella WLAN (OpenDNS), on page 337
- SNMP, on page 343



CHAPTER 3

Administration of Controller

- Using the Controller Interface, on page 33
- Enabling Web and Secure Web Modes, on page 38
- Telnet and Secure Shell Sessions, on page 41
- Management over Wireless, on page 44
- Configuring Management using Dynamic Interfaces (CLI), on page 46

Using the Controller Interface

You can use the controller interface in the following two methods:

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.

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

The controller GUI is supported on the following web browsers:

- Microsoft Internet Explorer 11 or a later version (Windows)
- Mozilla Firefox, Version 32 or a later version (Windows, Mac)
- Apple Safari, Version 7 or a later version (Mac)

Note We recommend that you use the controller GUI on a browser loaded with webadmin certificate (third-party certificate). We also recommend that you do not use the controller GUI on a browser loaded with self-signed certificate. Some rendering issues have been observed on Google Chrome (73.0.3675.0 or a later version) with self-signed certificates. For more information, see CSCvp80151.

Guidelines and Restrictions on using Controller GUI

Follow these guidelines when using the controller GUI:

- 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.
- The controller may intermittently or fail to respond when there is a high volume of packets destined for the controller's management IP address.
- 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 access the online help. You might have 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.

Procedure

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

Procedure

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 controller GUI.

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

Using the Controller CLI

A Cisco Wireless 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 We recommend that you do not run two simultaneous CLI operations because this might result in incorrect behavior or incorrect output of the CLI.

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 model's installation guide.

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:

Procedure

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.
- The **aes-cbc ciphers** are not supported on controller. The SSH client which is used to log in to the controller should have minimum a non-aes-cbc cipher.
- The controller may intermittently or fail to respond when there is a high volume of packets destined for the controller's management IP address.

Procedure

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 shows 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 the **logout** command. You are prompted to save any changes that 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 unambiguous.
- 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
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

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.

Note Due to a limitation in RFC-6797 for the HTTP Strict Transport Security (HSTS), when accessing the controller's GUI using the management IP address, HSTS is not honored and fails to redirect from HTTP to HTTPS protocol in the browser. The redirect fails if the controller's GUI was previously accessed using the HTTPS protocol. For more information, see RFC-6797 document.

This section contains the following subsections:

Enabling Web and Secure Web Modes (GUI)

Procedure

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 Choose **Controller** > **General** to open the **General** page.

Choose one of the following options from the **Web Color Theme** drop-down list:

- **Default**—Configures the default web color theme for the controller GUI.
- **Red**—Configures the web color theme as red for the controller GUI.

Step 8 Click **Apply**.

Step 9 Click **Save Configuration**.

Enabling Web and Secure Web Modes (CLI)

Procedure

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 Configure the web color theme for the controller GUI by entering this command:

config network webcolor {**default** | **red**}

The default color theme for the controller GUI is enabled. You can change the default color scheme as red using the **red** option. If you are changing the color theme from the controller CLI, you need to reload the controller GUI screen to apply your changes.

Step 3 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 4 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. With Release 8.10, this command is, by default, in enabled state.

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 5 Enable or disable SSLv3 for web administration by entering this command:

config network secureweb sslv3 {**enable** | **disable**}

Step 6 Enable 256 bit ciphers for a SSH session by entering this command:

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

Step 7 [Optional] Disable telnet by entering this command:

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

Step 8 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 9 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 10 (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 11 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 12 Reboot the controller by entering this command:

reset system

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.

In Release 8.10.130.0, Cisco Wave 2 APs support the following cipher suites:

- **HMAC:** hmac-sha2-256,hmac-sha2-512
- **KEX:** diffie-hellman-group18-sha512,diffie-hellman-group14-sha1,ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521
- **Host Key:** ecdsa-sha2-nistp256, ssh-rsa
- **Ciphers**: aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

This section contains the following subsections:

Guidelines and Restrictions on Telnet and Secure Shell Sessions

- When the controller's config paging is disabled and clients running OpenSSH_8.1p1 OpenSSL 1.1.1 library are connected to the controller, you may experience the output display freezing. You may press any key to unfreeze the display.

  We recommend that you use one of the following methods to avoid this situation:

  - Connect using different version of OpenSSH and Open SSL library
  - Use Putty
  - Use Telnet

- After an AP reboots, you need to enable Telnet if it reverts to its default disabled state.
- 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 many configurations and has a high count of APs and clients, or in either of the cases. We recommend that you 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.

- In Release 8.10.130.0 and later releases, controllers no longer support legacy cipher suites, weak ciphers, MACs and KEXs.

Configuring Telnet and SSH Sessions (GUI)

Procedure

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

Step 2 In the **Idle Timeout(minutes)** field, enter the number of minutes that a Telnet session is allowed to remain inactive before being terminated. The valid range is from 0 to 160 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 from 0 to 5 sessions (inclusive), and the default value is 5 sessions. A value of zero indicates that Telnet or SSH sessions are disallowed.

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

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

Step 7 Save your configuration.

What to do next

To see a summary of the Telnet configuration settings, choose **Management** > **Summary**. The **Summary** page that is displayed shows additional Telnet and SSH sessions are permitted.

Configuring Telnet and SSH Sessions (CLI)

Procedure

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 controller.

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*

The valid range for *timeout* is from 0 to 160 minutes, and 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*

The valid range *session_num* is from 0 to 5, and the default value is 5 sessions. A value of zero indicates that Telnet or 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

Procedure

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

show network summary

Information similar to the following is displayed:

```
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 is displayed:

```
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 is displayed:

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

Step 4 Clear Telnet or SSH sessions by entering this command:

clear session *session-id*

You can identify the *session-id* by using the **show login-session** command.

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.

Procedure

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

Step 2 On the **Local Management Users** page, check or uncheck 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**}

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 management 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)

Procedure

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)

Procedure

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*

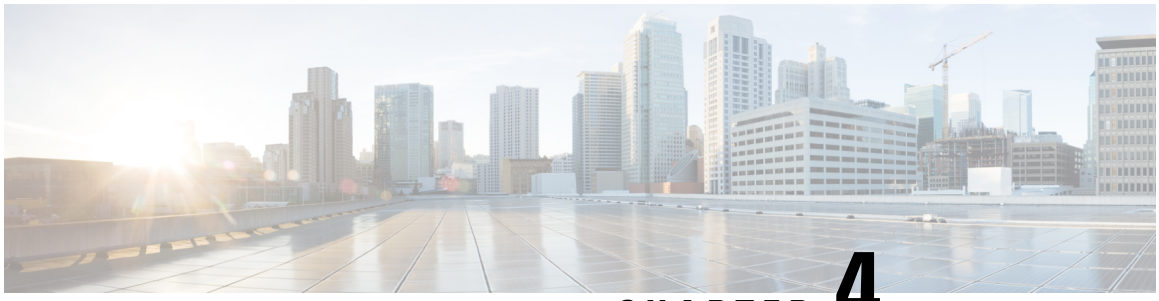
Configuring Management using Dynamic Interfaces (CLI)

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 4

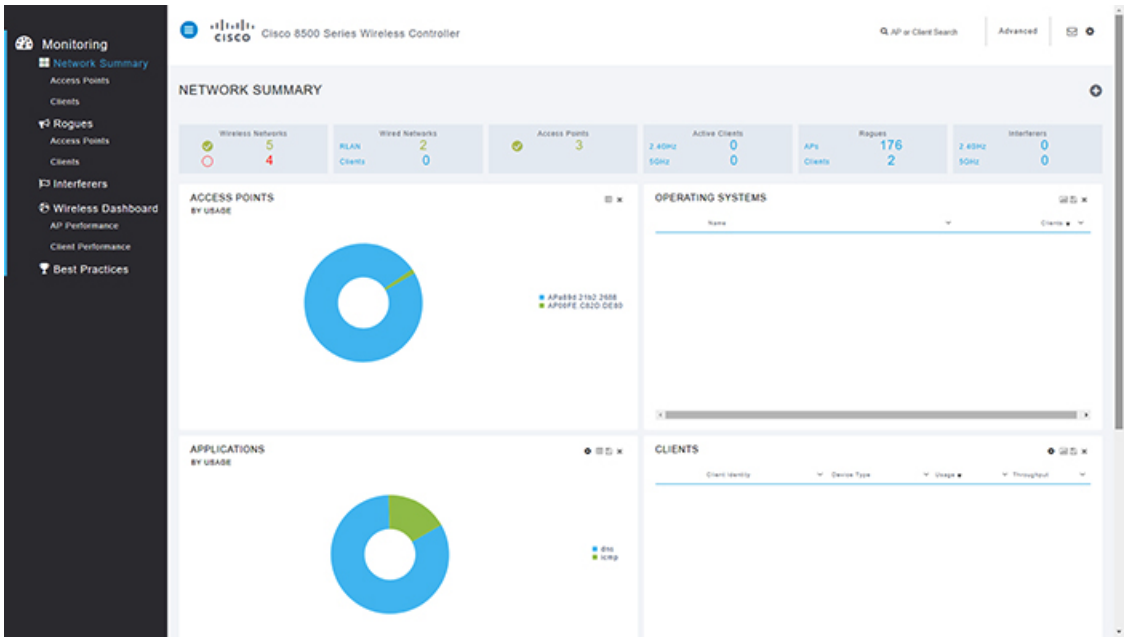
Monitoring Dashboard

- Monitoring Dashboard, on page 47
- Network Summary, on page 50
- Rogues, on page 51
- Interferers, on page 51
- Wireless Dashboard, on page 52
- Best Practices, on page 52

Monitoring Dashboard

The controller GUI has a monitoring dashboard that gives a single-window overview of the network devices that are connected to the controller.

Figure 14: Monitoring Dashboard



The monitoring dashboard is displayed by default when you log in to the controller GUI. The dashboard is split into three sections:

- Numerical statistics
- Graphical widgets
- Monitor pane with selection options

At an interval of 60 seconds, the dashboard widgets and the statistical data are automatically refreshed.

Note After you enable debugging on the controller using SSH protocol, you may experience sluggish GUI response. We recommend that you use one of the following two ciphers for SSH connection to minimize the sluggish response:

- aes256-gcm@openssh.com
- aes128-gcm@openssh.com

You can SSH to the controller by entering this command:

ssh -c { **aes128-gcm@openssh.com** | **aes256-gcm@openssh.com** } *controller username controller ip-addr*

This section contains the following subsections:

Numerical Statistics

This is the top section of the dashboard where you get a quick view of what is on the network:

- Wireless Networks: Shows the number of WLANs enabled and disabled on this controller.
- Wired Networks: Shows the number of RLANs and clients that are associated to the network.
- Access Points: Shows the number of active Cisco APs in the network.
- Active Clients: Shows the number of 2.4 and 5–GHz clients in the network.
- Rogues: Shows the number of APs and clients which are found in your network.
- Interferers: Shows the number of detected interference devices on 2.4 and 5–GHz bands.

Note Selecting the headline or the statistical value takes you to the respective page in the **Advanced** section.

Graphical Widgets

These graphical widgets present the numbers in the form of graphs. You can select the widgets to display from the available list.

Access Points

You can see the doughnut graph representing the AP usage in percentage on this controller. To change to the list view, click on the top right of the widget. The list view displays the APs with the number of connected

clients, amount of data traffic served, and the throughput values. By default, the AP list is sorted by name; however, you can also sort the list by clients, usage, or throughput.

Note The AP list is limited to display only top 10 APs. Therefore, you might not see all the APs associated with the controller in this widget.

Clicking on the AP takes you to the **Access Point View** page. The **Access Point View** page gives the Cisco AP's general, performance, and radio parameter details for both 2.4 GHz and 5-GHz radios. You can restart the AP from this page.

The AP performance values displayed are gathered from the AP. The **Usage Traffic** parameter shows the total amount of data transferred during the uptime duration of the AP. The **Throughput** value is the cumulative value of number of bytes (during the past 90 seconds) divided by the number of seconds (90 seconds).

To export the values, click and save the excel sheet to your system.

Click to remove this widget from the dashboard.

Operating Systems

You can see the operating system running in the connected clients. This list is sorted according to the number of clients of each OS type.

Applications

You can see the doughnut graph presenting the application with its usage and throughput. This widget gives you the ability to clear the current records to start afresh, click on the top right of this widget to clear the records.

To change to list view, click . This view shows details of each application like usage and the throughput values.

To export the values, click and save the excel sheet to your system.

Click to remove this widget from the dashboard.

Clients

You can see the doughnut graph presenting the network usage by each client in percentage. This widget gives you the ability to clear the current records to start afresh, click the on top right of this widget to clear the records.

To change to list view, click . This view shows each client's details like the type of device, data usage, and the throughput values. You can sort the client list by identity, device type, usage, throughput also.

Click the client to open the **Client View** page. The **Client View** page displays the general, the connectivity, the QoS, and the security and policy details.

To export the values, click and save the excel sheet to your system.

Click to remove this widget from the dashboard.

Top WLANs

The doughnut graph shows the top SSIDs based on the number of clients and usage. The list view displays the SSIDs with the statistics in numbers.

Network Summary

This section contains the following subsections:

Network Summary—Access Points

Selecting this option displays the list of Cisco APs connected to this controller. The page segregates the 2.4 and 5 GHz APs in two tabs. The AP details are shown on this page. Choose any AP to know more details.

The **Access Point View** page shows the general and performance summary of the selected AP. The AP details section provides tabs with information on the clients, RF Troubleshooting with neighboring and rogue APs (2.4 and 5 GHz) found in the surroundings, CleanAir with active interferers and the tool tab to restart the AP.

Note This section does not display access points in monitor mode.

Network Summary—Clients

This section displays the detailed information of clients that are associated with the access points in a list view.

The **Client View** page is displayed when a client is selected. On this page, the client's general details are shown. Click **Connection Score** value to see the connection quality between the client and the AP.

There are two info graphic representations on the **Client View** page.

- The first infographic shows the connection stage of the client.
- The second infographic shows the connectivity roadmap between the controller and the client. It also shows the types of connection and the path that is used in the network from the controller to the client.

The **Network and QoS** and the **Security Policy** dashlets show the status of their respective parameters.

The **Client View** page also offers debugging tools to assess the connectivity from the client with the controller. Tools available are:

- Ping Test—helps to know the connectivity status and the latency between the two systems in a network.

- Connection—shows the connection logs for a client.
- Event Log—records the events and the option to save the logs on to a spreadsheet.
- Packet Capture—select from the various options to get precise information about the flow of packets to help resolve issues.

Note Cisco Wave 2 APs do not support Packet Capture feature.

Rogues

This section contains the following subsections:

Rogue Access Points

This page displays the rogue access points grouped under 2.4-GHz and 5-GHz networks in the following groups.

- Unclassified
- Friendly
- Malicious
- Custom

Choose the rogue AP from the list to display the **Rogue AP Detail** page. This page displays the connection details and the APs that are detected this rogue AP. To view the AP details choose the AP to get the **Access Point View** page.

Rogue Clients

This page displays the list of clients that are yet to be identified. Choose the rogue client for more details.

The **Rogue Client View** page shows the connection information, the state and the APs that detected this client. To view the AP details choose the AP to get the **Access Point View** page.

Interferers

This page displays the list of interfering devices that are detected in the 2.4-GHz and 5-GHz spectrum. Use the filters available for each category to view a customized list which can help identify the interfering devices and take corrective actions to improve the air quality.

Wireless Dashboard

This page shows a graphical overview of various selectable widgets and their performances over 2.4 GHz and 5–GHz networks.

AP Performance

This page displays the performance values of the Cisco APs graphically. These parameters are selectable widgets to create a custom AP performance dashboard.

Client Performance

This page graphically displays the client parameters, which range from signal strength to state of association and other selectable widgets.

Best Practices

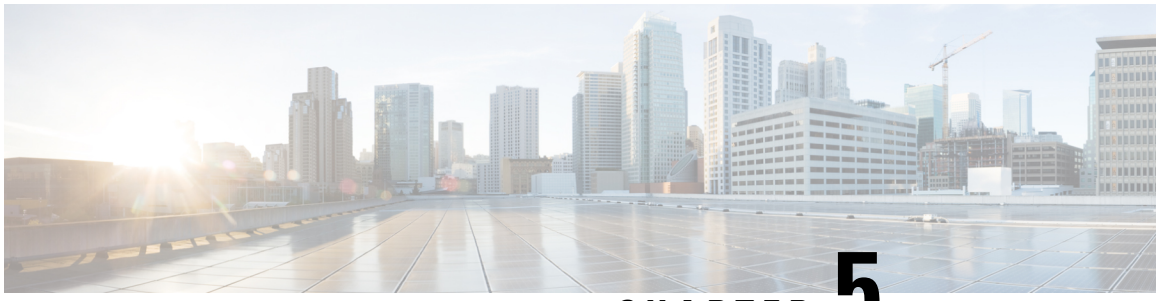
The **Best Practices** page offers current compliance assessment and available categories of best practices. The Best Practices are enabled by default if you have used the Cisco WLAN Express Setup to configure the controller.

Note The Best Practices are not enabled through CLI setup wizard or image upgrades.

Every parameter under each category has a + icon which provides an expert recommendation and the option **Learn More** gives detailed information on that parameter. Each parameter may have one or more of the following options.

- Fix it Now—sets the parameter to the Cisco recommended settings.
- Restore Default—resets the Best Practice parameter configurations to default values.
- Manual Configuration—opens the advanced view to configure the parameter.
- Ignore—removes the parameter from the best practice list.

  The ignored parameters are grouped under the icon. This icon is found at the top right corner of the Best Practices page. This icon displays the **Add Best Practice** window; click the parameter that you want to add to the main page.
- Detailed—opens a new window with WLAN profile settings and option to manual configuration.



CHAPTER 5

Managing Licenses

- Cisco Wireless Controller Licensing, on page 53
- Cisco Smart Software Licensing, on page 63
- Right to Use Licensing, on page 67
- Rehosting Licenses, on page 69
- License Agent, on page 72
- Call-Home, on page 74
- Retrieving the Unique Device Identifier on Controllers and Access Points, on page 77

Cisco Wireless Controller Licensing

For information about licensing in various Cisco Wireless Controller platforms, see the respective platform's datasheet:

- Cisco 3504 Wireless Controller

  https://www.cisco.com/c/en/us/products/collateral/wireless/3504-wireless-controller/datasheet-c78-738484.html

- Cisco 5520 Wireless Controller

  https://www.cisco.com/c/en/us/products/collateral/wireless/5520-wireless-controller/datasheet-c78-734257.html

- Cisco 8540 Wireless Controller

  https://www.cisco.com/c/en/us/products/collateral/wireless/8540-wireless-controller/datasheet-c78-734258.html

- Cisco Virtual Wireless Controller

  https://www.cisco.com/c/en/us/products/collateral/wireless/virtual-wireless-controller/data_sheet_c78-714543.html

Related Information

- Cisco Software Central

  https://software.cisco.com

- Licensing on 3504, 5520 and 8540 Wireless LAN Controllers: RTU FAQ

https://www.cisco.com/c/en/us/support/docs/wireless/3504-wireless-controller/214106-licensing-on-3504-5520-and-8540-wireles.html

- Special Notes for Licensed Data Payload Encryption on Cisco Wireless Controllers

  https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/ldpe/ldpe-on-wlc.html

- Smart Licensing Deployment Guide

  https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html

Installing a License

Installing a License (GUI)

Procedure

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 controller.

Installing a License (CLI)

Procedure

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 controller.

Viewing Licenses

Viewing Licenses (GUI)

Procedure

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.

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:

Note The maximum number of APs supported refers to the maximum number of APs supported by the controller. It is not linked to the installed licenses.

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
```

- 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.

Procedure

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)

Procedure

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)

Procedure

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.

Cisco Smart Software Licensing

Cisco started the initiative of simplifying customer license management by building a Cisco Smart Software Manager (SSM) portal. It helps the customers understand what licenses they have purchased and what licenses they are using. Various other Cisco products are already Smart Enabled and with the introduction of this release, Smart Licensing will now be available on the following platforms:

- Cisco 5520 Wireless Controller (AIR-CT5520-K9)
- Cisco 8540 Wireless Controller (AIR-CT8540-K9)
- Cisco vWLC (L-AIR-CTVM-5-K9)
- Cisco 3504 Wireless Controller (AIR-CT3504-K9)

You have to register for your own Smart Account, which is a one-time activity. Using the Smart Account you can activate, monitor usage, and track the purchased licenses. To know more about creating the Cisco Smart Account, see Smart Account Quick Reference Guide.

Note For information about migrating from RTU Licensing mechanism to Smart Licensing mechanism, consult Cisco Technical Assistance Center.

Additional Reference

Smart Licensing Deployment Guide—https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html

Related Topics

Information About Rehosting Licenses, on page 69

Guidelines and Restrictions for Using Cisco Smart Software Licensing

- We recommend that you perform the following procedure if you have the Cisco Smart License enabled and the controller is registered on Cisco Smart Account.

  You must perform this task before you upgrade the controller's boot image.

  1. Deregister the controller running the old build from the Cisco Smart Software Manager (CSSM).
  2. Upgrade the controller with new boot image.
  3. Reregister the upgraded controller with new build on Cisco Smart Software Manager (CSSM).

- If you try to deregister the controller when CSSM is not reachable, the controller is deregistered internally. This results in a stale entry in CSSM. The workaround for this issue is that you must remove the stale entry from CSSM manually.
- Token-ID that is generated for Cisco 5520 or 8450 Wireless Controller cannot be used with Cisco vWLC.
- Call-Home supports only HTTP and HTTPS mode of communication.
- Call-Home does not support email mode of communication.
- After the switchover to Smart Licensing mechanism, some of the parameter reports, for example: runtime statistics will not be cumulative reports.
- To create a new profile and avoid Smart Licensing transport mode from being disabled, ensure that you disable the active profile using the **config call-home tac-profile status disable** command before you create the new profile.

Note You can have a maximum of two profiles and only one active profile at any time. You can configure only one profile each for Smart Licensing messages and Call-Home events.

- Do not use a non-tac profile using call-home data reporting format as this will disable Smart Licensing service.
- There might be a difference in the timestamps when the controller is in a different time zone, as the controller is set to local time zone time, whereas the Smart License server is set to UTC time.
- In a Smart License active High Availability pair, when the primary controller stops functioning, and the standby controller takes over as the new primary, and initiates a reboot. After reboot, the device losses its registration information. Manually registering the device with the Cisco Smart License Manager or rebooting and re-pairing the primary and stand-by devices helps resolve this issue.
- On a Smart License active High Availability pair, any attempt to deregister before the switch over to active secondary from active primary is complete, and the renew message is sent, the deregistration process might fail.
- In a Smart License active High Availability pair, the standby device displays evaluation authorization state, this parameter gets updated to display the correct values after the switchover is complete and the controller is the active controller.
- To free the license on the server in a situation where the license mechanism is changed to Right To Use (RTU) from Smart Licensing, it is mandatory to manually deregister the device.

Related Topics

Information About Rehosting Licenses, on page 69

Configuring Cisco Smart Software Licensing (GUI)

Procedure

Step 1 To activate Smart Licensing mechanism, follow these steps:

a) Choose **Management** > **Software Activation** > **License Type** to open the **Smart-License** page.
b) From the **Licensing Type** drop-down list, choose **Smart-Licensing** option.
c) Enter the DNS Server IP address in the **DNS Server IP address** field.
d) Click **Apply**
e) Reboot the controller.

Step 2 To register a device, follow these steps:

a) Choose **Management** > **Smart-License** > **Device Registration** to open the **Device Registration** page.
b) From the **Action** drop-down list choose **Registration** to register a new device.
c) Enter the device **Token-ID**.
d) Click **Apply**.

Step 3 To de-register a device, follow these steps:

a) Choose **Management** > **Smart-License** > **Device Registration** to open the **Device Registration** page.
b) From the **Action** drop-down list choose **De-registration** to remove a registered device.
c) Click **Apply**.

Step 4 To view the current Smart Licensing parameters, follow these steps:

a) Choose **Management** > **Smart-License** > **Status** to open the **Status** page.
b) To view the **Smart-Licensing Parameters**, choose from the following options in the drop-down list:

- **Status**
- **Summary**
- **All**
- **UDI**
- **Usage**
- **Tech-Support**

Related Topics

Information About Rehosting Licenses, on page 69

Configuring the Cisco Smart Software Licensing on Controller (CLI)

Procedure

Step 1 Enable Cisco Smart Software Licensing by entering the following command:

config licensing smart-license dns-server *ip-address*

Note
Device reboot is required to activate the chosen license mechanism.

Step 2 To register or deregister a device and to retain the state of device registration after device reboots enter the following command:

license smart {**register** | **deregister**} *idtoken*

Step 3 View the license status by entering the following command:

show license {**status** | **summary** | **udi** | **all**}

Note
The Smart License service runs an asynchronous sync with the controller. Hence, until the sync is completed, on executing the show command the local controller information is displayed and when the show command invoked the next time, the updated values from the Smart License is displayed.

Step 4 Clear the Cisco Smart Software Licensing statistics by entering the following command:

clear stats smart-lic

Related Topics
Information About Rehosting Licenses, on page 69

Updating DNS IP Address for Cisco Smart Software Licensing (CLI)

In a situation where you need to update the DNS IP address for Smart Licensing, remove the device from the Cisco Smart Software Manager.

Procedure

Step 1 Reset the Smart Licensing DNS IP address by entering this command:

test smart-lic reset-all

Note
In a High Availability setup, execute the command in the active device first and then on the standby device.

Step 2 Reregister the device in Cisco SSM by entering this command:

license smart register *token-id* **force**

Step 3 Save the configuration and reboot the controller

Related Topics
Information About Rehosting Licenses, on page 69

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 3504 Wireless Controller
- Cisco 5520 Wireless Controller
- Cisco 8540 Wireless Controller
- 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 point 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.

Note Licenses embedded in the controller at the time of shipment are 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 controllers, when you enable High Availability, 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.

Configuring Right to Use Licensing (GUI)

Procedure

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, controller 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.

Related Topics

Cisco Smart Software Licensing, on page 63
Guidelines and Restrictions for Using Cisco Smart Software Licensing, on page 63
Configuring Cisco Smart Software Licensing (GUI), on page 65
Configuring the Cisco Smart Software Licensing on Controller (CLI), on page 65
Updating DNS IP Address for Cisco Smart Software Licensing (CLI), on page 66

Rehosting a License

Rehosting a License (GUI)

Procedure

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** field, 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**.

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 field.
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 field 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** field, 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** field, 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 field 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 license appears with high priority. Lower the priority of the evaluation license so that the permanent license is in "In Use" status.

Rehosting a License (CLI)

Procedure

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 http://slexui.cloudapps.cisco.com/SWIFT/LicensingUI. 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 http://slexui.cloudapps.cisco.com/SWIFT/LicensingUI.
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 license appears with High priority. Lower the priority of the evaluation license so that the permanent license is in "In Use" status.

License Agent

If your network contains various Cisco-licensed devices, you might want to consider using the Cisco License Manager (CLM) to manage all of the licenses using a single application. CLM is a secure client/server application that manages Cisco software licenses network wide.

The license agent is an interface module that runs on the controller and mediates between CLM and the controller's licensing infrastructure. CLM can communicate with the controller using various channels, such as HTTP, Telnet, and so on. If you want to use HTTP as the communication method, you must enable the license agent on the controller.

The license agent receives requests from CLM and translates them into license commands. It also sends notifications to CLM. It uses XML messages over HTTP or HTTPS to receive the requests and send the notifications. For example, CLM sends a **license install** command, and the agent notifies CLM after the license expires.

This section contains the following subsections:

Configuring the License Agent (GUI)

Procedure

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

Step 2 Select the **Enable Default Authentication** check box to enable the license agent, or leave it unselected to disable this feature. The default value is unselected.

Step 3 In the Maximum Number of Sessions text box, enter the maximum number of sessions for the license agent. The valid range is 1 to 25 sessions (inclusive).

Step 4 Configure the license agent to listen for requests from the CLM as follows:

a) Select the **Enable Listener** check box to enable the license agent to receive license requests from the CLM, or unselect this check box to disable this feature. The default value is unselected.

b) In the Listener Message Processing URL text box, enter the URL where the license agent receives license requests (for example, http://209.165.201.30/licenseAgent/custom). The Protocol parameter indicates whether the URL requires HTTP or HTTPS.

Note
You can specify the protocol to use on the HTTP Configuration page.

c) Select the **Enable Authentication for Listener** check box to enable authentication for the license agent when it is receiving license requests, or unselect this check box to disable this feature. The default value is unselected.

d) In the Max HTTP Message Size text box, enter the maximum size for license requests. The valid range is 0 to 9999 bytes, and the default value is 0.

Step 5 Configure the license agent to send license notifications to the CLM as follows:

a) Select the **Enable Notification** check box to enable the license agent to send license notifications to the CLM, or unselect this check box to disable this feature. The default value is unselected.

b) In the URL to Send the Notifications text box, enter the URL where the license agent sends the notifications (for example, http://www.cisco.com/license/notify).

c) In the User Name text box, enter the username required in order to view the notification messages at this URL.

d) In the Password and Confirm Password text boxes, enter the password required in order to view the notification messages at this URL.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your changes.

Configuring the License Agent (CLI)

Procedure

Step 1 Enable the license agent by entering one of these commands:

- **config license agent default authenticate**—Enables the license agent default listener with authentication.
- **config license agent default authenticate none**—Enables the license agent default listener without authentication.

Note
To disable the license agent default listener, enter the **config license agent default disable command**. The default value is disabled.

Step 2 Specify the maximum number of sessions for the license agent by entering this command:

config license agent max-sessions *sessions*

The valid range for the *sessions* parameter is 1 to 25 (inclusive), and the default value is 9.

Step 3 Enable the license agent to receive license requests from the CLM and to specify the URL where the license agent receives the requests by entering this command:

config license agent listener http {**plaintext** | **encrypt**} *url* **authenticate** [**none**] [**max-message** *size*] [**acl** *acl*]

The valid range for the *size* parameter is 0 to 65535 bytes, and the default value is 0.

Note
To prevent the license agent from receiving license requests from the CLM, enter the **config license agent listener http disable command**. The default value is disabled.

Step 4 Configure the license agent to send license notifications to the CLM and to specify the URL where the license agent sends the notifications by entering this command:

config license agent notify *url username password*

Note
To prevent the license agent from sending license notifications to the CLM, enter the **config license agent notify disable** *username password command.* The default value is disabled.

Step 5 Enter the **save config** command to save your changes.

Step 6 See statistics for the license agent's counters or sessions by entering this command:

show license agent {**counters** | **sessions**}

Information similar to the following appears for the **show license agent counters** command:

```
License Agent Counters
Request Messages Received:10: Messages with Errors:1
Request Operations Received:9: Operations with Errors:0
Notification Messages Sent:12: Transmission Errors:0: Soap Errors:0
```

Information similar to the following appears for the **show license agent sessions** command:

```
License Agent Sessions: 1 open, maximum is 9
```

Note
To clear the license agent's counter or session statistics, enter the **clear license agent** {**counters** | **sessions**} command.

Call-Home

You can create reporting profiles of your choice for the Smart Licensing messages and Call-Home events. Call-Home reports Smart Licensing messages that are based on the active profile. At any time, only one profile can be active. The messages use XML format. Therefore, ensure that you choose XML format for all the profiles that you create.

Note By default call-home TAC profile is enabled. However if you disable the TAC profile and try to register or deregister Smart Licensing service, the profile status changes to active (enabled) dynamically.

This section contains the following subsections:

Configuring Call-Home (GUI)

Procedure

Step 1 To enable or disable the Call-Home reporting function, follow the steps:

a) Choose **Management** > **Smart-License** > **Call-home** > **configuration** to open the **Call-Home** > **Configuration** page.

b) From the **Events** drop-down list choose from the following options in the drop-down list:

- **Enabled**–enables Call-Home reporting
- **Disabled**–disables Call-Home reporting

c) Click **Apply**

Step 2 To set the Data privacy level, follow the steps:

a) From the **Reporting Data-privacy-level** drop-down list choose from the following options in the drop-down list:

- **normal**–scrubs normal level commands
- **high**–scrubs all normal level commands, IP domain name and IP address commands

b) Click **Apply**

Step 3 Enter the hostname in the **Reporting Hostname** text box.

Step 4 To configure the http-proxy settings, following the steps:

a) In the **HTTP-proxy** field, enter the **IP-Address** and **port** number

b) Click **Apply**

Step 5 To enable or disable the TAC Profile Status, follow the steps:

a) From the **TAC Profile Status** drop-down list, choose from the following options in the drop-down list:

- **Enabled**–enables the TAC profile
- **Disabled**–disables the TAC profile

b) Click **Apply**

Step 6 Enter the email address in the **Contact person's email address** text box.

Step 7 To create a new profile, follow the steps:

a) Enter the name for the new profile in the **Name** text box.

b) From the **Status** drop-down list choose from the following options in the drop-down list:

- **Enabled**–activates the profile
- **Disabled**–deactivates the profile

c) From the **Module** drop-down list, choose from the following options in the drop-down list:

- **sm-license-data**–smart license data
- **all**–combines smart license and call-home data
- **call-home-data**–call-home data

d) From the **Reporting Format** drop-down list, choose from the following options in the drop-down list:

- **short-text**–data reporting in short-text format
- **long-text**–data reporting in long-text format
- **xml**–call-data reporting in xml format

Note
The messages use XML format, hence, ensure XML message format is chosen for all profiles created.

e) The current default is **xml** format.
f) Enter the url in the **url** text box.
g) Click **Add**

Step 8 To update an existing profile, follow the steps:

a) Place the mouse cursor over the **blue down arrow icon** in front of the Profile to edit.
b) Choose **update** from the drop-down list which appears.
c) Update the fields as required from the options available:

- **Status**
- **Module**
- **Url**

d) Click **Apply**

Step 9 To delete a profile, follow the steps:

a) Place the mouse cursor over the **blue down arrow icon** in front of the Profile to edit.
b) Choose **delete** from the drop-down list which appears.

Configuring Call-Home Parameters (CLI)

Configure Call-Home parameters by entering the following commands:

Procedure

Step 1 Enable or disable Call-Home reporting by entering the following command:

config call-home events {**enable** | **disable**}

The default value is enable.

Step 2 Create a new profile or update an existing profile by entering the following command:

config call-home profile {**create** | **update**} *profile-name* {**sm-license-data** | **all** | **call-home-data**} **XML** *url*

Note
Currently, only XML format is supported. Hence, when call-home-data profile option is selected, choose XML format from the drop-down menu.

Step 3 Delete an existing profile by entering the following command:

config call-home profile delete *profile-name*

Step 4 Configure the proxy settings by adding the IP address and port number by entering the following command:

config call-home http-proxy ipaddr *ip-address* **port** *port*

Step 5 Reset the proxy settings by entering the following command:

config call-home http-proxy ipaddr 0.0.0.0

Step 6 Enable user data privacy by entering the following command:

config call-home reporting data-privacy-level {**normal** | **high**} **hostname** *host-name*

Step 7 Enable or disable the user profile by entering the following command:

config call-home profile status {**enable** | **disable**}

Step 8 Configure the contact email address by entering the following command:

config call-home contact-email-addr *e-mail address*

Step 9 Enable or disable the status of the TAC profile by entering the following command:

config call-home tac-profile status {**enable** | **disable**}

The default value is enable.

Step 10 View the Call-Home settings by entering the following command:

config call-home summary

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)

Procedure

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.

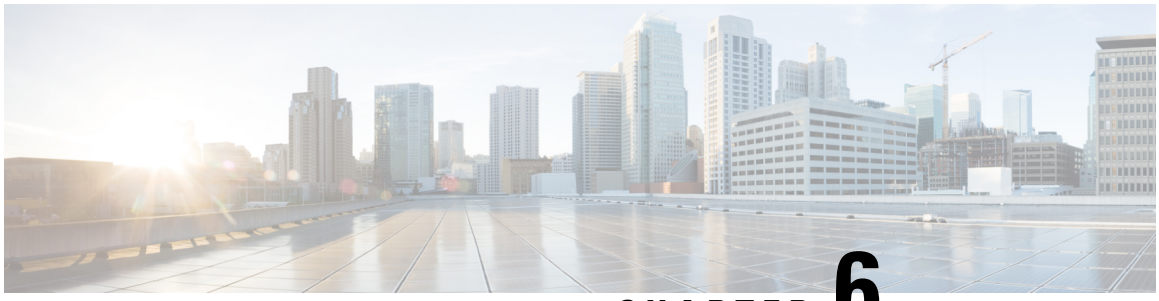
This page shows the inventory information for the access point.

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 6

Managing Software

- Upgrading the Controller Software, on page 79
- Guidelines and Restrictions for Upgrading Controller Software, on page 79
- Upgrading Controller Software (GUI), on page 81
- Upgrading Controller Software (CLI), on page 83
- Predownloading an Image to an Access Point, on page 85
- Bootloader and Recovery Image, on page 90

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, the software image could be corrupted. 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.

Guidelines and Restrictions for Upgrading Controller Software

The following are some of the general guidelines and 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, see 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, see the corresponding release notes for any caveats, considerations, or possible interim upgrades required to upgrade your controller to the desired release of software.
- For customers with Cisco Catalyst 9117 Series APs in their network: Due to an increase in the Cisco controller image size, the Cisco controller software images are split into two images:

- Base Install image, which includes the Cisco controller image and a subset of AP images
- Supplementary AP Bundle image, which includes AP9117 images that are excluded from the Base Install image

Note Download and install the Supplementary AP Bundle image only if you are using the Cisco Catalyst 9117 AP.

- We recommend that you have a backup of your configuration in an external repository before any software upgrade activity.
- Ensure that the configuration file that you back up does not contain < or > special character. If either of the special characters is present, then the download of the backed up configuration file fails.
- 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 section.
- Cisco AireOS 3504 Controller: If the controller has been running for more than 450 days, ensure that you free up the flash memory before downloading the software image to the controller. For more information, see CSCwh98302.

Related Topics

Predownloading an Image to an Access Point, on page 85

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.

Procedure

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.

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** field, 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** field and the amount of time (in seconds) that the TFTP server attempts to download the software in the **Timeout** field.

Step 10 In the **File Path** field, enter the directory path of the software.

Step 11 In the **File Name** field, 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** 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 13 Click **Download** to download the software to the controller. A message is displayed indicating the status of the download.

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 If you have disabled the 802.11 networks, reenable them.

Step 20 To verify the controller software version, choose **Monitor** on the controller GUI and see **Software Version** in the Controller Summary area.

Related Topics

Predownloading an Image to Access Points—Global Configuration (GUI), on page 88

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.

Procedure

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.

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 If you have disabled the 802.11 networks in Step 6, reenable them by entering this command:

config 802.11{a | b} enable network

Step 14 To verify the controller software that is installed, enter the **show sysinfo** command and see Product Version.

Step 15 (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.'

Related Topics

Predownloading an Image to Access Points (CLI), on page 88

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 5520 Wireless Controller	1000
Cisco 8540 Wireless Controller	1000
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
2700(I/E)	16 MB
1700(I/E)	16 MB

Note

- The required flash memory can vary based on the radio type and the number of antennas used.
- 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, 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.

Related Topics

Guidelines and Restrictions for Upgrading Controller Software, on page 79
FlexConnect AP Image Upgrades, on page 1213

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.

Related Topics

FlexConnect AP Image Upgrades, on page 1213

Guidelines and Restrictions for Predownloading an Image to an Access Point

- The maximum number of concurrent predownloads is limited to half the number of concurrent normal image downloads. This limitation allows new access points to join the controller during image downloading.
- If you reach the predownload limit, then the access points that cannot get an image sleep for a time between 180 to 600 seconds and then reattempt the predownload.
- 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.
- 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.
```

- 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.

Procedure

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**.

Related Topics

Upgrading Controller Software (GUI), on page 81

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.

Procedure

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.
- 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.
```

Related Topics

Upgrading Controller Software (CLI), on page 83

Bootloader and Recovery Image

The controller, by default, maintains two software images: a primary image and a backup image. The primary image is the active image used by the controller and the backup image is used as a backup for the primary (active) image.

The controller bootloader (ppcboot) stores a copy of the primary (active) image and the backup image. If the primary image is corrupted, you must use the bootloader to boot with the backup image.

You can change the active image using either of the following two methods:

- Assuming that the controller has a valid backup image, reboot the controller. During the boot process on the controller, press **Esc** key to see additional options. You are prompted to choose an option from the following:

  1. Run primary image
  2. Run backup image
  3. Manually upgrade primary image
  4. Change active boot image
  5. Clear configuration

  Choose *Option 4: Change active boot image* from the boot menu to set the backup image as the active boot image. The controller, when rebooted, boots with the new active image.

- You can also manually change the active booti image of the controller using the **config boot** {**primary** | **backup**} command.

  Each controller can boot off the primary, previously loaded OS image or boot off the backup image, an OS image that was loaded earlier. To change the controller boot option, use the **config boot** command. By default, the primary image on the controller is chosen as the active image.

Note To properly use the bootloader menu, you must have a console connection.

Configuring Boot Order (GUI)

Procedure

Step 1 Choose **Commands** > **Config Boot** to navigate to the **Config Boot Image** page, which displays the primary and backup images presently available on the controller and also indicates the current image in use.

Step 2 From the **Image** drop-down list, choose the image to be used as the active image.

Step 3 Save the configuration and reboot the controller.

- The controller, when rebooted, boots with the image that you chose.
- When you upgrade the controller with the new image, the controller automatically writes the new image as the primary image and the previously existing primary image is written over the backup image.

Note The previously existing backup image will be lost.

- On the controller GUI, to see the active image that the controller is currently using, choose **Monitor** > **Summary** to navigate to the **Summary** page and see the **Software Version** field.

  On the controller CLI, use the **show boot** command to view the primary and backup image present on the controller.

Recovering an Access Point Using TFTP

The recovery image provides a backup image that can be used if an AP power-cycles during an image upgrade. The best way to avoid the need for AP recovery is to prevent an AP from power-cycling during a system upgrade. If a power-cycle occurs during an upgrade to an oversized AP image, you can recover the AP using the following TFTP recovery procedure.

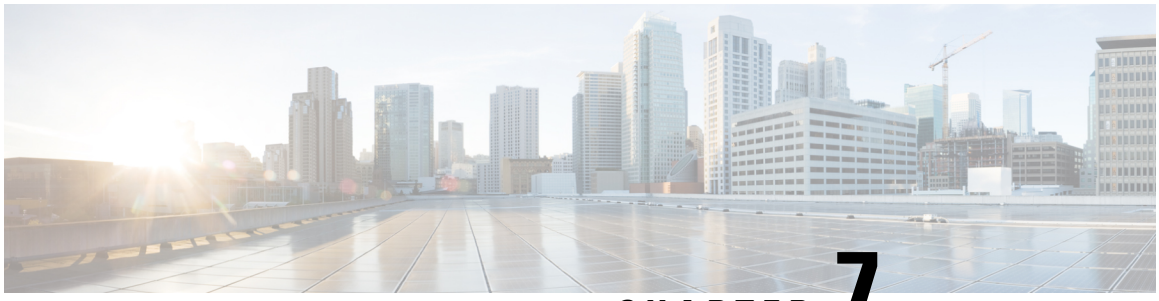
Note IPv6 is not supported in AP recovery images.

Procedure

Step 1 Download the required recovery image from Cisco.com 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 can remove the TFTP server.



CHAPTER 7

Managing Configuration

- Resetting the Controller to Default Settings, on page 93
- Saving Configurations, on page 94
- Editing Configuration Files, on page 94
- Clearing the Controller Configuration, on page 96
- Restoring Passwords, on page 96
- Rebooting the Controller, on page 97
- Transferring Files to and from a Controller, on page 97

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)

Procedure

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)

Procedure

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.

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.

Procedure

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

Related Topics

Uploading Configuration Files, on page 98
Downloading Configuration Files, on page 100

Clearing the Controller Configuration

Procedure

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.

Restoring Passwords

Before you begin

Ensure that you are accessing the controller CLI through the console port.

Procedure

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.

Rebooting 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 the **reset system** command. At the confirmation prompt, press **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.

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:

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.

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.

Related Topics

Editing Configuration Files, on page 94

Uploading the Configuration Files (GUI)

Procedure

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**

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)

Procedure

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.

Related Topics

Editing Configuration Files, on page 94

Downloading the Configuration Files (GUI)

Procedure

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**

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.

Procedure

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.

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)

Procedure

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**

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 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 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)

Procedure

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)

Procedure

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.

Uploading Diagnostic Support Bundle

Some commonly collected diagnostic information of various types can be made available in a single bundle that you can upload from controller. The diagnostic information that you can include in the bundle are core files, crash files, **show run-config** and **config** commands, msglog, and traplog.

Uploading Diagnostic Support Bundle (GUI)

Procedure

Step 1 Choose **Commands** > **Upload File** to open the **Upload File from Controller** page.

Step 2 From the **File Type** drop-down list, choose **Support Bundle**.

Step 3 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP**

Step 4 In the **IP Address (IPv4/IPv6)** field, enter the IPv4/IPv6 address of the server.

Step 5 In the **File Path** field, enter the directory path of the bundle.

Step 6 In the **File Name** field, enter the name of the bundle file.

Step 7 If you are using an FTP or SFTP server, follow these steps:

a) In the **Server Login Username** field, enter the username to log into the server.
b) In the **Server Login Password** field, enter the password to log into the server.
c) In the **Server Port Number** field, enter the port number on the server through which the upload occurs. The default value is 22.

Step 8 Click **Upload** to upload the diagnostic bundle from the controller.

Uploading Diagnostic Support Bundle (CLI)

Procedure

Step 1 Log on to the controller CLI.

Step 2 Specify the transfer mode used to upload the bundle file by entering this command:

transfer upload mode {**tftp** | **ftp** | **sftp**}

Step 3 Upload the diagnostic support bundle by entering this command:

transfer upload datatype support-bundle

Step 4 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 5 Specify the directory path of the bundle file by entering this command:

transfer upload path *server-path-to-file*

Step 6 Specify the name of the bundle file to be uploaded by entering this command:

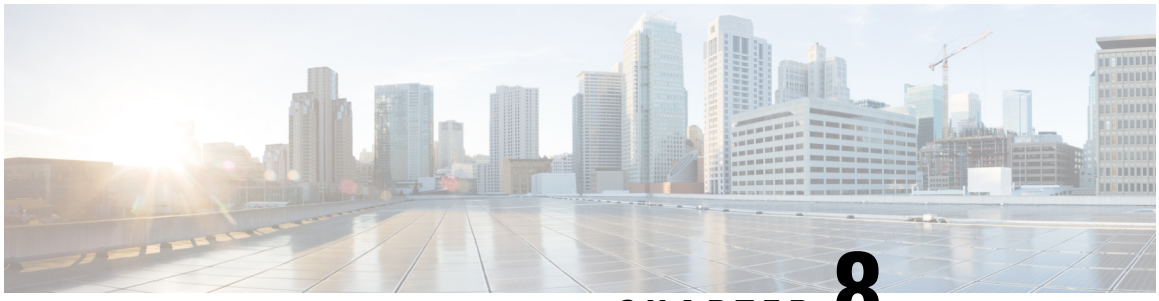
transfer upload filename *file-name*

Step 7 If you are using an FTP or SFTP 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 22.

Step 8 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.



CHAPTER 8

Network Time Protocol Setup

- Authentication for the Controller and NTP/SNTP Server, on page 107
- Configuring the NTP/SNTP Server to Obtain the Date and Time (GUI), on page 108
- Configuring the NTP/SNTP Server to Obtain the Date and Time (CLI), on page 108
- Configuring NTPv4 Keys for Authentication (GUI), on page 109

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.
- As a part of the federal certification requirements, controller supports NTPv4 protocol which is a standard Open Source Code.
- Controllers support both the versions—NTPv3 and NTPv4 versions. However you can use either one of the two versions and not both at the same time.
- NTPv4 supports both IPv4 and IPv6 servers, and supports SHA1 authentication for NTP messages.

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

Procedure

Step 1 Choose **Controller** > **NTP** > **Server** to open the **NTP Severs** page.

Step 2 From the **NTP Version** drop-down list, choose 4.

Step 3 Click **Apply**.

Step 4 Click **New** to add a new NTP/SNTP Server.

Step 5 (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 6 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 7 Enable or disable the NTP/SNTP Authentication.

Step 8 If you enable the NTP/SNTP Authentication, enter the Key Index.

Step 9 Click **Apply**.

Step 10 Delete an existing 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 11 Confirm the deletion by clicking on **OK** in the dialog box.

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*

- Configure the NTP version by entering this command:

  config time ntp version *version*

Note When the NTP version changes, the configured servers are deleted.

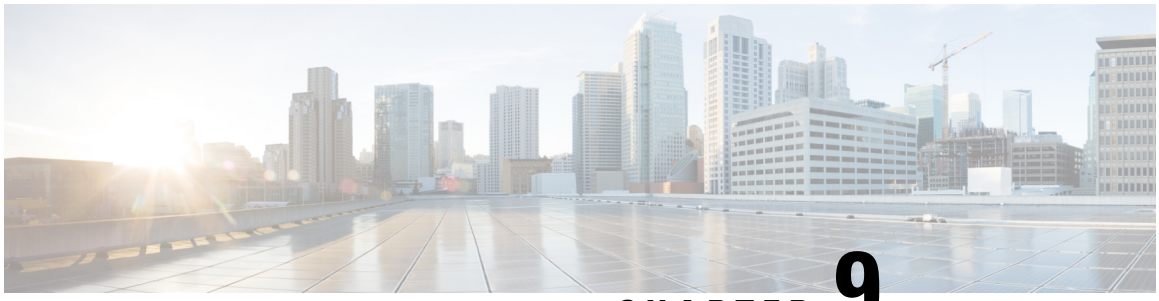
- Configuring the NTP polling interval when using NTP version 4 by entering this command:

  config time ntp pollinterval *maxpoll minpoll server-index*

Configuring NTPv4 Keys for Authentication (GUI)

Procedure

Step 1 Choose **Controller** > **NTP** > **Keys** to open the **NTP Key** page.
Step 2 Click **New** to add a new NTP key.
Step 3 Enter the **Key Index** number in the **Key Index** field.
Step 4 From the **Checksum** drop-down list, choose **SHA1**.
Step 5 From the **Key Format** drop-down list, choose **ASCII**.
Step 6 Enter the **Key** in the **Key** field.
Step 7 Click **Apply**.



CHAPTER 9

High Availability

- Information About High Availability, on page 111
- Restrictions for High Availability, on page 115
- Configuring High Availability (GUI), on page 118
- Enabling High Availability (CLI), on page 120
- vWLC and N+1 High Availability, on page 123
- Adding a Hash Key to a Cisco vWLC (GUI), on page 123
- Adding a Hash Key to Cisco vWLC (CLI), on page 124
- Monitoring High Availability Standby Controller, on page 125
- Replacing the Primary Controller in an HA Setup, on page 126

Information About High Availability

High Availability in controllers allows you to reduce the downtime of the wireless networks that could occur due to failover of controllers.

A 1:1 (Active:Standby-Hot) stateful switchover of access points and clients is supported (HA SSO). In a High Availability architecture, one controller is configured as the primary controller and another controller as the secondary controller.

After you enable High Availability, 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 High Availability, 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

In the Release 8.0 and later releases, the output of the **show ap join stats summary** command displays the status of the access points based on whether the access point joined the controller or it was synchronized from Active controller. One of the following statuses is displayed:

- Synched—The access point joined the controller before the SSO.
- Connected—The access point joined the controller after the SSO.
- Joined—The access point rejoined the controller, or a new AP has joined the controller after the SSO.

In Release 8.0 and later, the output of the **show redundancy summary** command displays the bulk synchronization status of access points and clients after the pair-up of active and standby controllers occurs. The values are:

- Pending— Indicates that synchronization of access points and the corresponding clients details from the active to standby controller is yet to begin.
- In-progress— Indicates that synchronization of access points and the corresponding clients details from the active to standby controller has begun and synchronization is in progress.
- Complete—Indicates that synchronization is complete and the standby controller is ready for a switchover to resume the services of the active controller.

From release 8.0 and later, in a High Availability scenario, the sleeping timer is synchronized between active and standby.

ACL and NAT IP configurations are synchronized to the High Availability standby controller when these parameters are configured before High Availability 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.
- We recommend that you disable High Availability and add license in Cisco 5520and 8540 controllers (RTU based). However, it is not mandatory to disable High Availability as AP licenses added in Primary controller will be inherited to Secondary controller.
- 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 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 a High Availability setup. This occurs if mobility HA MAC field is more than 128.

- When High Availability 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.

- You must ensure that the maximum transmission unit (MTU) on RMI port is 1500 bytes or higher before you enable high availability.
- When High Availability is enabled, ensure that you do not use the backup image. If this image is used, the High Availability 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.
  - 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 a High Availability 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.
- To enable an access point to maintain controlled quality of service (QoS) for voice and video parameters, all the bandwidth-based or static call admission control (CAC) parameters are synchronized from active to standby when a switchover occurs.
- The standby controller does not reboot; instead enters the maintenance mode when unable to connect to the default gateway using the redundant port. Once the controller reconnects to the default gateway, the standby controller reboots and the High Availability pair with the active controller is initiated. However, the active controller still reboots before entering the maintenance mode.
- The following are supported from Release 8.0:
  - Static CAC synchronization—To maintain controlled Quality-of-Service (QoS) for voice and video parameters, all the bandwidth-based or static CAC parameters services are readily available for clients when a switchover occurs.
  - Internal DHCP server—To serve wireless clients of the controller, the internal DHCP server data is synchronized from the active controller to the standby controller. All the assigned IP addresses remain valid, and IP address assignation continues when the role changes from active to standby occurs.
  - Enhanced debugging and serviceability—All the debugging and serviceability services are enhanced for users.
- The physical connectivity or topology of the access points on the switch are not synchronized from the active to the standby controller. The standby controller learns the details only when the synchronization is complete. Hence, you must execute the **show ap cdp neighbors all** command only after synchronization is complete, and only when the standby becomes the then active controller.
- To enable access points to join the HA SKU secondary controller that has been reset to factory defaults, you must:
  - Configure the HA SKU controller as secondary controller. To do this, you must run the **config redundancy unit secondary** command on the HA SKU controller.
  - Reboot the HA SKU controller after you successfully execute the **config redundancy unit secondary** command.

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.

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.
- You should apply an access list for SSH to the redundancy interface on upper switch, if controller is configured for HA SSO and redundancy management is configured over a dynamic interface. Failure to do so enables the SSH client to connect through the redundancy management interface regardless of the CPU ACL.
- 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.

- 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.
- When you enable both RADIUS profiling and WSA in an SSID, local profiling gets enabled in the same SSID.
- 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.

- When a failover occurs and the standby controller becomes the new active controller, it takes approximately 15–20 minutes to synchronize the database (AP, client, and multicast) between the two controllers. If another failover occurs during this time, the HA structures would not yet be synchronized. Therefore, the APs and clients would have to get reassociated and reauthenticated respectively.
- 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.
- 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

- 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.

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.

Procedure

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 [Optional] To encrypt the link between the HA pair, on the **Global Configuration** page, select **Enabled** from the **Link Encryption** drop-down list

Step 7 Click **Save Configuration**.

Step 8 View the redundancy status of the HA pair by choosing **Monitor > Redundancy > Summary**.

The **Redundancy Summary** window is displayed.

Step 9 View the redundancy status of the HA pair by choosing **Monitor > Redundancy > Detail**.

The **Redundancy Detail** page is displayed.

Step 10 View the redundancy statistics information of the HA pair by choosing **Monitor > Redundancy > Statistics**.

The **Redundancy Statistics** page is displayed.

Step 11 (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)

Procedure

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 High Availability 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 redundancy 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 controller 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.

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 connected 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 (CLI)

Procedure

- 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.
- From Release 8.0.132.0 onwards, mobility MAC configuration is no longer present in the uploaded configuration. Therefore, if you download this configuration file back to the controller, you must add the **config redundancy mobilitymac** *mac_address* command in the config file before download.

- 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

- View information about sleeping clients after a switchover, by entering this command on the then active controller :

  show custom-web sleep-client summary

Troubleshooting Tips for IPsec Encryption for High Availability

Procedure

- If the HA pair does not come up, check the link encryption setting on both controllers.
- Both the controllers must have same link encryption setting.
- Check IPsec status on both controllers to check which link is broken RP or RMI.
- Perform **rping** on both controllers to check if the peer is reachable.
- Check the link encryption status by entering this command:

  show redundancy summary

- Check the IPsec status between the HA pair by entering this command:

  show ipsec status

- Enable IPsec debug messages and reboot the peer secondary controller by entering this command:

  debug ipsec events enable

  This command enables the IPsec debug messages. Reboot the peer secondary controller after enabling this command.

Note The **debug ipsec events enable** will not print logs during next reboot (at bootup).

vWLC and N+1 High Availability

Release 8.4 introduces support for N+1 High Availability (HA) on the Cisco Virtual Wireless Controller (vWLC) platform. For information on how to configure HA, see:

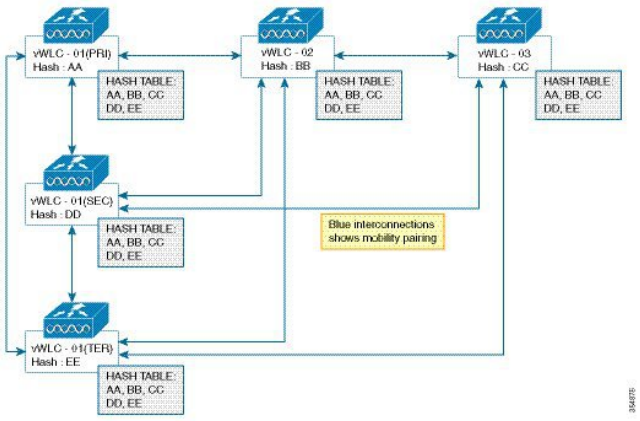
https://www.cisco.com/c/en/us/td/docs/wireless/technology/hi_avail/N1_High_Availability_Deployment_Guide/N1_HA_Overview.html#pgfId-1054644

The Cisco vWLC HA has the following prerequisites:

- The primary, secondary, and tertiary vWLCs should be part of the same mobility group.
- The vWLC in the mobility group should have a uniform set of hash keys to seamlessly move an AP from one vWLC to another. For example, if we have vWLCs, N, in a mobility group, or vWLC, M, and normal controllers (where M is greater than N), then all vWLCs should have the hashes of other vWLCs in the same group.
- For effective connectivity of the APs on all the vWLCs in a mobility group (including vWLC mobility members in N+1 format), the mobility hash table should contain all the vWLC hash keys.

Note A hash table works only when vWLCs are paired as mobility members.

Figure 15: vWLC N+1 in a Mobility Group



Adding a Hash Key to a Cisco vWLC (GUI)

Perform the procedure given below to add hash key to Cisco vWLC.

Before you begin

Create mobility peers before adding a hash key to Cisco vWLC.

Procedure

Step 1 Choose **Controller > Mobility Management > Mobility Groups**.

The **Static Mobility Group Members** window displays the existing members and the hash keys configured for them.

Step 2 Click **New**.

The **Mobility Group Member > New** window is displayed.

Step 3 In the **Member IP Address(Ipv4/Ipv6)** field, enter the member's IP address. In the **Member MAC Address** field, enter the member's MAC address. In the **Group Name** field, enter the group name. In the **Hash** field, enter the hash key.

Step 4 Click **Apply**.

Adding a Hash Key to Cisco vWLC (CLI)

Perform the procedure given below to add a hash key to a Cisco vWLC, using the CLIs.

- Read the hash key.
- Copy the hash key to the other members of the mobility group.
- Verify the mobility hash configuration.

Before you begin

- The hash value should be unique for each vWLC.
- Create mobility peers before adding a hash key to a vWLC.

Procedure

Step 1 **show mobility group member hash**

Example:

```
(Cisco Controller)> show mobility group member hash
```

Reads the existing hash key.

Step 2 **config mobility group member hash** *ipv4-address hash-key*

Example:

```
(Cisco Controller)> config mobility group member hash 9.11.34.55
1f81d80082e9d30312d3b4920be22aed34b93b56
```

Copies the hash to other members in the mobility group.

Step 3 **show mobility group member hash**

Example:

```
(Cisco Controller)> show mobility group member hash
Default Mobility Domain..................... default

 IP Address      Hash Key
-------------------------------------------------------
 9.11.34.55     1f81d80082e9d30312d3b4920be22aed34b93b56
```

Verifies the mobility hash configuration on all the mobility members in the group.

Monitoring High Availability Standby Controller

You can view the status and health information of active and standby controller separately. This section describes the details of getting health information and traps from the standby controller.

The standby controller uses the redundancy management interface for any external communications such as when talking to Syslog, NTP server, TFTP server, and so on. On the standby controller, the management user authentication and accounting is performed on the redundancy management interface. RADIUS or TACACS+ server can be used for user authentication, apart from a local management user account. To support this, the redundancy interface IP address(es) should be added as network device on the RADIUS or TACACS+ server. The authentication request is sent to RADIUS or TACACS+ server over redundancy management interface. Whenever you log on to the standby controller, accounting message is sent to the RADIUS server. The purpose of the accounting message is to log the admin logon events on the standby controller console.

This feature is supported on all controller models supporting HA SSO feature:

- Cisco 8500 Series Controllers
- Cisco 3504 Controllers
- Cisco 5500 Series Controllers

Events and Notifications

- Trap when controller becomes Hot Standby—A trap is reported with time stamp when HA peer becomes Hot Standby and the trap shown below is reported

  "RF notification EventType:37 Reason :HA peer is Hot-Standby...At:..."

  A new trap type is added in CISCO-RF-SUPPLEMENTAL-MIB.my

- Trap when Bulk Sync Complete—After the HA pairing is done and Bulk sync is complete, the following trap is reported:

  "RF notification EventType:36 Reason :Bulk Sync Completed...At:.."

  A new trap type is added in CISCO-RF-SUPPLEMENTAL-MIB.my

- Trap when Standby controller goes down—When the standby peer goes down due to manual reset, crash, memory leak/hang, or moving to maintenance mode, the following trap is reported:

  "RF failure notification ErrorType: 34 Reason :Lost Peer, Moving to Active-No-Peer State!"

On the CLI, you can view the trap by entering the **show traplog** command.

- Syslog notification when Admin login on Standby

  1. Admin login to Standby via SSH generates an event in msglog/syslog. The following is a sample system message:

     ***emWeb: Mar 06 20:34:42.675: #CLI-3-LOGIN_STANDBY: [SS] cli_lvl7.c:4520 [USER@9 name="admin" from="SSH"] user login success on standby controller.**

     You can view this message on the standby controller by entering the **show msglog** command.

  2. Admin login to Standby via console generates an event in msglog/syslog. The following is a sample system message:

     ***emWeb: Mar 06 20:34:42.675: #CLI-3-LOGIN_STANDBY: [SS] cli_lvl7.c:4520 [USER@9 name="admin" from="console"] user login success on standby controller.**

     You can view this message on the standby controller by entering the **show msglog** command.

- Peer Process Statistics—The CPU and Memory statistics of all the threads of the standby controller are synchronized with the active controller every 10 seconds. This information is displayed when you query for the Peer statistics on the active controller.

  Enter these commands on the active controller to view the peer process system, CPU, and memory statistics:

  - **show redundancy peer-system statistics**
  - **show redundancy peer-process cpu**
  - **show redundancy peer-process memory**

  On the GUI, choose **Monitor** > **Redundancy** > **Peer Statistics** to view the peer process system, CPU, and memory statistics.

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:

Procedure

Step 1 Ensure that the new controller and the controller to be replaced are running the same version of the controller software.

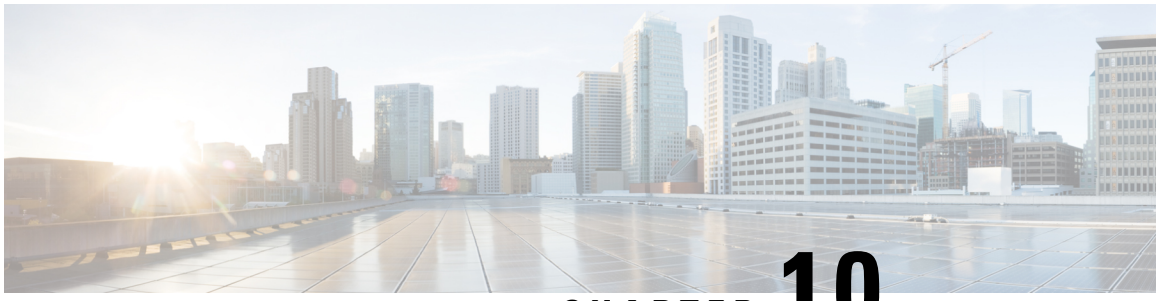
Step 2 Configure the new controller with the same subnet management IP addresses as the controller to replaced.

Step 3 Configure the new controller with HA configuration that includes redundancy management, IP address, and peer primary. Accept the licensing EULA on the primary controller and then enable AP SSO.

Note
If you enable AP SSO without accepting the EULA, the controllers do not synchronize.

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 10

Managing Certificates

- Information about Loading an Externally Generated SSL Certificate, on page 129
- Downloading Device Certificates, on page 131
- Uploading Device Certificates, on page 134
- Downloading CA Certificates, on page 136
- Uploading CA Certificates, on page 138
- Generating a Certificate Signing Request, on page 140
- Downloading Third-Party Certificate, on page 143

Information about 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 Controller—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)

Procedure

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.

Procedure

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

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.

Related Topics

Local EAP, on page 971

Downloading Device Certificates (GUI)

Procedure

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)

Procedure

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

Uploading Device Certificates

Uploading Device Certificates (GUI)

Procedure

Step 1 Choose **Commands** > **Upload File** to open the Upload File from Controller page.

Step 2 From the File Type drop-down list, choose **IPSec Device Certificate**.

Step 3 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP**

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 certificate.

Step 6 In the File Name text box, enter the name of the certificate.

Step 7 If you are using an FTP server, follow these steps (skip this step if you are not using FTP server):

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. For SFTP, the default value is 22.

Step 8 Click **Upload** to upload the CA certificate from the controller. A message appears indicating the status of the upload.

Step 9 After the upload is complete, choose **Commands** > **Reboot** > **Reboot**.

Step 10 If prompted to save your changes, click **Save and Reboot**.

Step 11 Click **OK** to confirm your decision to reboot the controller.

Uploading Device Certificates (CLI)

Procedure

Step 1 Log on to the controller CLI.

Step 2 Specify the type of the file to be uploaded by entering this command:

transfer upload datatype ipsecdevcert

Step 3 Specify the transfer mode used to upload the file by entering this command:

transfer upload mode {**tftp** | **ftp** | **sftp**}

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:

transfer upload serverip *server-ip-address*

Step 5 Specify the directory path of the file by entering this command:

transfer upload path *server-path-to-file*

Step 6 Specify the name of the file to be uploaded by entering this command:

transfer upload filename *filename*

Step 7 If you are using an FTP server, enter these commands (skip this step if you are not using FTP server):

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note
The default value for the port parameter for is 21. For SFTP, the default value is 22.

Step 8 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 9 Reboot the controller by entering the **reset system** command.

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)

Procedure

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)

Procedure

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 CA Certificates

Uploading CA Certificates (GUI)

Procedure

Step 1 Choose **Commands** > **Upload File** to open the Upload File from Controller page.

Step 2 From the File Type drop-down list, choose **IPSec CA Certificate**.

Step 3 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP**

Step 4 In the **IP Address** field, enter the IP address of the server.

Step 5 In the **File Path** field, enter the directory path of the certificate.

Step 6 In the **File Name** field, enter the name of the certificate.

Step 7 (Optional) If you are using an FTP server, follow these steps (skip this step if you are not using FTP server):

a) In the **Server Login Username** field, enter the username to log on to the FTP server.
b) In the **Server Login Password** field, enter the password to log on to 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. For SFTP, the default value is 22.

Step 8 Click **Upload** to upload the CA certificate from the controller. A message appears indicating the status of the upload.

Step 9 If prompted to save your changes, click **Save**.

Uploading CA Certificates (CLI)

Procedure

Step 1 Log on to the controller CLI.

Step 2 Specify the type of the file to be uploaded by entering this command:

transfer upload datatype ipseccacert

Step 3 Specify the transfer mode used to upload the file by entering this command:

transfer upload mode {**tftp** | **ftp** | **sftp**}

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:

transfer upload serverip *server-ip-address*

Step 5 Specify the directory path of the file by entering this command:

transfer upload path *server-path-to-file*

Step 6 Specify the name of the file to be uploaded by entering this command:

transfer upload filename *filename*

Step 7 (Optional) If you are using an FTP server, enter these commands (skip this step if you are not using FTP server):

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note
The default value for the port parameter is 21. For SFTP, the default value is 22.

Step 8 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 9 Reboot the controller by entering the **reset system** command.

Generating a Certificate Signing Request

This section describes how to generate a Certificate Signing Request (CSR) to get a third-party certificate and how to download a chained certificate to the controller. You can generate a CSR using either of the following methods:

- Using OpenSSL
- Using the controller itself

Related Documentation

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

Generating a Certificate Signing Request using OpenSSL

Procedure

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 maximum 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.

Generating a Certificate Signing Request using Cisco Wireless Controller (GUI)

In Release 8.3 or a later release, the more secure option is to use the controller itself to generate the CSR.

If you generate the CSR and do not install the resulting certificate, the controller will be inaccessible over HTTPS upon the next reboot because the controller looks for the newly generated CSR key after the reboot.

Procedure

Step 1 Choose **Security** > **Certificate** > **CSR**.

Step 2 On the **CSR** page, specify the following details:

- Certificate Type
- Country Code
- State
- City
- Organization
- Department
- Common Name
- E-mail
- Key Type

Step 3 Click **Generate**.

What to do next

Download the CSR certificate file that is generated by navigating to **Commands** > **Upload File**.

Generating a Certificate Signing Request using Cisco Wireless Controller (CLI)

In Release 8.3 or a later release, the more secure option is to use the controller itself to generate the CSR.

If you generate the CSR and do not install the resulting certificate, the controller will be inaccessible over HTTPS upon the next reboot because the controller looks for the newly generated CSR key after the reboot.

Procedure

- Generate a CSR by entering this command:

  config certificate generate csr-webauth {**csr-webauth** | **csr-webadmin**} *country state city organization department common-name e-mail*

  The CSR is printed on the terminal after you enter the command.

What to do next

You must copy and paste the CSR printed on the terminal to a file on your computer. You must hand over the CSR to your third-party signing authority or your enterprise public key infrastructure (PKI).

The generated key stays in the controller until the next CSR is generated (the previously generated CSR is overwritten). If you have to change the controller hardware later on (RMA), it is not possible to reinstall the same certificate; instead, you must generate the certificate newly on the new controller.

Downloading Third-Party Certificate

Downloading Third-Party Certificate (GUI)

Procedure

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)

Procedure

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.

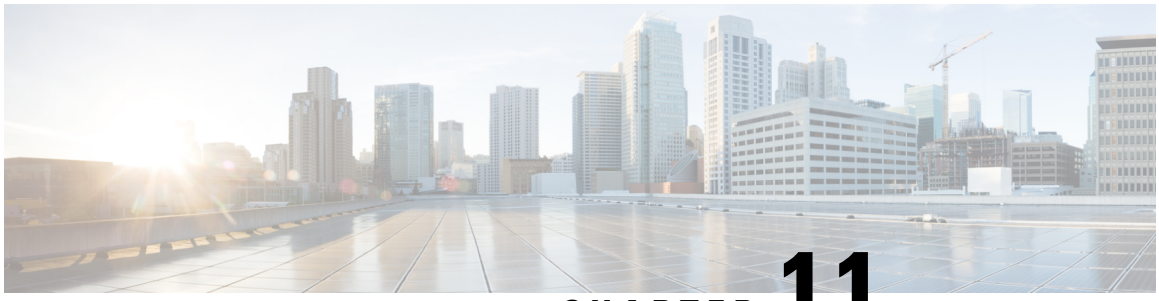
Step 3 Start the certificate and key download by entering the this command:

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 11

AAA Administration

- Setting up RADIUS for Management Users, on page 145
- Setting up TACACS+, on page 186
- Maximum Local Database Entries, on page 193

Setting up RADIUS for Management Users

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 tried.

Note The management password for RADIUS server or controller, which is set for local authentication, is limited to 127 characters in length.

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 32 RADIUS authentication and accounting servers.
- 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 Cisco 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:

Restrictions on Configuring RADIUS

- You can configure the session timeout value for RADIUS server up to 65535 seconds. The controller does not support configuring session timeout value for RADIUS server higher than 65535 seconds.
- The session timeout value configured on RADIUS server if set beyond 24 days, then the RADIUS session timeout value does not override the session timeout value configured locally over a WLAN.
- A network address translation (NAT) scenario when IPSec is enabled on traffic between the controller and RADIUS server is not supported.

Configuring RADIUS Authentication (GUI)

Procedure

Step 1 Choose **Security** > **AAA** > **RADIUS** > **Authentication**.

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 2 From the **Auth Called Station ID Type** drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message for network users. 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
- AP Ethernet MAC Address
- AP Ethernet MAC Address:SSID

Step 3 From the **MAC Delimiter** drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message for network users. The following options are available:

- Colon
- Hyphen
- Single-hyphen
- None

Step 4 Click **Apply**. Perform one of the following:

- To edit an existing RADIUS server, click the server index number for that server. The **RADIUS Authentication Servers > Edit** page appears.
- To add a RADIUS server, click **New**. The **RADIUS Authentication Servers > New** page appears.

Step 5 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 6 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 7 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 8 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 9 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 10 (Optional) Check the **Apply Cisco ISE Default settings** check box.

Enabling Cisco ISE Default settings changes the following parameters:

- CoA is enabled by default.
- The Authentication server details (IP and shared-secret) are also applied to the Accounting server.
- The Layer 2 security of the WLAN is set to WPA+WPA2
- 802.1X is the default AKM.
- MAC filtering is enabled if the Layer 2 security is set to None.

The Layer 2 security is either WPA+WPA2 with 802.1X or None with MAC filtering. You can change these default settings if required.

Step 11 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.

Step 12 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 13 If you are configuring a new RADIUS authentication server, from the **Support for CoA** 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 CoA 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 14 In the **Server Timeout** 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 15 Check the **Network User** check box to enable network user authentication, or uncheck it to disable this feature. The default value is unchecked. 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.

Step 16 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 17 Enter the **Management Retransmit Timeout** value, which denotes the network login retransmission timeout for the server.

Step 18 If you want to use a tunnel gateway as AAA proxy, check the **Tunnel Proxy** check box. The gateway can function as a proxy RADIUS server as well as a tunnel gateway.

Step 19 Check the **PAC Provisioning** check box to enable PAC for RADIUS authentication, or uncheck it to disable this feature. The default value is unchecked. If you enable this feature, the entry is considered by the RADIUS authentication server to provision PAC for users.

Note
You must not enable PAC Provisioning for RADIUS authentication server, if the **Tunnel Proxy** check box is enabled for an AAA server.

Step 20 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
From Release 8.3 onwards, IPSec is supported over IPv6 interfaces as well.

Step 21 From the **IPSec Profile Name** drop-down list, choose the IPSec profile.

You can create an IPSec profile by navigating to **Management** > **IPSec**. For more information, see the "IPSec Profile" section in the "Controller Security" chapter.

Step 22 Click **Apply**.

Step 23 Click **Save Configuration**.

Step 24 Repeat the previous steps if you want to configure any additional services on the same server or any additional RADIUS servers.

Configuring RADIUS Accounting Servers (GUI)

Procedure

Step 1 Choose **Security** > **AAA** > **RADIUS** > **Accounting**.

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 2 From the **Acct Called 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
- AP Ethernet MAC Address
- AP Ethernet MAC Address:SSID

Step 3 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 4 Click **Apply**. Perform one of the following:

- To edit an existing RADIUS server, click the server index number for that server. The **RADIUS Accounting Servers > Edit** page is displayed.
- To add a RADIUS server, click **New**. The **RADIUS Accounting Servers > New** page is displayed.

Step 5 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 6 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 7 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 8 In the **Shared Secret** and **Confirm Shared Secret** text boxes, enter the shared secret key to be used for accounting between the controller and the server.

Note
The shared secret key must be the same on both the server and the controller.

Step 9 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 1813 for accounting.

Step 10 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 11 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 12 Check the **Network User** check box to enable network user accounting, or uncheck it to disable this feature. The default value is unchecked. 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.

Step 13 Check the **Management** check box to enable management accounting, 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 accounting server for management users, and accounting requests go to the RADIUS server.

Step 14 If you want to use a tunnel gateway as AAA proxy, check the **Tunnel Proxy** check box. The gateway can function as a proxy RADIUS server as well as a tunnel gateway.

Step 15 Check the **PAC Provisioning** check box to enable PAC for RADIUS accounting, or uncheck it to disable this feature. The default value is unchecked. If you enable this feature, the entry is considered by the RADIUS accounting server to provision PAC for users.

Note
You must not enable PAC Provisioning for RADIUS accounting server, if the **Tunnel Proxy** check box is enabled for an AAA server.

Step 16 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
From Release 8.3 onwards, IPSec is supported over IPv6 interfaces as well.

Step 17 From the **IPSec Profile Name** drop-down list, choose the IPSec profile.

You can create an IPSec profile by navigating to **Management** > **IPSec**. For more information, see the "IPSec Profile" section in the "Controller Security" chapter.

Step 18 Click **Apply**.

Step 19 Click **Save Configuration**.

Step 20 Repeat the previous steps if you want to configure any additional services on the same server or any additional RADIUS servers.

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-ethmac-only** | **ap-ethmac-ssid** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-mac-ssid-ap-group** | **ap-name** | **ap-name-ssid** | **flex-group-name** | **vlan-id**}

  This command supports both IPv4 and IPv6 address formats.

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.

    This command supports both IPv4 and IPv6 address formats.
  - **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 profile** *ipsec-profile-name radius-index*—Configures an IPSec profile for the RADIUS server specified. You can apply all of the IPSec parameters via this IPSec profile.

You can create a generic IPSec profile by entering the **config ipsec-profile** command. For more information, see the "IPSec Profile" section in the "Controller Security" chapter.

- **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.

  This command supports both IPv4 and IPv6 address formats.
- **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** {**enable** | **disable**} index—Enables or disables a RADIUS accounting server.
- **config radius acct delete index**—Deletes a previously added RADIUS accounting server.
- **config radius acct region** {**group** | **none** | **provincial**}—Configures the RADIUS region.
- **config radius acct realm** {**add** | **delete** } *radius-index realm-string*—Configures the realm of the RADIUS accounting server.
- **config radius auth callStationIdType** {**ap-ethmac-only** | **ap-ethmac-ssid**}—Sets the Called Station ID type to be AP's radio MAC address or AP's radio MAC address with SSID.
- **config radius auth callStationIdType** *ap-label-address*—Sets the Called Station ID Type to the AP MAC address that is printed on the AP label, for the authentication messages.

  config radius auth callStationIdType *ap-label-address-ssid*—Sets the Called Station ID Type to the <AP label MAC address>:<SSID> format, for the authentication messages.
- **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-mac-ssid-ap-group**—Sets Called Station ID type to the format <AP MAC address>:<SSID>:<AP Group>.
- **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.

Note When the Called Station ID type is set to AP name, the conversion of uppercase letters to lowercase letters for the AP name is not considered. For example, while creating an AP, if the AP name is provided with uppercase letters, then the AP name for the call station ID type gets displayed with upper case letters only.

- **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 probing is enabled, the RADIUS server will be probed at every probing time interval irrespective of the probe response having been received or not. For more information, see CSCvc01761.Active management RADIUS servers are probed only if management-kick-out feature is enabled.

Note RADIUS server is probed if you enable probing at every probing time interval irrespective of the probe response. For more information, see CSCvc01761.

- 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).

Note While configuring more than seven servers, you must increase the fallback-test interval to 1000 for a default retransmit timeout of 5 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.
- Configure RADIUS extended source ports support by entering this command:

  config radius ext-source-ports {**enable** | **disable**}

  Enabling multiple source ports allows the number of outstanding RADIUS requests to be increased. With single source port, the number of outstanding requests was limited to 255 for each authentication and accounting request.

  The number of RADIUS queues supported on various controller platforms:
  - Cisco 5520 and 8540 controllers support 16 RADIUS queues
- 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*

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 3: 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

[1] 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 4: 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 5: 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 6: Authentication Attributes Honored in Access-Accept Packets (Microsoft)

Attribute ID	Description
11	MS-CHAP-Challenge
16	MS-MPPE-Send-Key
17	MS-MPPE-Receive-Key
25	MS-MSCHAP2-Response
26	MS-MSCHAP2-Success

Table 7: 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

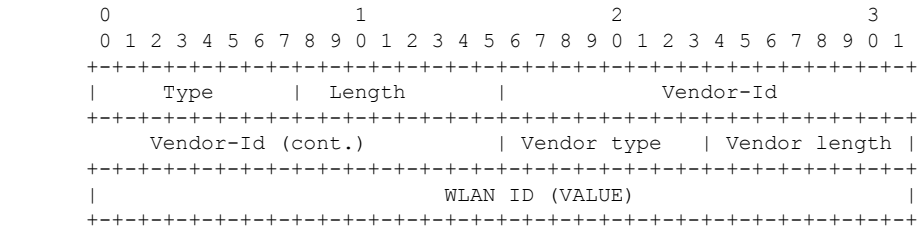
Attribute ID	Description
8	Real-Time-Bandwidth-Average-Contract
9	Data-Bandwidth-Burst-Contract
10	Real-Time-Bandwidth-Burst-Contract
11	Guest-Role-Name **Note** Guest-Role-Name is honored only on L3 security web authentication with AAA over-ride enabled on the controller.
13	Data-Bandwidth-Average-Contract-US
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

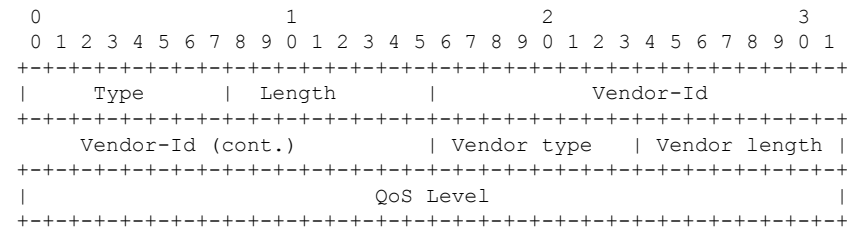
This attribute indicates the WLAN ID of the WLAN to which the client should belong. When the WLAN-ID attribute is present in the RADIUS Access Accept, the system applies the WLAN-ID (SSID) to the client station after it authenticates. The WLAN ID is sent by the controller in all instances of authentication 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

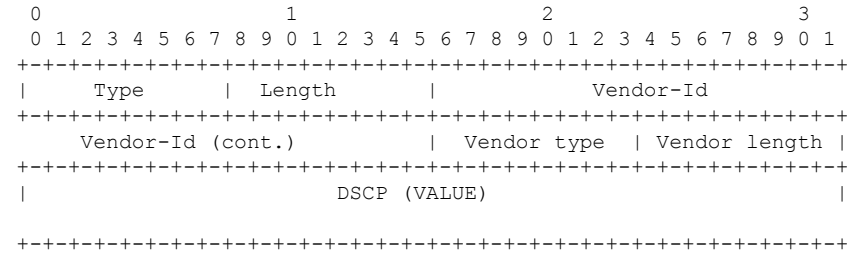
This attribute indicates the QoS level to be applied to the mobile client's traffic within the switching fabric, as well as over the air. This example shows a summary of the QoS-Level Attribute format. The fields are transmitted from left to right.



- 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.

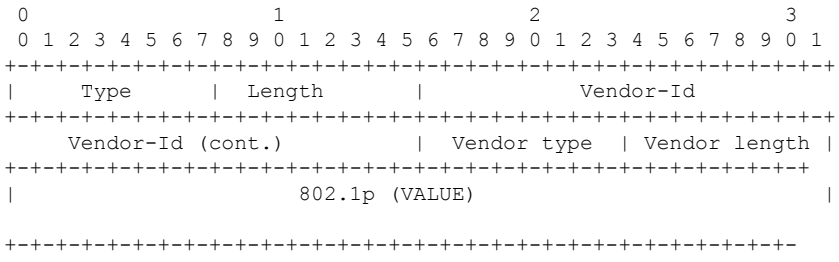


- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179

- Vendor type – 3
- Vendor length – 4
- Value – DSCP value to be applied for the client.

802.1p Tag Type

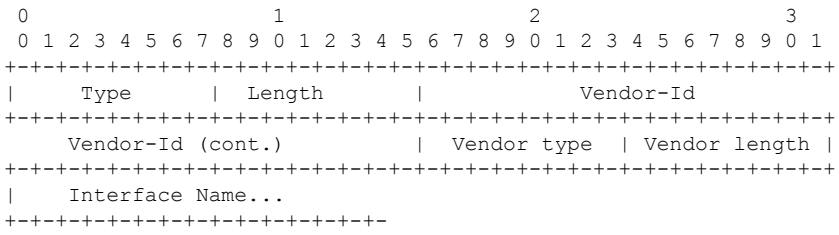
802.1p VLAN tag received from the client, defining the access priority. This tag maps to the QoS Level for client-to-network packets. This attribute defines the 802.1p priority to be applied to the client. When present in a RADIUS Access Accept, the 802.1p value overrides the default specified in the 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.



- 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...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

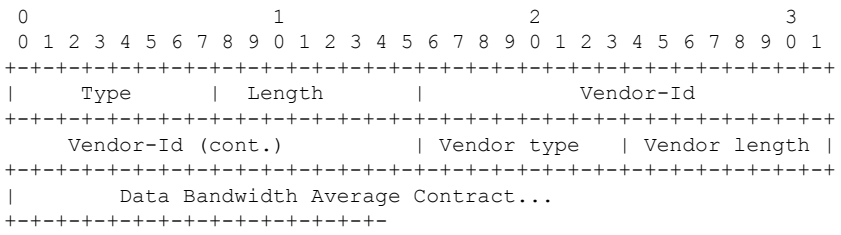
- Type – 26 for Vendor-Specific
- Length – >7
- Vendor-Id – 14179
- Vendor type – 6
- Vendor length – >0
- Value – A string that includes the name of the ACL to use for the client

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 client will be de-authenticated if the ACL is not preconfigured on the controller. 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.

Data Bandwidth Average Contract

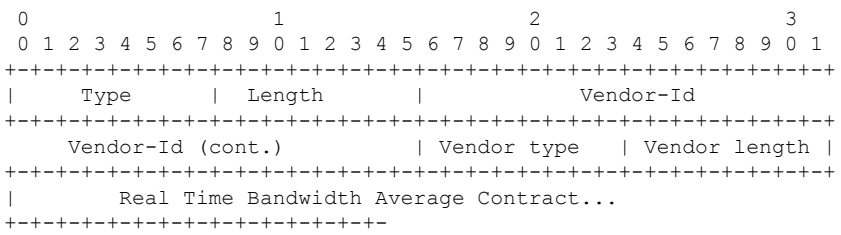
This attribute is a rate limiting value. It indicates the Data Bandwidth Average Contract that will be applied for a client for non-realtime traffic such as TCP. This value is specific for downstream direction from wired to wireless. When present in a RADIUS Access Accept, the Data Bandwidth Average 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.

```
 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 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Data Bandwidth Burst Contract...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- 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.

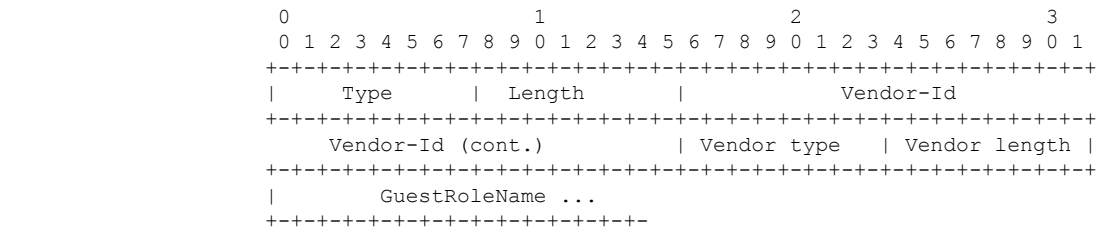
Note If you try to implement Average Data Rate and Burst Data Rate as AAA override parameters to be pushed from a AAA server, both Average Data Rate and Burst Data Rate have to be sent from ISE.

```
 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 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Real Time Bandwidth Burst Contract...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 10
- Vendor length – 4
- Value – A value in kbps

Guest Role Name

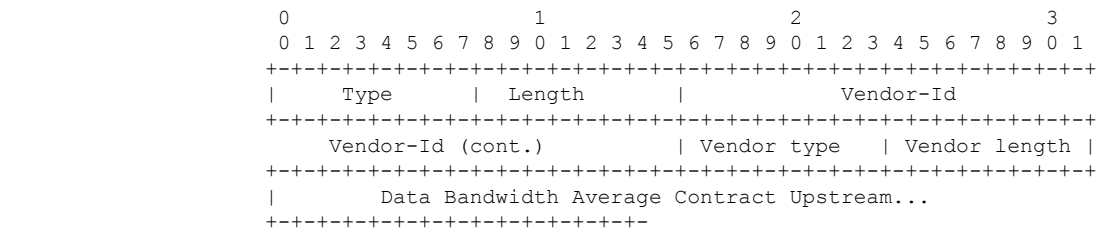
This attribute provides the bandwidth contract values to be applied for an authenticating user. When present in a RADIUS Access Accept, the bandwidth contract values defined for the Guest Role overrides the bandwidth contract values (based on QOS value) specified for the WLAN. The fields are transmitted 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

Data Bandwidth Average Contract Upstream

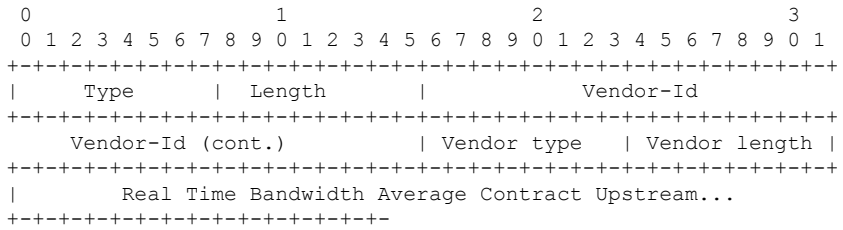
This attribute is a rate limiting value. It indicates the Data Bandwidth Average Contract that will be applied to a client for non-realtime traffic such as TCP. This value is specific to upstream direction from wireless to wired. When present in a RADIUS Access Accept, the Data Bandwidth Average Contract 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 – 13
- Vendor length – 4
- Value – A value in kbps

Real Time Bandwidth Average Contract Upstream

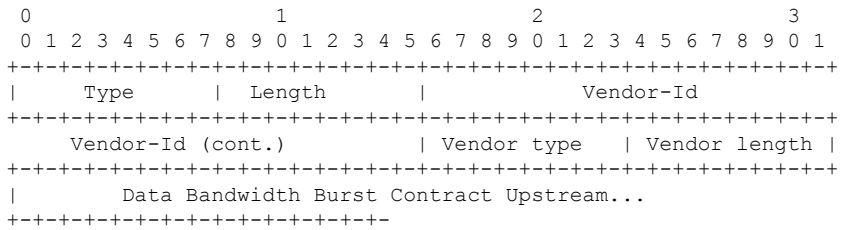
This attribute is a rate limiting value. It indicates the Data Bandwidth Average Contract that will be applied to a client for realtime traffic such as UDP. This value is specific to upstream direction from wireless to wired. When present in a RADIUS Access Accept, the Real Time Bandwidth Average Contract 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 – 14
- Vendor length – 4
- Value – A value in kbps

Data Bandwidth Burst Contract Upstream

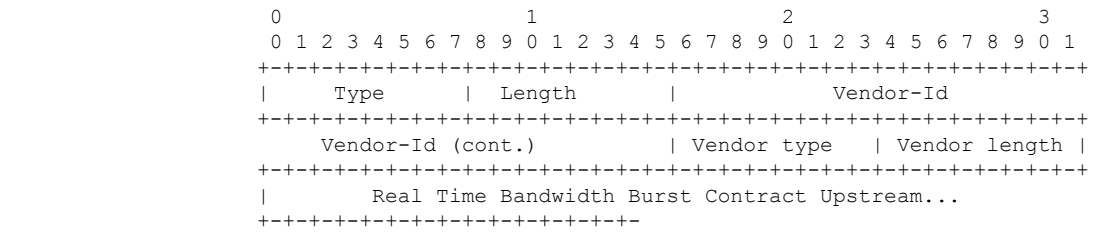
This attribute is a rate limiting value. It indicates the Data Bandwidth Burst Contract that will be applied to a client for non-realtime traffic such as TCP. This value is specific to upstream direction from wireless to wired. When present in a RADIUS Access Accept, the Data Bandwidth Burst Contract 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 – 15
- Vendor length – 4
- Value – A value in kbps

Real Time Bandwidth Burst Contract Upstream

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 upstream direction from wireless to wired. 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.



- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 16
- Vendor length – 4
- Value – A value in kbps

RADIUS Accounting Attributes

This table identifies the RADIUS accounting attributes for accounting requests sent from a controller to the RADIUS server.

Table 8: Accounting Attributes for Accounting Requests

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
8	Framed-IP-Address
25	Class
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)

Attribute ID	Description
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 9: 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.
7	Accounting-On
8	Accounting-Off
9-14	Reserved for Tunneling Accounting
15	Reserved for Failed

RADIUS VSA

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using vendor specific attributes (VSA). VSA allow vendors to support their own extended attributes otherwise not suitable for general use. VSA are predefined in an XML file. You need to add the vendor specific attributes to the XML file and this XML file is downloaded to the controller. There is no configuration required on the controller to enable the support. The file contains the RADIUS attributes in a specific format as explained by the XML schema to specify the XML tags.

The XML file with the vendor specific attributes defined can be downloaded from a FTP server. The downloaded file is stored in the flash memory and retained across several reboot processes. The file is parsed upon successful download and each time when the controller boots up. The XML file can be uploaded to RADIUS server for authentication and accounting. Once controller parses these values, it stores the file in a separate data structures meant for vendor specific attributes storage. The controller uses these attributes value in authentication or accounting packets, or both based on specified usage format. If there are any errors in the file, the controller parsing fails, and the attributes are not applied. You should address the errors in the file or download the file from the FTP server again to the controller.

This section contains the following subsections:

Sample RADIUS AVP List XML File

You can use the sample RADIUS AVP list XML file for reference. The sample XML file contains only two attributes, one for authentication and the other for accounting. You can add more number of RADIUS attributes and value pairs but those attributes and value pairs should be appended in the format specified.

Note The maximum number of WLANs that is supported in an AVP download is 32.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file edited by User1-->

<radiusFile>
<avpList SSID_PROF="test" incAuth="true" incAcct="false">
        <radiusAttributes>
                <attributeName>Idle-Timeout</attributeName>
                <vendorId>9</vendorId>
                <attributeId>21</attributeId>
                <valueType>INTEGER</valueType>
                <attributeValue>100</attributeValue>
        </radiusAttributes>
        <radiusAttributes>
                <attributeName>remote-name</attributeName>
                <vendorId>9</vendorId>
                <attributeId>26</attributeId>
                <valueType>STRING</valueType>
                <attributeValue>TEST</attributeValue>
        </radiusAttributes>
</avpList>
<avpList SSID_PROF="test" incAcct="true">
        <radiusAttributes>
                <attributeName>Idle-Timeout</attributeName>
                <vendorId>9</vendorId>
                <attributeId>21</attributeId>
                <valueType>INTEGER</valueType>
```

```
                <attributeValue>100</attributeValue>
        </radiusAttributes>
        <radiusAttributes>
                <attributeName>remote-name</attributeName>
                <vendorId>9</vendorId>
                <attributeId>26</attributeId>
                <valueType>STRING</valueType>
                <attributeValue>TEST</attributeValue>
        </radiusAttributes>
</avpList>
</radiusFile>
```

Downloading RADIUS AVP List (GUI)

Procedure

Step 1 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 2 From the File Type drop-down list, choose **RADIUS AVP List**.

Step 3 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP**

Step 4 In the IP Address text box, enter the IPv4 or IPv6 address of the server.

Step 5 In the File Path text box, enter the directory path of the RADIUS AVP list.

Step 6 In the File Name text box, enter the name of the RADIUS AVP list.

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 download occurs. The default value is 21. For SFTP, the default value is 22.

Step 8 Click **Download** to download the RADIUS AVP list to the controller. A message appears indicating the status of the download.

Step 9 Choose **Security** > **AAA** > **RADIUS** > **Downloaded AVP** to open the Download RADIUS AVP List page.

Step 10 From the WLAN SSID Profile name drop-down list, choose the WLAN SSID profile name.

Step 11 Click the **Auth AVP** tab to view the RADIUS authentication attributes mapped to the AVP list.

Step 12 Click the **Acct AVP** tab to view the RADIUS accounting attributes mapped to the AVP list.

Uploading RADIUS AVP List (GUI)

Procedure

Step 1 Choose **Commands** > **Upload File** to open the Upload File from Controller page.

Step 2 From the File Type drop-down list, choose **RADIUS AVP List**.

Step 3 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP**

Step 4 In the IP Address text box, enter the IPv4 or IPv6 address of the server.

Step 5 In the File Path text box, enter the directory path of the RADIUS AVP list.

Step 6 In the File Name text box, enter the name of the RADIUS AVP list.

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 download occurs. The default value is 21. For SFTP, the default value is 22.

Step 8 Click **Upload** to upload the RADIUS AVP list from the controller. A message appears indicating the status of the upload.

Uploading and Downloading RADIUS AVP List (CLI)

Procedure

Step 1 Log on to the controller CLI.

Step 2 Download the RADIUS AVPs in the XML file format from the FTP server to the controller by entering this command:

transfer download datatype radius-avplist

Step 3 Upload the XML file from the controller to the RADIUS server using the command:

transfer upload datatype radius-avplist

Step 4 Display VSA AVPs using the command:

show radius avp-list *ssid-profile-name*

Custom NAS-ID for RADIUS Accounting Using Downloadable RADIUS AVP

This feature addresses the need to have a configurable custom NAS-ID for custom accounting purposes on per WLAN basis. To download the XML file to the controller, you can use the FTP (server) method or use the transfer download method. This file is retained in the controller even after the reboot.

The custom AVP supersedes only the WLAN NAS-ID in the accounting messages. The priority of the other NAS-IDs is not affected.

Note

- The Global WLAN NASID is not used in accounting messages. If no NASID (WLAN/Interface/apgroup) is configured at the WLAN, then the system name is sent as the default NASID.
- The AVP list is only available as an uploaded and downloaded config file. You cannot configure or modify the AVP list on the controller using GUI, CLI, or SNMP methods.
- If there are no AVP lists that are downloaded or WLAN specific or interface-specific NAS-ID configured, then the system name is the default NAS-ID.
- The standby controller also receives the AVP list during the XML file is download to the primary controller.

Refer to *RADIUS VSA* section from the *Controller Configuration guide* to create the custom AVP file.

The following are the supported value type for NAS-ID (strictly uppercase):

- SYSNAME
- SYSIP
- SYSMAC
- APIP
- APNAME
- APMAC
- APETHMAC
- APGROUP
- FLEXGROUP
- SSID
- APLOCATION

Note Software downgrade from the 8.6 to older version will not be supported for the new NAS-identifier AVP. If you decide to downgrade to an older version, perform the following steps:

1. Upload the existing RADIUS AVP attribute file.
2. Edit the file to remove the NAS-Identifier AVPs.
3. Downgrade the controller.
4. Download the changed RADIUS AVP file without the NAS-identifier AVP.

Restrictions on Custom NAS-ID for RADIUS Accounting Using Downloadable RADIUS AVP

- The custom NAS-ID string should contain minimum one value type and a maximum of three value type using ":" as the delimiter.

- When a downloaded NAS-ID has multiple custom NAS-ID syntaxes for the same SSID profile, by default the latest syntax is used after overwriting the older one.
- Maximum number of downloadable WLAN SSID profiles are 32.
- The maximum supported length of the custom NAS-IDs that are derived from the syntax is 253.

This section contains the following subsections:

Configuring Custom NAS-ID AVP XML File

Procedure

Step 1 Edit the XML file using a notepad.

Step 2 Update the **SSID_PROF** tag with the WLAN profile name you wish to apply the AVP to.

Step 3 Update the following fields:

- **vendorId** tag to 0
- **attributeId** to 32
- **Valuetype** to "STRING"
- **attributeValue** to attribute tag string with delimiter as ":"

Note
It is necessary to set either the **incAuth** or the **incAcct** value to true. The custom NASID is updated for auth and accounting packets. Only the standard **attributeID** value 32 is supported. Other values are sent as a vendor attribute.

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<radiusFile>
    <avpList SSID_PROF="DocTest_8500_OPEN" incAuth="true" incAcct="true">
        <radiusAttributes>
            <attributeName>SVR-Zip-Code</attributeName>
            <vendorId>0</vendorId>
            <attributeId>32</attributeId>
            <valueType>STRING</valueType>
            <attributeValue> SYSNAME:APNAME:APLOCATION </attributeValue>
        </radiusAttributes>
        <radiusAttributes>
            <attributeName>W2BW-NASId</attributeName>
            <vendorId>0</vendorId>
            <attributeId>32</attributeId>
            <valueType>STRING</valueType>
        <attributeValue>SYSNAME:APNAME:APLOCATION</attributeValue>
                </radiusAttributes>
             </avpList>
        </radiusFile>
```

Step 4 Download the updated AVP XML file to the controller.

Step 5 When the RADIUS download fails, use **debug option debug radius avp-xml enable** to know more about the error.

Deleting a NAS-ID AVP (GUI)

Procedure

Step 1 Edit the AVP XML file using a text editor and delete the SSID_PROF name.

Step 2 Download the updated NAS-ID AVP XML file to the controller.

Step 3 Choose **Security** > **RADIUS** > **Downloaded AVP**. On the **DOWNLOADED RADIUS AVP LIST** page, the **Acct** tab displays an empty page.

The NAS-ID AVP is successfully deleted.

Note
This procedure deletes the selected SSID profile. If multiple AVPs are listed in the XML AVP list file, they continue to function unless deleted using the delete procedure.

Viewing Custom NAS-ID Enhancement Configuration (GUI)

Procedure

Step 1 Choose **WLANs** > **WLAN ID** > **General** to open the **WLAN > Edit** page.

Step 2 In the general tab, view the greyed out NAS-ID field to view the value type.

Check if the format syntax for that file is downloaded and the string is displayed.

Example:

Downloaded NAS-ID syntax	Acct and auth NASID encoded format	Delimiter used
APIP:APNAME:SYSNAME	9.11.12.2:AP_BASEMENT_1:WLC_1	":" Colon

Step 3 Choose **Security** > **RADIUS** > **Downloaded AVP** > **Acct AVP** tab to open the **DOWNLOADED RADIUS AVP LIST** page.

Step 4 Select the **Wlan SSID Profile Name** from the drop-down list.

The AVP details are displayed.

Viewing Custom NAS-ID Enhancement (CLI)

Procedure

- View the downloaded AVP for the NAS-ID by entering this command:

  show radius avp-list *profile-name*
- View detailed information of a client by MAC address by entering this command:

  show client detail *mac-addr*
- View the RADIUS packets by entering this command:

  debug aaa all enable
- Enable the debug log to identify the cause of download failure by entering this command:

  debug aaa avp-xml enable

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:

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.

Configuring Per-WLAN RADIUS Source Support (GUI)

Before you begin

Ensure that the WLAN is in disabled state. You can enable the WLAN after the configuration is done.

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the WLAN ID.

Step 3 Click the **Security** tab, and then click the **AAA Servers** tab.

Step 4 Check the **RADIUS Server Overwrite interface** check box to enable the per-WLAN RADIUS source support.

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 5 From the **Interface Priority** drop-down list, select either **AP Group** or **WLAN** as the interface for RADIUS packet routing.

Step 6 Ensure that the **Interim Interval** for RADIUS Server Accounting is within the valid range.

Step 7 Save the configuration.

Configuring Per-WLAN RADIUS Source Support (CLI)

Procedure

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
```

RADIUS Realm

When mobile clients associate to a WLAN, RADIUS realm is received as a part of EAP-AKA identity response request in the authentication request packet. The Network Access Identifier (NAI) format (EAP-AKA) for WLAN can be specified as *0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org*. The realm in the NAI format is represented after the @ symbol, which is specified as *wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org*. If vendor specific attributes are added for MCC as 311 and MNC as 480 to 489, then the NAI format can be represented as: *0311480999999999@wlan.mnc480.mcc311.3gppnetwork.org*.

For a mobile subscriber, the controller sends the authentication request to the AAA server only when the realm in the NAI format received from the device complies as per the given standards. Apart from authentication, accounting requests are also required to be sent to AAA server based on realm filtering.

In order to support realm filtering on the controller, you need to configure realm on the RADIUS. When a user is connected with a particular SSID, the user is authenticated and authorized using the NAI format received against the realm configured on the RADIUS server.

Realm Support on a WLAN

Each WLAN is configured to support NAI realms. Once the realm is enabled on a particular SSID, the lookup is done to match the realms received in the EAP identity response against the configured realms on the RADIUS server.

Realm Support on RADIUS Server

The RADIUS server needs to redirect the authentication and accounting requests based on configured realms. Each RADIUS server support realms to a maximum of 30 each for authentication and accounting.

- **Realm Match for Authentication**—In WPA2 dot1x with EAP methods (similar to EAP AKA), the username is received as part of EAP identity response. The realm is derived from the username and match with the realms configured in the RADIUS authentication server. If there is a match, then the authentication requests are forwarded to the RADIUS server. If there is a mismatch, then the client is deauthenticated.
- **Realm Match for Accounting**—Username is received in access accept messages. When accounting messages are triggered, the realm is derived from the username and compared against the accounting realms configured on the RADIUS accounting server. If succeeded, accounting requests are forwarded to the RADIUS server. If there is a mismatch, the accounting requests are dropped. For example, if realm is configured as **cisco** on the controller, then the username is authenticated as **xyz@cisco** on the RADIUS server.

Note Even if the NAI realm is enabled on a WLAN and if there is no realm in the username, then the behavior is defaulted to no lookup, and the usual selection of the RADIUS server is followed.

Note When the client uses fast re-authentication identity, the realm name is required from the authentication server in order for the controller to forward corresponding requests to the correct server.

When EAP-AKA is used along with realm, fast reauthentication is supported when EAP server responds with AT_NEXT_REAUTH_ID attribute that has both the username portion and realm portion. Purpose of the realm is received controller picks up the right server for the subsequent fast reauthentication requests. For example, host APD server which supports EAP-AKA does not support realm portion. Therefore, the controller supports fast reauthentication only with those EAP servers which have this compatibility.

This section contains the following subsections:

Prerequisites for Configuring RADIUS Realm

RADIUS authentication or accounting server has to be disabled before adding realm and enabled after adding realm on the controller.

Restrictions for Configuring RADIUS Realm

- You can configure a maximum of 17 RADIUS authentication and accounting servers to one controller.

- The total number of realms that you can configure for one RADIUS authentication and accounting server is 30.

Configuring Realm on a WLAN (GUI)

Procedure

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 Select the **RADIUS NAI-Realm** check box to enable realm on the WLAN.
Step 5 Click **Apply** to commit your changes.
Step 6 Click **Save Configuration** to save your changes.

Configuring Realm on a WLAN (CLI)

Procedure

Step 1 Enable or disable realm on a WLAN by entering this command:
config wlan *radius_server* **realm** {**enable** | **disable**} *wlan-id*
Step 2 View the realm configuration on a WLAN by entering this command:
show wlan *wlan-id*

Configuring Realm on a RADIUS Authentication Server (GUI)

Procedure

Step 1 Choose **Security** > **AAA** > **RADIUS** > **Authentication** to open RADIUS Authentication Servers > Edit page.
Step 2 Click the Realm List link to open the Authentication Server Index page.
Step 3 Enter the realm name in the Realm Name text box.
Step 4 Click **Add**.

Configuring Realm on a RADIUS Authentication Server (CLI)

Procedure

Step 1 Add realm to a RADIUS authentication server by entering this command:

config radius auth realm add *radius_index realm_string*

Step 2 Delete realm from a RADIUS authentication server by entering this command:
config radius auth realm delete *radius_index realm_string*

Step 3 View RADIUS authentication server information by entering this command:
show radius auth detailed *radius_index*

Configuring Realm on a RADIUS Accounting Server (GUI)

Procedure

Step 1 Choose **Security** > **AAA** > **RADIUS** > **Accounting** to open RADIUS Accounting Servers > Edit page.
Step 2 Click the Realm List link to open the Accounting Server Index page.
Step 3 Enter the realm name in the Realm Name text box.
Step 4 Click **Add**.

Configuring Realm on a RADIUS Accounting Server (CLI)

Procedure

Step 1 Add realm to a RADIUS accounting server by entering this command:
config radius acct realm add *radius_index realm_string*

Step 2 Delete realm from a RADIUS accounting server by entering this command:
config radius acct realm delete *radius_index realm_string*

Step 3 View RADIUS accounting server information by entering this command:
show radius acct detailed *radius_index*

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.

Procedure

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.

User Login Policies

User Login Policies control the maximum number of concurrent netuser logins under one netuser name. The user name is case sensitive (CSCuu42548). Setting this to 0 means that there is no limit, and 8 is the maximum.

User Login Policies also control the logins under Layer 3 authentications and EAP. For EAP logins, the behavior of the maximum number of user logins is affected by the setting of the **Max-Login Ignore Identity Response** option. If you enable this, then the EAP identity response user name values are ignored for the purposes of enforcing a user name login limit.

Configuring User Login Policies (GUI)

Procedure

Step 1 Choose **Security** > **AAA** > **User Login Policies**.

Step 2 In the **User Policies** window, enter the maximum number of login sessions for a single user.

The valid range is 0 to 8. The default value is 0. If you set this to 0, unlimited login sessions are permitted for a single user.

Step 3 Save the configuration.

Configuring User Login Policies (CLI)

Procedure

Step 1 Configure the maximum number of login sessions for a single user by entering this command:

config netuser maxUserLogin *count*

The valid range is 0 to 8. The default value is 0. If you set *count* to 0, unlimited login sessions are permitted for a single user.

Step 2 Save the configuration by entering this command:

save config

AAA Override (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.

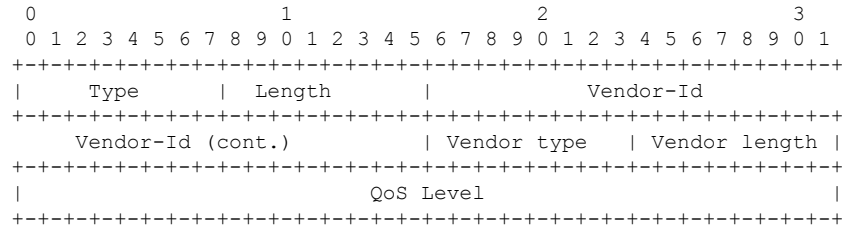
This section contains the following subsection:

RADIUS Attributes Used in Identity Networking

QoS-Level

This section explains the RADIUS attributes used in identity networking.

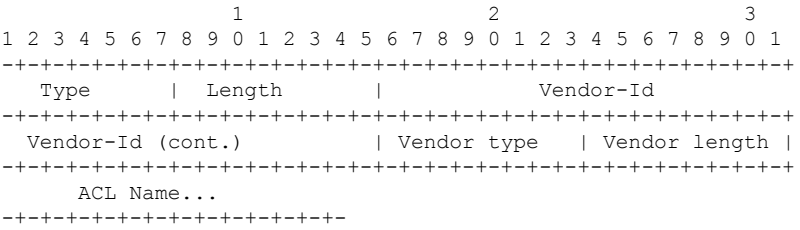
This attribute indicates the QoS level to be applied to the mobile client's traffic within the switching fabric, as well as over the air. This example shows a summary of the QoS-Level Attribute format. The text boxes are transmitted from left to right.



- 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

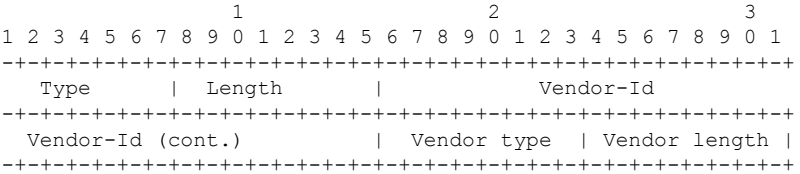
This attribute indicates the ACL name to be applied to the client. A summary of the ACL-Name Attribute format is shown below. The text boxes are transmitted from left to right.



- 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.



```
|    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.

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.

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.

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 The TACACS+ management password is limited to 127 characters in length.

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.

Note Both MANAGEMENT and SECURITY roles are needed for creating local management user and IPsec profile.

- 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.
- To configure the TACACS+ server, using Cisco 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.

Dynamic Management User Login via AAA Server

The management users, who logged in using local credentials when external AAA servers were not available, are notified to re-authenticate within the set timeframe when external TACACS+ servers are available. Failing to authenticate terminates the user session. TACACS+ uses the TACACS+ fallback-test configuration and the re-authentication configuration is common to RADIUS and TACACS+. This enhancement was introduced in 8.2 release.

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)

Procedure

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 controller. 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 Configure the TACACS+ probe duration mode as follows:
a) Choose **Security** > **AAA** > **TACACS+** > **Fallback**. The **TACACS+ Fallback Parameters** page appears.
b) From the **Fallback Mode** drop-down list, select **Enable**.
c) In the **Interval in sec** text box, enter the time in seconds. The valid range is between 180 and 3600 seconds.
d) Click **Apply**.

Step 14 Configure the re-authentication terminal interval for a user before being logged out as follows:
a) Choose **Security** > **AAA** > **General**. The **AAA General** page appears.
b) In the **Mgmt User Re-auth Interval** text box, enter the time in seconds. The valid range is between 0 and 300.
c) Click **Apply**.

Step 15 Click **Save Configuration**.

Step 16 Repeat the previous steps if you want to configure any additional services on the same server or any additional TACACS+ servers.

Step 17 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 18 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 19 Click **Apply**.

Step 20 Click **Save Configuration**.

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.

    This command supports both IPv4 and IPv6 address formats.

- **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.

    This command supports both IPv4 and IPv6 address formats.
  - **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.
  - **config tacacs athr mgmt-server-timeout** *index timeout*—Configures the default management login server timeout 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.

    This command supports both IPv4 and IPv6 address formats.
  - **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.
  - **config tacacs acct mgmt-server-timeout** *index timeout*—Configures the default management login server timeout 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.
- Configure TACACS+ probe and re-authentication interval by entering these commands:
  - **config tacacs fallback-test interval** *seconds*—Enables and sets the probe interval for TACACS+ server. The valid range is `0` to disable and between `180` and `3600` seconds when enabled.
  - **config mgmtuser termination-interval** *seconds*—Sets the interval of re-authentication window for the user before being logged out of the system. The valid range is between `0` and `300`. Default value is 0.
- View the user authentication server configuration by entering the following commands:
  - **show aaa auth** —Displays AAA related information for authentication servers.
  - **show tacacs summary** —Displays TACACS+ summary
- Enable or disable TACACS+ debugging by entering this command:

  debug aaa tacacs {**enable** | **disable**}
- Save your changes by entering this command:

  save config

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.

The maximum entries that are supported by each platform are listed in the following table.

Table 10: Maximum Supported Local Database Entries

Platform	Maximum Entries Supported
Cisco 3504 Wireless Controller	12000

Platform	Maximum Entries Supported
Cisco 5520 Wireless Controller	12000
Cisco 8540 Wireless Controller	12000
Cisco Virtual Wireless Controller	2048

Note If you modify the maximum local database entry parameter, you must reboot the controller for the changes to take effect.

This section contains the following subsections:

Related Topics

Restrictions on Managing User Accounts, on page 197

Configuring Maximum Local Database Entries (GUI)

Procedure

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)

Procedure

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:

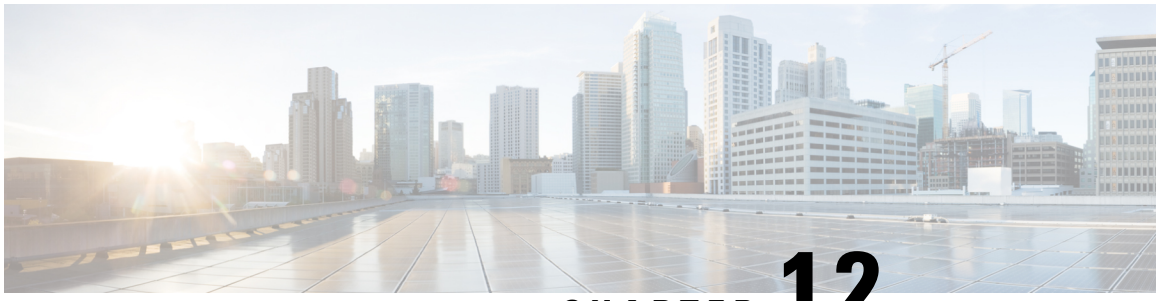
config database size *max_entries*

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 12

Managing Users

- Administrator Usernames and Passwords, on page 197
- Lobby Ambassador Account, on page 199
- Guest Accounts, on page 201
- Client Whitelisting, on page 202
- Password Policies, on page 207

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.

Restrictions on Managing User Accounts

- The local user database is limited to a maximum of 12000 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 \.

Related Topics

Maximum Local Database Entries, on page 193

Configuring Usernames and Passwords (GUI)

Procedure

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)

Procedure

- 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.
  - **config mgmtuser type5-add** *username md5-crypt_password* { **read-write** | **read-only** | **lobby-admin** } *description* —Creates a management username-password pair with type-5 encryption.
  - **config mgmtuser type5-password** *username md5-crypt_password* —Configures type-5 encrypted password for an existing management user account.
- List the configured users by entering this command:

  show mgmtuser
- View the type of password encryption used for the current user by entering this command:

  debug aaa detail enable

Lobby Ambassador Account

This section contains the following subsections:

Creating a Lobby Ambassador Account (GUI)

Procedure

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)

Procedure

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.

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 configuration 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:

Viewing the Guest Accounts (GUI)

Procedure

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

- To see all of the local net user accounts (including guest user accounts) using the controller CLI, enter this command:

  show netuser summary

Client Whitelisting

Locations such as a university receive many guests with multiple devices. It becomes eminent to protect the network from misuse or unauthorized access and allow legitimate clients to connect to the network. Registering or deregistering of clients is a tedious and time consuming task to perform regularly. Hence the requirement for a simpler solution.

This feature addresses the need of allowing clients on a particular WLAN or SSID based on the MAC address. For this purpose, the currently existing features are reused - MAC filtering option on WLAN, adding lobby admin user and reuse AAA DB to store the list of allowed clients on a WLAN.

Two types of administrators manage the feature administration:

- Global Administrator—Creates a lobby admin user on the controller and enables the lobby administrator access on a WLAN.
- Lobby Administrator—Adds or deletes the clients from an allowed list to manage the association to a WLAN or SSID through the GUI interface only. Existing lobby administrators can also be used to configure the allowed lists.

This section contains the following subsections:

Restrictions for Client Whitelisting

- For Cisco vWLC, the AAA database is restricted to 2048 entries.
- For Cisco 5520, 3504, and 8540 Wireless Controllers, the AAA database size is increased to 12000 entries.
- The MAC address cannot be registered under multiple WLANs or SSIDs.
- Lobby Administrator can only configure using GUI interface.

Note This AAA database is shared across:

- MAC filtering
- Local net users
- Management users
- Manual blocked list users
- AP authenticated list users
- Guest users

Configuring Lobby Administrator by Global Administrator (GUI)

This section provides instructions to create or delete the lobby administrator on the controller for the management of guest users and allowed users by the global administrator.

Procedure

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

Step 2 In the Local Management Users section, add the lobby administrator:

a) Click **New**.
b) Enter the **User Name**.
c) Enter the **Password**.
d) Confirm **Password**.
e) Choose **lobby admin** under the **User Access Mode** drop-down list.
f) Click **Apply**.

What to do next

Configure Lobby Administrator Access on WLAN.

Configuring Lobby Administrator by Global Administrator (CLI)

Procedure

Step 1 Add a local lobby admin to controller by entering this command.

config mgmtuser add *username password* **lobby-admin**

Step 2 Enable or disable the lobby admin access on the WLAN by entering this command.

config wlan lobby-admin-access { **enable | disable**} *wlan-id*

Configuring Client Whitelist by Global Administrator (CLI)

The global administrator can configure clients that need to be allowed by using the following commands.

Procedure

Step 1 View the WLAN lobby access status by entering this command.

show wlan lobby-admin-access

Step 2 View the WLAN associated client list by entering this command.

show client wlan *wlan-id*

Step 3 Add selected or all clients of the allowed group by entering this command.

config mac-filter add *mac-address wlan-id interface description*

Note
For this feature, the interface field value is set to 0.

Step 4 Delete selected or all selected clients of the allowed group by entering this command.

config mac-filter delete *mac-addr*

Step 5 View the summary of all the MAC filter entries on all WLANs by entering this command.

show macfilter summary

Step 6 View the list of all MAC filter entries on a given WLAN entering this command.

show macfilter wlan *wlan-id*

Step 7 Enable or disable MAC filtering on a WLAN by entering this command.

config wlan mac-filtering {**enable** | **disable**} *wlan-id*

Configuring Lobby Administrator Access on WLAN by Global Administrator (GUI)

This section provides instructions to enable the lobby admin for a WLAN.

Procedure

Step 1 Choose **WLANs** > **WLAN ID** > **Security** tab.

Step 2 Check the **Lobby Admin Access** check box.

Step 3 Click **Apply**.

Creating Client Whitelist by Lobby Administrator (GUI)

Adding MAC Addresses to a Whitelist by SSID

This section provides multiple methods which you can use as a lobby administrator to create an allowed list of valid users for a WLAN.

Before you begin

1. The lobby administrator must be in config mode under the required WLAN.
2. Inform the target users to connect their devices to a particular SSID.

Procedure

Step 1 Log in to the Controller as the lobby administrator.

Step 2 Choose **White List Users**.

Step 3 Choose the WLAN from the drop-down list for which the allowed list must be applied.

Step 4 Choose **Config Mode**.

Step 5 Click **Apply**.

Step 6 Click **Filter by**.

Select AP Name and enter the AP name.

Step 7 Click the **search icon**.

The result displays the connected clients to the select AP.

Step 8 Check the **Select All** check box.

All the clients displayed are selected.

Step 9 Enter the description in the **Description** field.

Enter an identity tag to this list for easy administration.

Step 10 Click **Add**.

Step 11 Select **Running Mode**.

Step 12 Click **Apply**.

The radio will restart for the new WLAN configuration to take effect.

Only clients in the allowed list continue to be associated, rest of the clients are disassociated from the AP.

Adding Single MAC Address to Whitelist

Procedure

Step 1 Log in to the Controller as the lobby ambassador.
Step 2 Choose **White List Users**.
Step 3 Choose the WLAN from the drop-down list for which the allowed list must be applied.
Step 4 Enter the **MAC address**.
Step 5 Enter the **Description**.
Step 6 Click **Add**.

Note
Repeat steps 4 to 6 to add more single MAC address.

Importing MAC Address CSV List to Whitelist

Procedure

Step 1 Log in to the Controller as the lobby ambassador.
Step 2 Choose **White List Users**.
Step 3 Choose the WLAN from the drop-down list for which the allowed list must be applied.
Step 4 Click the **Config Mode** radio button.
Step 5 Click **Apply**.
Step 6 Check the **Upload CSV file** check box.
Step 7 Click **Browse File**.
Step 8 Choose the CSV file to import.
Click **OK** in the dialog box.
Step 9 Click **Add**

Deleting MAC Address from Whitelist (GUI)

You can delete a single MAC address or in bulk from the whitelist.

Procedure

Step 1 Log in to the Controller as the lobby administrator
Step 2 Choose **White List Users**
Step 3 Choose the WLAN from the drop-down list to retrieve the allowed list.

Step 4 Choose one of the following deletion methods:

a) Single client deletion—Either enter the **client MAC address** and click **delete** or click the **X** delete icon in front of the MAC address to delete.

b) Multiple client deletion—Filter the clients to be deleted based on either AP name or description, select all or selected multiple MAC addresses and click **delete**

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.

Guidelines and Restrictions for 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 8 characters and maximum of 127 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)

Procedure

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 controller 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:

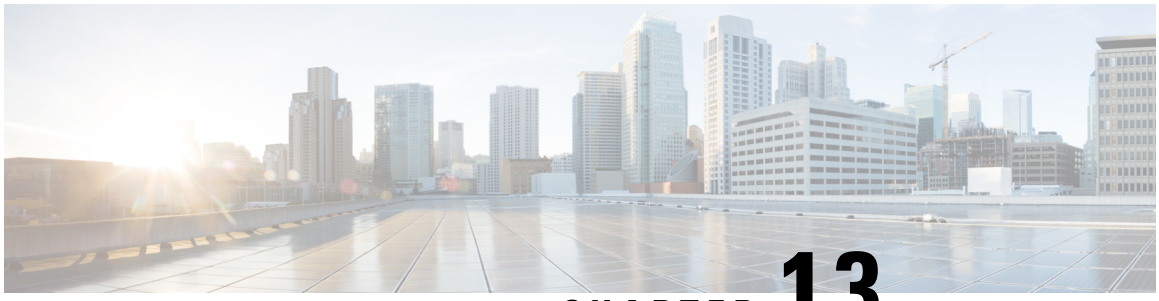
  config switchconfig strong-pwd lifetime {**mgmtuser** | **snmpv3user**} *lifetime-in-days*

- 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 13

Ports and Interfaces

- Ports, on page 211
- Link Aggregation, on page 215
- Interfaces, on page 219

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

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

- 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 controller box. If the same IPv6 packet comes as a network packet to the controller, 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.

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 respective controller documentation:

- Cisco 3504 Wireless Controller Deployment Guide
- Cisco 5520 Wireless Controller Deployment Guide
- Cisco 8540 Wireless Controller Deployment Guide

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.

Procedure

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.
- 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.

Configuring Ports (CLI)

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.

Procedure

Step 1 Configure the administrative mode for a specific port or all ports by entering this command:

config port adminmode {*port* | **all**} {**enable** | **disable**}

Step 2 Configure the up and down link traps for a specific port or all ports by entering this command:

config port linktrap {*port* | **all**} {**enable** | **disable**}

Step 3 Configure the maximum speed for a port by entering this command:

config port maxspeed *port* {**1000** | **2500** | **5000**}

- **1000**: 1 Gbps
- **2500**: 2.5 Gbps
- **5000**: 5 Gbps

Step 4 Configure Power over Ethernet for a specific port or all ports by entering this command:

config port power {*port* | **all**} {**enable** | **disable**}

Monitoring Ports (CLI)

Procedure

- See a summary or a detailed information about all ports by entering this command:

  show port {**summary** | **detailed-info**}

- See information about a specific port by entering this command:

  show port *port-num*

- See a VLAN port table summary by entering this command:

  show port vlan

- See port statistics information by entering this command:

show stats port {**detailed** | **summary**}

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.

LAG in Transition

We recommend that the best practice, when enabling or disabling LAG on the controller, is to not leave the controller in a transitional state. Instead, we recommend that you reboot the controller immediately to implement the desired change.

A controller that supports link aggregation (LAG) can go into a LAG-in-Transition (LAT) mode during transition between LAG to non-LAG mode or vice-versa. The transition is complete only when the controller is rebooted. During the LAT mode, you can make configuration or interface changes and also revert to the previous LAG mode. After the controller is rebooted, your configuration could be lost or you might encounter a system failure. From Release 8.4, it is possible to prevent such incidents by restricting interface related configuration changes when the controller is in LAT state (CSCuz53972).

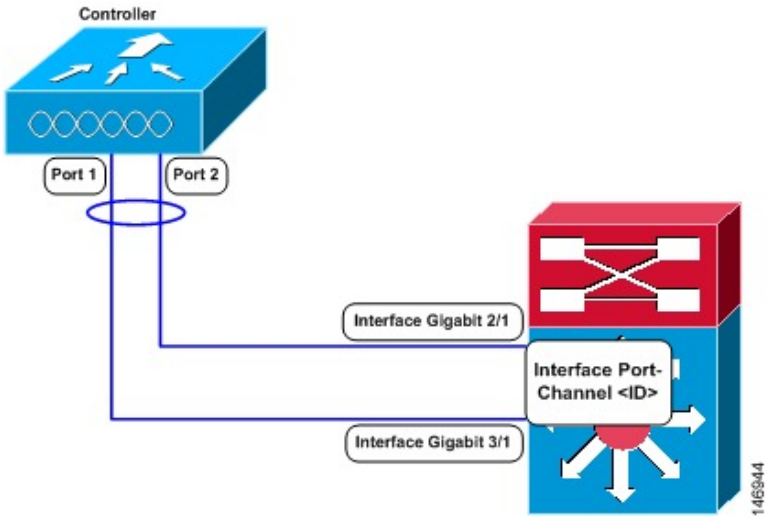
This section contains the following subsections:

Restrictions on Link Aggregation

- 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 16: 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.
- 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)

Procedure

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)

Procedure

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)

Procedure

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.

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 An 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)
- 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 controllers 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 for Configuring Interfaces

- 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

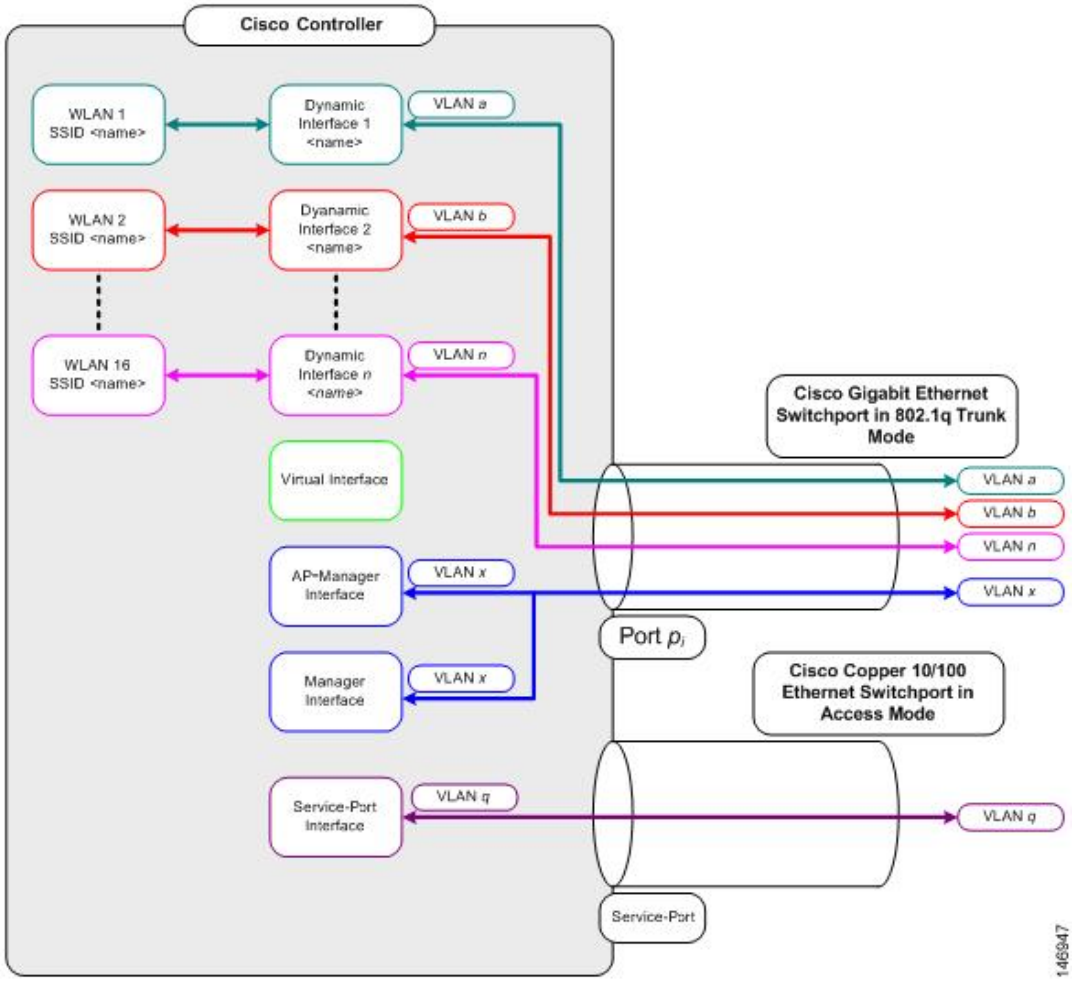
A dynamic interface is created as a WLAN interface by default. However, any dynamic interface can be configured as an AP-manager interface, with one AP-manager interface allowed per physical port. A dynamic interface with the Dynamic AP Management option enabled is used as the tunnel source for packets 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 17: 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.

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)

Procedure

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
- 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.

- Physical port assignment
- 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)

Procedure

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.

Note
This command output shows the port 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.

- **config interface port management** *primary-port* [*secondary-port*]

- **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.

- **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 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.

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)

Procedure

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)

Procedure

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.

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 While IPv6 addressing is used along with stateless address auto-configuration, the controller does not perform the subnet verification; however, you must not connect the service-port in the same subnet as the other interfaces in the controller.

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:

Configuring Service-Port Interfaces Using IPv4 (GUI)

Procedure

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)

Procedure

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)

Procedure

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)

Procedure

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.

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.
- You must allocate a dedicated, static IP address for the subnet and VLAN that will be assigned to the dynamic interface.

Restrictions on Configuring Dynamic Interfaces

The following restrictions apply for configuring the dynamic interfaces on the controller:

- If the SNMP management station is in the same subnet that is assigned to a dynamic interface, then for any SNMP polling, the request should be issued to the IP address assigned to that dynamic interface, rather than the management interface of the controller.
- 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)

Procedure

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 configuring 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
- NAT address

  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)

Procedure

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.

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)

Procedure

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:

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

A controller configured with IPv6 address does not support Dynamic AP-Manager. The management interface acts like an AP-manager interface by default.

Procedure

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.

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.

- Dual stack clients with a static-IPv4 address is not supported.

Creating Interface Groups (GUI)

Procedure

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)

Procedure

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)

Procedure

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)

Procedure

Add interfaces to interface groups by entering this command:

config interface group interface add *interface_group interface_name*

Viewing VLANs in Interface Groups (CLI)

Procedure

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)

Procedure

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**.

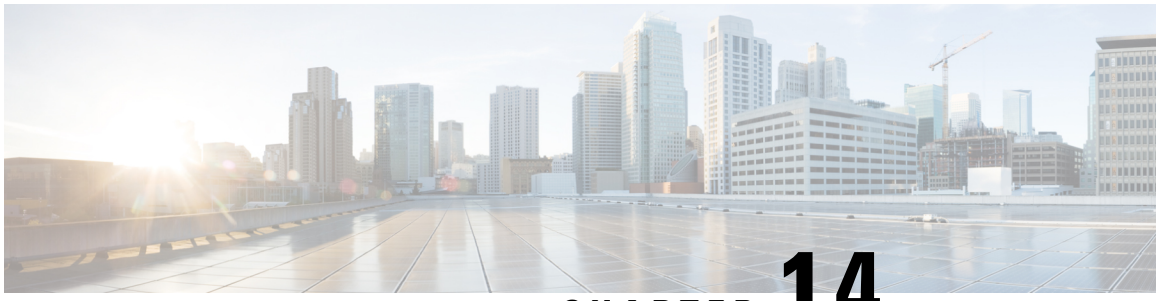
Note
Suppose that the interface group that you add to a WLAN has RADIUS Server Overwrite interface enabled. In this case, when a client requests for authentication, the controller selects the first IP address from the interface group as the RADIUS server.

Adding an Interface Group to a WLAN (CLI)

Procedure

Add an interface group to a WLAN by entering this command:

config wlan interface *wlan_id interface_group_name*



CHAPTER 14

IPv6 Clients

- IPv6 Client Mobility, on page 241
- Prerequisites for Configuring IPv6 Mobility, on page 241
- Restrictions on Configuring IPv6 Mobility, on page 242
- Global IPv6, on page 242
- RA Guard, on page 243
- RA Throttling, on page 244
- IPv6 Neighbor Discovery, on page 245

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.

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 controllers is assigned to the same dynamic interface with the same VLAN ID on all the controllers. The client receives the correct IPv4 address; however, it receives a router advertisement from the different subnets that reach the other controllers. There could be an 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.
- 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.

Global IPv6

This section contains the following subsections:

Restrictions on Global IPv6

- IPv4 address needs to be configured on the interface prior to configuring the IPv6 address.

Configuring IPv6 Globally (GUI)

Procedure

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

- Enable or disable IPv6 globally by entering this command:

  config ipv6 {**enable** | **disable**}

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)

Procedure

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

- Configure RA Guard by entering this command:

  config ipv6 ra-guard ap {**enable** | **disable**}

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)

Procedure

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)

Procedure

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**}}

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)

Procedure

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:

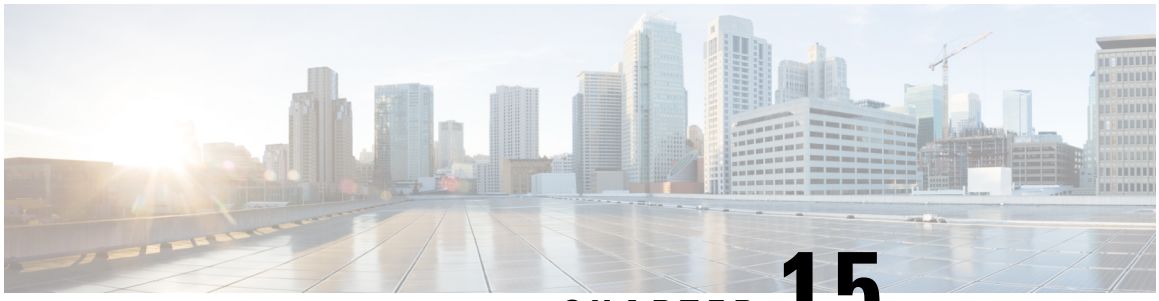
  config ipv6 neighbor-binding timers {**down-lifetime** | **reachable-lifetime** | **stale-lifetime**} {**enable** | **disable**}
- Configure the Unknown Address Multicast NS Forwarding by entering this command:

  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 15

Access Control Lists

- Information about Access Control Lists, on page 247
- Guidelines and Restrictions on Access Control Lists, on page 248
- Configuring Access Control Lists (GUI), on page 249
- Applying an Access Control List to an Interface (GUI), on page 251
- Applying an Access Control List to the Controller CPU (GUI), on page 251
- Applying an Access Control List to a WLAN (GUI), on page 252
- Applying a Preauthentication Access Control List to a WLAN (GUI), on page 253
- Configuring Access Control Lists (CLI), on page 253
- Applying Access Control Lists (CLI), on page 254
- Layer 2 Access Control Lists, on page 255
- DNS-based Access Control Lists, on page 259
- URL Filtering, on page 262
- CNAME IPv6 Filtering, on page 269
- Domain-based Filtering, on page 272

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.
- 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.
- Multicast traffic received from wired networks that is destined to wireless clients is not processed by controller ACLs. Multicast traffic initiated from wireless clients, destined to wired networks or other wireless clients on the same controller, is processed by controller ACLs.
- ACLs are configured on the controller directly or configured through 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.
- DNS traffic is permitted by default with or without ACL entries for clients that are awaiting web authentication.

Configuring Access Control Lists (GUI)

Procedure

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.

Related Topics

Configuring FlexConnect Access Control Lists (GUI), on page 1225

Applying an Access Control List to an Interface (GUI)

Procedure

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.

Procedure

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)

Procedure

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)

Procedure

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 Access Control Lists (CLI)

Procedure

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)

Procedure

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.

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

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.

Configuring Layer 2 Access Control Lists (GUI)

Procedure

Step 1 Choose **Security** > **Access Control Lists** > **Layer2 ACLs** to open the Layer2 Access Control Lists page.

Step 2 Add a new ACL by clicking **New**. The Layer2 Access Control Lists > New page appears.

Step 3 In the Access Control List Name text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 4 Click **Apply**. When the Layer2 Access Control Lists page reappears, click the name of the new ACL.

Step 5 When the Layer2 Access Control Lists > Edit page appears, click **Add New Rule**. The Layer2 Access Control Lists > Rules > New page appears.

Step 6 Configure a rule for this ACL as follows:

a) The controller supports up to 16 rules for each ACL. These rules are listed in order from 1 to 16. In the Sequence text box, enter a value (between 1 and 16) 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 15, 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 Ether Type drop-down list, choose any option from the following Ether type:

- AppleTalk Address Resolution Protocol
- VLAN-tagged Frame & Short Path Bridging
- IPX (0x8137)
- IPX (0x8138)
- QNS Qnet
- Internet Protocol Version 6
- Ethernet Flow Control
- Slow Protocol
- CobraNet
- MPLS Unicast
- MPLS Multicast
- PPPoE Discovery Stage
- PPPoE Session Stage
- Jumbo Frames
- HomePlug 1.0 MME
- EAP over LAN
- PROFINET over Protocol
- HyperSCSI
- ATA over Ethernet
- EtherCAT Protocol

Note
You can select any predefined Ether Types from the Ether Type drop-down list or enter your own Ether type value using the custom option from the Ether Type drop-down list.

c) 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.

d) Click **Apply** to commit your changes. The Layer2 Access Control Lists > Edit page reappears, showing the rules for this ACL.

e) Repeat this procedure to add any additional rules for this ACL.

Step 7 Click **Save Configuration** to save your changes.

Step 8 Repeat this procedure to add any additional ACLs.

Applying a Layer2 Access Control List to a WLAN (GUI)

Procedure

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 **Layer2 ACL** drop-down list, choose the ACL you have created.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Applying a Layer2 Access Control List to an AP on a WLAN (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs** 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 On the **All APs > Details** page, click the **FlexConnect** tab.

Step 4 From the **PreAuthentication Access Control Lists** area, click the **Layer2 ACLs** link to open the **ACL Mappings** page.

Step 5 From the **Layer2 ACL** drop-down list in the WLAN ACL Mapping area, choose the ACL you have created and click **Add**.

Step 6 Save the configuration.

DNS-based Access Control Lists

The DNS-based ACLs are used for client devices such as Apple and Android devices. When using these devices, you can set pre-authentication ACLs on the controller to determine where devices have the right to go.

To enable DNS-based ACLs on the controller, you need to configure the allowed URLs for the ACLs. The URLs need to be pre-configured on the ACL.

With DNS-based ACLs, the client when in registration phase is allowed to connect to the configured URLs. The controller is configured with the ACL name and that is returned by the AAA server for pre-authentication

ACL to be applied. If the ACL name is returned by the AAA server, then the ACL is applied to the client for web-redirection.

At the client authentication phase, the ISE server returns the pre-authentication ACL (url-redirect-acl). The DNS snooping is performed on the AP for each client until the registration is complete and the client is in SUPPLICANT PROVISIONING state. When the ACL configured with the URLs is received on the controller, the CAPWAP payload is sent to the AP enabling DNS snooping on the client and the URLs to be snooped.

With URL snooping in place, the AP learns the IP address of the resolved domain name in the DNS response. If the domain name matches the configured URL, then the DNS response is parsed for the IP address, and the IP address is sent to the controller as a CAPWAP payload. The controller adds the IP address to the allowed list of IP addresses and thus the client can access the URLs configured.

This section contains the following subsections:

Guidelines and Restrictions on DNS-based Access Control Lists

- In Release 8.0, support was added for DNS-based ACL with local web authentication.
- Local authentication is not supported for FlexConnect APs.
- In Release 8.2 and later releases, a maximum of 20 URLs can be allowed for an ACL.
- In Release 8.2 and later releases, on the controller, 40 IP addresses are allowed for one client.
- DNS-based ACLs are not supported on FlexConnect APs with Local Switching.

Note In Release 8.7, support was added in Cisco Wave 2 APs for DNS-based ACLs on FlexConnect APs with Local Switching.

- If a client is anchored, be it auto-anchor or after roaming, DNS-based ACLs do not work.

Configuring DNS-based Access Control Lists (CLI)

Procedure

Step 1 Specifies to create ACL. You can enter an IPv4 ACL name up to 32 alphanumeric characters.

config acl create *name*

Example:

```
(Cisco Controller) > config acl create android
```

Step 2 Specifies to add a new URL domain for the access control list. URL domain name should be given in a valid format, for example, Cisco.com, bbc.in, or play.google.com. The hostname comparison is a sub string matched (wildcard based). You must use the ACL name that you have created already.

config acl url-domain add *domain-name acl-name*

Example:

```
(Cisco Controller) > config acl url-domain add cisco.com android
(Cisco Controller) > config acl url-domain add play.google.com android
```

Step 3 Specifies to delete an existing URL domain for the access control list.

config acl url-domain delete *domain-name acl-name*

Example:

```
(Cisco Controller) > config acl url-domain delete cisco.com android
```

Step 4 Specifies to apply the ACL.

config acl apply *acl-name*

Example:

```
(Cisco Controller) > config acl apply android
```

Step 5 Displays DNS-based ACL information by entering this command:

show acl summary

Example:

```
(Cisco Controller) > show acl summary

ACL Counter Status              Disabled
---------------------------------------
IPv4 ACL Name                    Applied
-------------------------------- -------
android                          No
StoreACL                         Yes
---------------------------------------
IPv6 ACL Name                    Applied
-------------------------------- -------
```

Step 6 Displays detailed DNS-based ACL information by entering this command:

show acl detailed *acl-name*

Example:

```
(Cisco Controller) > show acl detailed android
o rules are configured for this ACL.
DenyCounter : 0
URLs configured in this ACL
---------------------------
*.play.google.com
*.store.google.com
```

Step 7 Displays the IP addresses per client learned through DNS snooping (DNS-based ACL) by entering this command:

show client detail *mac-address*

Example:

```
(Cisco Controller) > show client detail mac-address
```

Step 8 Enables debugging of information related to DNS-based ACL.

debug aaa events enable

Example:

```
(Cisco Controller) > debug aaa events enable
```

Configuring DNS-based Access Control Lists (GUI)

Procedure

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, check 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 Select the ACL type as IPv4.

Step 6 Click **Apply**.

Step 7 When the **Access Control Lists** page reappears, click the name of the new ACL. The ACLs have no IP rules. Hover your cursor over the blue drop-down arrow, choose **Add-Remove URL** from the drop-down list to open the URL List page.

Step 8 To add a new URL domain for an ACL, enter the new URL domain for the access control list in the **URL String Name** text box. The URL domain name should be given in a valid format, for example, Cisco.com or play.google.com.

Step 9 To delete an URL domain, hover your cursor over the blue drop-down arrow under the URL Name you want to delete, and select **Delete**.

URL Filtering

URL filtering feature allows you to control access to websites. It does so by permitting or denying access to specific websites based on information contained in a URL access control list (ACL). The URL filtering then restricts access based on the ACL.

Using location-based filtering, APs are grouped under various AP groups and WLAN profiles separate trusted and non-trusted clients within the same SSID. This forces reauthentication and new VLAN when a trusted client moves to a non-trusted AP or vice-versa.

Controllers support up to 64 ACLs. These ACLs are configured to either permit or deny requests, and can be associated with different interfaces (ex: WLAN, LAN), thus increasing effective filtering. Policies can be implemented locally on a WLAN or an AP group that is different from the applied global policy.

The following is the policy priority order:

1. Policy
2. Interface
3. WLAN

The number of rules (URLs) supported in each ACL varies for different controllers:

- Cisco 5520, 8540 Wireless Controllers support 100 rules in one ACL.

This section contains the following subsections:

Restrictions for URL Filtering

- URL filtering is not supported in the following controllers:
  - Cisco vWLC
  - Cisco Mobility Express
- This feature is supported only on WLAN central switching and not local switching.
- Not supported in FlexConnect mode with local switching.
- The following types of URLs are not supported:
  - Wildcard URLs (ex: www.uresour*loc.com).
  - Sub-URL (ex: www.uresour*loc.com/support).
  - Sub-Domain (ex: reach.url.com or sub1.url.com)
- URL name is limited to 32 characters in length.
- No AVC Profile for the matched URLs. ACL Actions support for the Matched URLs.
- Allowed list and blocked list can be created using the "*" implicit rule in the ACL to permit or deny requests respectively.
- Only HTTP URLs are supported.
- RADIUS server returning URL filtering ACL name is not supported.
- ACL might fail to filter in the following situations:
  - URL is across fragmented packets.
  - IP packets are fragmented.
  - Direct IP address or proxy setup used instead of URL.

Configuring URL Filtering (GUI)

Configuring Access Control Lists (GUI)

To create or delete access control lists in an WLAN.

Procedure

Step 1 Choose **Security** > **Access Control Lists** > **URL ACLs** to open the URL Access Control Lists page.

Step 2 Select the **Enable URL Acl** check box to enable the URL ACL feature.

Step 3 Add a new ACL by clicking **New**. The **URL Access Control Lists** > **New** page appears.
In the URL ACL Name text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 4 Click **Apply**.

- Repeat this procedure to add any additional URL ACLs.
- To delete any URL ACL, in the URL Access Control Lists page, hover the mouse cursor over the blue drop-down arrow for that ACL and choose **Remove**.

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**.

Configuring an URL ACL List (GUI)

Configuring rules in an URL ACL List.

Procedure

Step 1 Choose **Security** > **Access Control Lists** > **URL ACLs** to open the URL Access Control Lists page

Step 2 Choose the URL ACL.

URL Access Control Lists > **Edit**page appears.

Step 3 Choose **Add New Rule**.

Step 4 Configure a rule for this ACL from the drop-down menu.

- Rule Index—range between 1 and 100.
- URL—enter the URL address.
- Action—select Permit or Deny.

Step 5 Click **Apply**.

Repeat this procedure to add any additional rules.

Note

To have seamless access to websites which use different port number instead of default port 80, you will need to create a rule which includes the port number in URL-name:Port format. Example: Enter the URL as website.com:8080 and apply permit action.

Applying a URL Filtering Access Control List Globally (GUI)

Applying the URL ACL to the entire network.

Procedure

Step 1 Choose **Security** > **Local Policies** to open the local policy page.

Step 2 Choose the desired policy.

Policy > **Edit**page appears.

Step 3 Enter the **Match Role String** in the text box.

Step 4 Select the URL ACL from the **URL ACL** drop-down list.

Step 5 Click **Apply**.

Note
The **Match Role String** name should match the role name in Cisco AV pair.

Applying a URL Filtering Access Control List to an Interface (GUI)

Applying the URL ACL to an interface in the network.

Procedure

Step 1 Choose **Controller** > **Interfaces** to open the interface page.

Step 2 Choose the desired interface.

The interface page for the selected interface appears.

Step 3 Select the URL ACL from the **URL ACL** drop-down list.

Step 4 Click **Apply**.

Applying a URL Filtering Access Control List for a WLAN (GUI)

Applying the URL ACL to a WLAN in the network.

Procedure

Step 1 Choose **WLANs** to open the WLAN page.

Step 2 Click the ID number of the desired WLAN.

The **WLANs** > **Edit** page appears.

Step 3 Choose the **Advanced** tab.

Step 4 From the **URL ACL** drop-down list, choose the ACL that you want to apply to this WLAN.

Step 5 Click **Apply**.

Mapping the policy to a WLAN (GUI)

Mapping the policy to a WLAN in the network.

Procedure

Step 1 Choose **WLANs** to open the WLAN page.

Step 2 Click the ID number of the desired WLAN.

The **WLANs** > **Edit** page appears.

Step 3 Choose the **Policy-Mapping** tab.

a. Enter the **`Priority Index`** value.

b. Choose the local policy from the **Local Policy** drop-down list.

c. Click **Add**.

Step 4 Click **Apply**.

To delete a Policy-Mapping in a WLAN (GUI)

This procedure helps delete the policy-mapping in a WLAN.

Procedure

Step 1 Choose **WLANs** to open the WLAN page.

Step 2 Click the ID number of the desired WLAN.

The **WLANs** > **Edit** page appears.

Step 3 Hover the mouse cursor over the blue drop-down arrow for that local policy

Step 4 Choose **Remove**

The confirmation box appears.

Step 5 Click **OK**.

Step 6 Click **Apply**.

Mapping the policy to an AP Group (GUI)

Mapping the policy to an AP Group in the network.

Procedure

Step 1 Choose **WLANs** to open the WLAN page.

Step 2 Choose **Advanced** > **AP Groups**.

Step 3 Choose the **AP Group**.

The **AP Groups** > **Edit** page appears.

Step 4 Choose the **WLANs** tab.

Step 5 Hover the mouse cursor over the blue drop-down arrow of the required WLAN, select **Policy-Mapping**.

Step 6 In the **AP Group** > **Policy** > **Mappings** page.

a. Enter the **`Priority Index`** value.

b. Choose the local policy from the **Local Policy** drop-down list.

c. Click **Add**.

Step 7 Click **Apply**.

The WLAN and AP Group are Local Role based policies.

Configuring URL Filtering (CLI)

Configuring URL Filtering (CLI)

Procedure

Step 1 Configure the URL based Filtering feature by entering this command:
config acl url-acl {**enabled** | **disable**}

Step 2 Create or delete a URL ACL by entering this command:
config acl url-acl {**create** | **delete**} *id-token*

Step 3 Apply the URL ACL to the data path by entering this command:
config acl url-acl apply *acl-name*

Step 4 Configure an acl to an interface by entering this command:

config interface url-acl *interface-name acl-name*

Step 5 Configure an acl to a WLAN by entering this command:
config wlan url-acl *wlan-id acl-name*

Configuring Access Control List Rules (CLI)

Procedure

Step 1 Create or delete a ACL by entering this command:
config acl url-acl rule { **add | delete** } *acl-name index*

Step 2 Configure the URL address in a valid format (example: www.cisco.com) by entering this command:
config acl url-acl rule url *acl-name index url-name*

Step 3 Configure the action of the rule by entering this command:
config acl url-acl rule action *acl-name index* { **permit | deny** }

Note
To have seamless access to websites which use different port number instead of default port 80, you will need to create a rule which includes the port number in URL-name:Port format. Example: enter the URL as website.com:8080 and apply permit action.

Applying Local Policy (CLI)

Procedure

Step 1 Create or delete a local profiling policy by entering this command:
config policy *policy-name* { **create | delete** }

Step 2 Configure a match type to a policy by entering this command:
config policy *policy-name* **match role** { **role-name| none** }

Step 3 Configure an action to a policy by entering this command:
config policy *policy-name* **action url-acl** { **enable | disable** } *acl-name*

Step 4 Activate a local policy to a WLAN by entering this command:
config wlan policy add *priority-index policy-name wlan-id*

Step 5 Add or delete a local policy in an AP group in a WLAN by entering this command:
config wlan apgroup policy { **add | delete** } *priority-index policy-name ap-group-name wlan-id*

Viewing URL Filtering (CLI)

Procedure

- View ACL summary by entering this command:

  show acl url-acl summary

- View detailed URL ACL profile information by entering this command:

  show acl url-acl detailed *acl-name*

- View the details of a policy by entering this command:

  show policy {**summary** | *policy-name*}

- View client details by MAC address by entering this command:
  show client detail *mac-address*
- View the WLAN configuration details by entering this command:
  show wlan *wlan-id*
- View the interface details by entering this command:
  show interface detailed *interface-name*
- Clear the counters by entering this command:
  clear url-acl-counters

Troubleshooting URL Filtering (CLI)

You can troubleshoot the URL Filtering feature by entering these commands:

Procedure

- **debug fastpath dump urlacldb** *aclid ruleindex dataplane*
- **debug fastpath dump stats** *dataplane*

  The dataplane options available are 0, 1, All.

- **debug fastpath dump scbdb**

CNAME IPv6 Filtering

This feature enables the use of IPv6 address via FQDN in the network to authenticate the client traffic via controller and external AAA server. The client pre-authentication can be configured to use internal or external URL ACLs.

For the feature to function, you must set the SSID to central switching and the APs to local mode.

Restrictions for CNAME IPv6 Filtering

- Supported only on Cisco 3504, 5520, and 8540 Wireless Controllers.
- Maximum supported ACLs are 64.
- Maximum supported rules in an ACL are 20.

- Total number of resolved IPs is 40.
- CNAME parsing in different packets is not supported.
- AP in FlexConnect mode is not supported.

Configuring CNAME URL ACL (GUI)

Procedure

Step 1 Choose **Security** > **Access Control Lists** > **URL ACLs** to open the URL Access Control Lists page.

Step 2 Add a new ACL by clicking **New**.

The **URL Access Control Lists** > **New** page appears. In the **URL ACL Name** field, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 3 Click the URL ACL name that you want to configure.

Step 4

Note
You can add the FQDN of the IPv6 server in the pre-authentication IPv4 ACL in the controller so that the AAA server can allow or deny the requested traffic to the client.

Click **Add New Rule**.

Step 5 Configure a rule for this ACL from the drop-down list.

- Rule Index—range between 1 and 100.
- URL—enter the URL address.

  Note
  To use a IPv6 address, add the FQDN of the server address.

Step 6 Click **Apply**.

Repeat this procedure to add any additional rules in the URL ACL.

Step 7 To delete any rule within a URL ACL, in the **URL Access Control Lists > Edit** page, hover the mouse cursor over the blue drop-down arrow for that ACL and choose **Remove**.

Step 8 To delete any URL ACL, in the URL Access Control Lists page, hover the mouse cursor over the blue drop-down arrow for that ACL and choose **Remove**.

Step 9 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**.

Configuring Web Authentication for CNAME IPv6 Filtering on a WLAN (GUI)

Procedure

Step 1 Select **Security** > **Authentication** tab.
Step 2 Click **New** to add a new RADIUS server or click the **Server Index** of an existing server.
Step 3 Choose **Enable** from the **Support for CoA** drop-down list.
Step 4 Choose **WLAN** > **WLAN ID** > **Security** > **Layer 3** to open the Layer 3 page.
Step 5 Choose **Web Policy** from the **Layer 3 Security** drop-down list.
Step 6 Choose the URL ACL from the **Preauthentication ACL IPv4** drop-down list.
Step 7 Click **Apply**.

Configuring Web Authentication for CNAME IPv6 Filtering Using External RADIUS Server (GUI)

Procedure

Step 1 Select **Security** > **Authentication** tab.
Step 2 Click **New** to add a new RADIUS server or click the **Server Index** of an existing server.
When adding a new RADIUS server, enter appropriate details in the fields.
Step 3 Choose **Enable** from the **Support for CoA** drop-down list.
Step 4 Choose **WLAN** > **WLAN ID** > **Advanced** to open the advanced page.
Step 5 Choose **ISE NAC** from the **NAC State** drop-down list.
Step 6 Click **Apply**.

Configuring IPv6 CNAME Filtering (CLI)

Procedure

- Create a URL ACL by entering this command:
  config acl create *acl-name*
- Add a URL rule in a URL ACL by entering this command:
  config acl URL-domain add *domain-name acl-name*
- Enable a URL ACL by entering this command:
  config acl apply *acl-name*
- View the ACL summary by entering this command:

show acl summary

- View detailed ACL profile statistics by entering this command:

  show acl detailed *acl-name*

Domain-based Filtering

This feature allows you to control access to websites by permitting or denying access to websites using DNS-based access control list (ACL).

Cisco 3504, 5520, and 8540 Wireless Controllers support up to 64 ACLs. These ACLs are configured to either permit or deny traffic based on allowed list or blocked list on any protocol. Hence when a URL request is blocked, access is denied regardless of the protocol. An ACL can either be an allowed list (permit) or a blocked list (deny). Rules with an independent permit or deny settings are not supported within an ACL. Each ACL supports up to 100 rules (URLs).

Note By default, all the URLs that do not match the applied ACL are denied.

ACLs can be associated with different interfaces (for example: WLAN, LAN, and so on) using the following priority:

1. Role-based Policy
2. Interface
3. WLAN

Note Policies can be implemented locally on a WLAN or on an AP group that is different from the applied global policy.

This section contains the following subsections:

Restrictions on Domain-based Filtering

- The following are not supported:
  - vWLC
  - Mobility Express
- Supported only on WLAN Central Switching.
- Not supported on Local switching or FlexConnect mode with local switching.
- ACLs can have a maximum of 10 wildcard URLs (for example: *.example.com) and 5 sub-domains per wildcard (for example: sub.example.com).
- Sub-URL are not allowed (for example: www.example.com/support).

- URL name is limited to a maximum of 255 characters.
- Direct IP address access is blocked in the allowed list. However, it is not blocked in the blocked list.
- Layer 2 roaming is not supported.
- IPv6 is not supported.
- RADIUS server returning URL filtering ACL name is not supported.
- ACL may fail to filter in the following situations:
  - URL is across fragmented packets
  - IP packets are fragmented

Configuring Domain-based Filtering (GUI)

Configuring Access Control Lists (GUI)

Configuring rules in a URL ACL List.

Procedure

Step 1 Choose **Security** > **Access Control Lists** > **URL ACLs** to open the URL Access Control Lists page

Step 2 Choose the URL ACL.

URL Access Control Lists > **Edit** page appears.

Step 3 Choose **Add New Rule**.

Step 4 Configure a rule for this ACL as follows

- Rule Index – Range between 1 and 100
- URL—Enter the URL address.
- Action—Select **Permit** or **Deny**.

Step 5 Click **Apply**.

Repeat this procedure to add any additional rules.

Note
To have seamless access to websites which use a different port number instead of the default port 80, create a rule which includes the port number in URL-name: Port format. Example: Enter the URL as website.com:8080 and apply permit action.

Creating a URL ACL List (GUI)

To create or delete access control lists in a WLAN.

Procedure

Step 1 Choose **Security** > **Access Control Lists** > **URL ACLs** to open the URL Access Control Lists page.

Step 2 Select the **Enable URL Acl** check box to enable the URL ACL feature.

Step 3 Add a new ACL by clicking **New**. The **URL Access Control Lists** > **New** page appears.
In the URL ACL Name text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 4 Click **Apply**.

- Repeat this procedure to add any additional URL ACLs.
- To delete any URL ACL, in the URL Access Control Lists page, hover the mouse cursor over the blue drop-down arrow for that ACL and choose **Remove**.

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**.

Applying a URL Filtering Access Control List Globally (GUI)

Applying the URL ACL to the entire network.

Procedure

Step 1 Choose **Security** > **Local Policies** to open the local policy page.

Step 2 Choose the desired policy.

Policy > **Edit** page appears.

Step 3 Enter the **Match Role String** in the text box.

Step 4 Select the URL ACL from the **URL ACL** drop-down list.

Step 5 Click **Apply**.

Note
The **Match Role String** name must match the role name in the Cisco AV pair.

Applying a URL Filtering Access Control List to an Interface (GUI)

Applying the URL ACL to an interface in the network.

Procedure

Step 1 Choose **Controller** > **Interfaces** to open the interface page.

Step 2 Choose the desired interface.

The interface page for the selected interface appears.

Step 3 Select the URL ACL from the **URL ACL** drop-down list.

Step 4 Click **Apply**.

Applying a URL Filtering Access Control List for a WLAN (GUI)

Applying the URL ACL to a WLAN in the network.

Procedure

Step 1 Choose **WLANs** to open the WLAN page.

Step 2 Click the ID number of the desired WLAN.

The **WLANs** > **Edit** page appears.

Step 3 Choose the **Advanced** tab.

Step 4 From the **URL ACL** drop-down list, choose the ACL that you want to apply to this WLAN.

Step 5 Click **Apply**.

Mapping the Policy to a WLAN (GUI)

Mapping the policy to a WLAN in the network.

Procedure

Step 1 Choose **WLANs** to open the WLAN page.

Step 2 Click the ID number of the desired WLAN.

The **WLANs** > **Edit** page appears.

Step 3 Choose the **Policy-Mapping** tab.

a. Enter the **`Priority Index`** value.

b. Choose the local policy from the **Local Policy** drop-down list.

c. Click **Add**.

Step 4 Click **Apply**.

To Delete a Policy-Mapping in a WLAN (GUI)

This procedure helps delete the policy-mapping in a WLAN.

Procedure

Step 1 Choose **WLANs** to open the WLAN page.

Step 2 Click the ID number of the desired WLAN.

The **WLANs** > **Edit** page appears.

Step 3 Hover the mouse cursor over the blue drop-down arrow for that local policy

Step 4 Choose **Remove**

The confirmation box appears.

Step 5 Click **OK**.

Step 6 Click **Apply**.

Mapping the Policy to an AP Group (GUI)

Mapping the policy to an AP Group in the network.

Procedure

Step 1 Choose **WLANs** to open the WLAN page.

Step 2 Choose **Advanced** > **AP Groups**.

Step 3 Choose the **AP Group**.

The **AP Groups** > **Edit** page appears.

Step 4 Choose the **WLANs** tab.

Step 5 Hover the mouse cursor over the blue drop-down arrow of the required WLAN, select **Policy-Mapping**.

Step 6 In the **AP Group** > **Policy** > **Mappings** page.

a. Enter the **`Priority Index`** value.

b. Choose the local policy from the **Local Policy** drop-down list.

c. Click **Add**.

Step 7 Click **Apply**.

The WLAN and AP Group are Local Role based policies.

Configuring Domain Based Filtering (CLI)

Configuring URL Filtering (CLI)

Procedure

Step 1 Configure the URL-based Filtering feature by entering this command:
config acl url-acl {**enabled | disable**}

Step 2 Create or delete a URL ACL by entering this command:
config acl url-acl{ **create | delete**} *id-token*

Step 3 Apply the URL ACL to the data path by entering this command:
config acl url-acl apply*acl-name*

Step 4 Configure an acl to an interface by entering this command:
config interface url-acl *interface-name acl-name*

Step 5 Configure an acl to a WLAN by entering this command:
config wlan url-acl *wlan-id acl-name*

Configuring Access Control List Rules (CLI)

Procedure

Step 1 Create or delete an ACL by entering this command:
config acl url-acl rule{ **add | delete**} *acl-name index*

Step 2 Configure the URL address in a valid format (example: www.cisco.com) by entering this command:
config acl url-acl rule url*acl-name index url-name*

Step 3 Configure the action of the rule by entering this command:
config acl url-acl rule action *acl-name index*{ **permit | deny**}

Note
To have seamless access to websites which use a different port number instead of the default port 80, create a rule which includes the port number in URL-name: Port format. Example: enter the URL as website.com:8080 and apply permit action.

Step 4 Configure the allowed list or blocked list ACL by entering this command:
config acl url-acl list-type *acl-name* {*whitelist* | *blacklist*}

Step 5 Configure the external server to the redirect the web page requests by entering this command:
config acl url-acl external-server-ip *ip-address*

Related Topics
Configuring FlexConnect Access Control Lists (CLI), on page 1228

Applying Local Policy (CLI)

Procedure

Step 1 Create or delete a local profiling policy by entering this command:
config policy *policy-name* {**create | delete**}

Step 2 Configure a match type to a policy by entering this command:
config policy *policy-name* **match role** {**role-name| none**}

Step 3 Configure an action to a policy by entering this command:
config policy *policy-name* **action url-acl** {**enable | disable**} *acl-name*

Step 4 Activate a local policy to a WLAN by entering this command:
config wlan policy add *priority-index policy-name wlan-id*

Step 5 Add or delete a local policy in an AP group in a WLAN by entering this command:
config wlan apgroup policy {**add | delete**} *priority-index policy-name ap-group-name wlan-id*

Viewing URL Filtering (CLI)

Procedure

- View ACL summary by entering this command:
  show acl url-acl summary
- View detailed URL ACL profile information by entering this command:
  show acl url-acl detailed *acl-name*
- View the details of a policy by entering this command:
  show policy {**summary**|*policy-name*}
- View client details by MAC address by entering this command:
  show client detail *mac-address*
- View the WLAN configuration details by entering this command:
  show wlan *wlan-id*
- View the interface details by entering this command:
  show interface detailed *interface-name*
- Clear the counters by entering this command:

clear url-acl-counters

Troubleshooting URL Filtering (CLI)

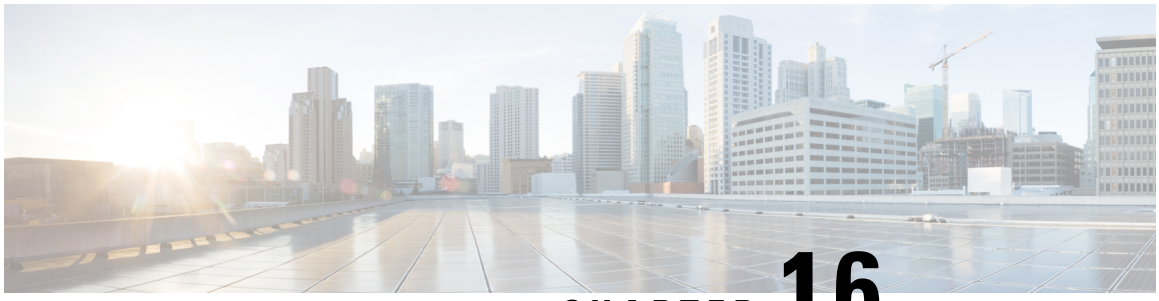
You can troubleshoot the URL Filtering feature by entering these commands:

Procedure

- **debug fastpath dump urlacldb** *aclid ruleindex dataplane*
- **debug fastpath dump stats** *dataplane*

  The dataplane options available are 0, 1, All.

- **debug fastpath dump scbdb**



CHAPTER 16

Multicast/Broadcast Setup

- Multicast/Broadcast Mode, on page 281
- Media Stream, on page 288
- Multicast Domain Name System, on page 296

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 are 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.
- 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.
- 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 11: Platform Support for Global Multicast and Multicast Mode

Platform	Global Multicast	Multicast Mode	Supported
Cisco 5520 and 8540 Controllers	Enabled	Unicast	No
	Enabled	Multicast	Yes
	Disabled	Unicast	No multicast support (config supported)
	Disabled	Multicast	No multicast support (config supported)
Cisco vWLC	Multicast is not supported; only Unicast mode is supported.		

Platform	Global Multicast	Multicast Mode	Supported
Cisco 3504 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)

Procedure

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)

Procedure

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)

Procedure

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)

Procedure

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.

Procedure

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*

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

For more information about deploying Media Stream, see:https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/112889-cuwns-vidstrm-guide-00.html

This section contains the following subsections:

Prerequisites for Media Stream

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

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

Verify that the access points have joined the controllers.

Make sure that the clients are able to associate to the configured WLAN at 802.11n speed.

Restrictions for Configuring Media Stream

- Media Stream is supported in the 7.0.98.0 and later controller software releases.
- To enforce the EDCA parameter changes on an AP, all clients must be disconnected irrespective of the radio to which they are connected. This requires that all WLANs must also be disabled. For more information about this, see CSCvq29269.

Configuring Media Stream (GUI)

Procedure

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)

Procedure

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

Configuring Media Parameters (GUI)

Procedure

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.

Viewing and Debugging Media Stream

Procedure

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}

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.

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.
- 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.
- mDNS-AP feature is not supported in CAPWAP V6.
- ISE dynamic mDNS policy mobility is not supported.
- mDNS user profile mobility is not supported in guest anchors.

Configuring Multicast DNS (GUI)

Procedure

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 controller supports Bonjour gateway functionality on controller itself for which you need not even enable multicast on the controller. The controller 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 controller 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.

Configuring mDNS Service Groups (GUI)

Procedure

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)

Procedure

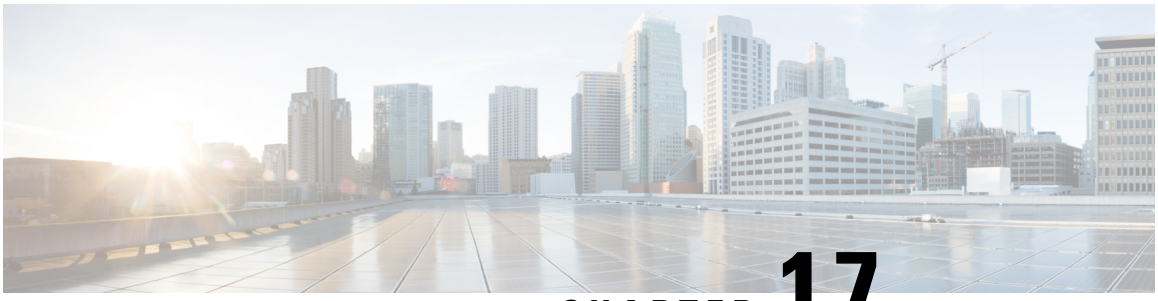
Step 1 Enable or disable the mDNS policy by entering this command: **config mdns policy enable | disable**

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*>



CHAPTER 17

Controller Security

- FIPS, CC, and UCAPL, on page 307
- Cisco TrustSec, on page 313
- IPSec Profile, on page 333

FIPS, CC, and UCAPL

This section contains the following subsections:

FIPS

Federal Information Processing Standard (FIPS) 140-2 is a security standard used to validate cryptographic modules. The cryptographic modules are produced by the private sector for use by the U.S. government and other regulated industries (such as financial and healthcare institutions) that collect, store, transfer, share and disseminate sensitive but unclassified (SBU) information.

Note Cisco TrustSec (CTS) is not supported when the controller is in FIPS mode.

For more information about FIPS, see

https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html.

FIPS Self-Tests

A cryptographic module must perform power-up self-tests and conditional self-tests to ensure that it is functional.

Power-up self-tests run automatically after the device powers up. A device goes into FIPS mode only after all self-tests are successfully completed. If any self-test fails, the device logs a system message and moves into an error state. Also, if the power-up self test fails, the device fails to boot.

Using a known-answer test (KAT), a cryptographic algorithm is run on data for which the correct output is already known, and then the calculated output is compared to the previously generated output. If the calculated output does not equal the known answer, the known-answer test fails.

Power-up self-tests include the following:

- Software integrity
- Algorithm tests

Conditional self-tests must be run when an applicable security function or operation is invoked. Unlike the power-up self-tests, conditional self-tests are executed each time their associated function is accessed.

The device uses a cryptographic algorithm known-answer test (KAT) to test FIPS mode for each FIPS 140-2-approved cryptographic function (encryption, decryption, authentication, and random number generation) implemented on the device. The device applies the algorithm to data for which the correct output is already known. It then compares the calculated output to the previously generated output. If the calculated output does not equal the known answer, the KAT fails.

Conditional self-tests run automatically when an applicable security function or operation is invoked. Unlike the power-up self-tests, conditional self-tests are executed each time their associated function is accessed.

Conditional self-tests include the following:

- Pair-wise consistency test—This test is run when a public or private key-pair is generated.
- Continuous random number generator test—This test is run when a random number is generated.
- Bypass
- Software load

Information About CC

Common Criteria (CC) is a testing standard to verify that a product provides security functions that are claimed by its developer. CC evaluation is against a created protection profile (PP) or security target (ST).

The four security levels in FIPS 140–2 do not map directly to specific CC EALs or CC functional requirements. For more information about CC, see Common Criteria Portal and CC evaluation and validation scheme.

To configure the controller into CC mode of operation, refer the *Admin Guidance Document* published on the Certified Product page of the Common Criteria Portal website.

After providing CC for the controller, the controller series name is listed in the Common Criteria Portal. Click the **Security Documents** tab to view the list of documented available for the controller.

Information About UCAPL

The US Department of Defense (DoD) Unified Capabilities Approved Product List (APL) certification process is the responsibility of the Defense Information Systems Agency (DISA) Unified Capabilities Certification Office (UCCO). Certifications are performed by approved distributed testing centers including the Joint Interoperability Test Command (JITC).

DoD customers can only purchase unified capabilities related equipment, both hardware and software, that has been certified. Certified equipment is listed on the DoD UC APL. UC APL certifications verify the system complies with and is configured consistent with the DISA Field Security Office (FSO) Security Technical Implementation Guides (STIG).

For more information about the UC APL process, see Defense Information System Agency.

Guidelines on UCAPL

- In UCAPL web authentication login, multifactor authentication, which includes client (browser) certificate validation and user authentication, is performed; Certificate validation prior to user authentication is mandatory. Certificate validation is part of DTLS handshake, which is performed only once for a session till its lifetime (default session lifetime is 5 minutes). When a user tries to login again, certificate validation is not performed because the old session is not yet flushed and user authentication is not performed without certificate validation. For more information, see https://tools.ietf.org/html/rfc5246.
- UCAPL certification requires a maximum of three unsuccessful login attempts to SSH. With some SSH clients, fourth attempts are also observed; however, controller does not accept the fourth attempt even if the credentials are correct.

Configuring FIPS (CLI)

Procedure

Step 1 Configure FIPS on the controller by entering this command:
config switchconfig fips-prerequisite {**enable** | **disable** }

In FIPS mode both TLSv1.0 and TLSv1.2 are supported and only FIPS 140-2 compliant algorithms are used.

Step 2 View the FIPS configuration by entering this command:
show switchconfig

Information similar to the following appears:

```
802.3x Flow Control Mode..................... Disable
FIPS prerequisite features................... Enabled
WLANCC prerequisite features................. Enabled
UCAPL prerequisite features.................. Disabled
secret obfuscation........................... Enabled
```

Configuring CC (CLI)

Before you begin

FIPS must be enabled on the controller.

Procedure

Step 1 Configure FIPS on the controller by entering this command:
config switchconfig wlancc {**enable** | **disable** }

Step 2 View the FIPS configuration by entering this command:
show switchconfig

Information similar to the following appears:

```
802.3x Flow Control Mode..... Disable
FIPS prerequisite features..... Enabled
WLANCC prerequisite features..... Enabled
UCAPL prerequisite features..... Disabled
secret obfuscation..... Enabled
```

Configuring UCAPL (CLI)

Before you begin

FIPS and WLAN CC must be enabled on the controller.

Procedure

Step 1 Configure UCAPL on the controller by entering this command:
config switchconfig ucapl {**enable** | **disable** }

Step 2 View the FIPS configuration by entering this command:
show switchconfig

Information similar to the following appears:

```
802.3x Flow Control Mode..... Disable
FIPS prerequisite features..... Enabled
WLANCC prerequisite features..... Enabled
UCAPL prerequisite features..... Enabled
secret obfuscation..... Enabled
```

Preparing Controller in FIPS Mode for Management in Cisco Prime Infrastructure (CLI)

This is an update to the existing FIPS feature function. As per this update, when the controller is in FIPS mode or when the Cisco Prime Infrastructure (PI) is used for SNMP management, SNMP trap logger, and as a syslog server with IPsec, you must add the Cisco PI IP address in the controller before adding the controller IP address in the PI configuration.

Procedure

Step 1 Enable FIPS mode in controller

Note
Do not execute the optional steps (b, c) when using Cisco 3702E AP in the network.

Cisco Wave 1 APs (AP3702/AP2702/AP1702) support FIPS DTLS 1.0 with AES128-SHA1 or AES256-SHA256 only. WLAN Common Criteria (WLAN CC) requires DTLS 1.2 with Ephemeral Diffie-Hellman (DHE) cipher suite. Hence, these APs cannot join the controller with WLANCC enabled.

a) Configure FIPS on the controller by entering this command:

config switchconfig fips-prerequisite {**enable** | **disable**}

b) [Optional] Configure WLAN Common Criteria on the controller by entering this command:

config switchconfig wlancc {**enable** | **disable**}

c) [Optional] Configure UCAPL on the controller by entering this command:

config switchconfig ucapl {**enable** | **disable**}

d) Save the current configuration to the NVRAM by entering this command:

save config

e) Reboot the controller by entering this command:

reset system

Step 2 Configure the Cisco PI IP address to manage the controller by entering this command:

config snmp pi-ip-address *ip-address* {**add** | **delete**}

Note
The IP address is the Cisco PI eth0 interface IP address.

Step 3 Configure the IPSec profile.

a) Create the IPSec profile by entering this command:

config ipsec-profile {**create** | **delete** } *profile-name*

b) Configure the IPSec profile encryption by entering this command:

config ipsec-profile encryption {**aes-128-cbc | aes-256-cbc | aes-128-gcm | aes-256-gcm** } *profile-name*

c) Configure the IPSec profile authentication by entering this command:

config ipsec-profile authentication {**hmac-sha256 | hmac-sha384** } *profile-name*

d) Configure the IPSec life time in seconds by entering this command:

config ipsec-profile life-time-ipsec *life-time-ipsec seconds profile-name*

The valid range is between 1800 and 28800 seconds. Default is 1800 seconds.

e) Configure Internet Key Exchange (IKE) lifetime in seconds by entering this command:

config ipsec-profile life-time-ike *life-time-ipsec seconds profile-name*

The valid range is between 1800 and 86400 seconds. Default is 28800 seconds.

f) Configure the IPSec profile Internet Key Exchange (IKE) version by entering this command:

config ipsec-profile ike version {**1 | 2** } *profile-name*

Note
Currently only IKE version 1 is supported.

g) Configure the IKE authentication method by entering this command:

config ipsec-profile ike auth-mode certificate *profile-name*

h) Attach the IPSec profile to SNMP by entering this command:

config snmp community ipsec profile *profile-name*

i) Enable IPSec for SNMP by entering this command:

config snmp community ipsec enable

Step 4 Configure SNMP Trap Receiver.

a) Configure the IPSec profile to the Trap receiver by entering this command:

config snmp trapreceiver ipsec profile *profile-name trap-receiver-name*

b) Enable SNMP Traps over IPSec by entering this command:

config snmp trapreceiver ipsec enable *trap-receiver-name*

Step 5 Configure Syslog.

a) Configure the host IP for the syslog by entering this command:

config logging syslog host *ip address*

You can add up to three syslog servers to the controller.

b) Assign an IPSec profile to syslog by entering this command:

config logging syslog ipsec profile *profile-name*

c) Enable logging messages to syslog over IPSEC by entering this command:

config logging syslog ipsec enable

d) Deleting syslog server IP address by entering this command:

config logging syslog host *ip address* **delete**

Step 6 Disabling and unlinking the IPSec profile prior to editing the IPSec profile.

- SNMP
  - **a.** Disable—**config snmp community ipsec disable**
  - **b.** Unlink—**config snmp community ipsec none**
- Trap Receiver
  - **a.** Disable—**config snmp trapreceiver ipsec disable** *trapreceiver-name*
  - **b.** Unlink—**config snmp trapreciver ipsec profile none** *trapreceiver-name*
- Syslog
  - **a.** Disable—**config logging syslog ipsec disable**
  - **b.** Unlink—**config logging syslog ipsec profile none**

Step 7 View the active IPSec tunnel details by entering this command:

show ipsec status

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.

From Release 8.4, SXPv4 is supported in FlexConnect mode APs.

For more information about Cisco TrustSec, see http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html.

Environment Data

Cisco TrustSec environment data is a set of information or attributes that helps controller to perform Cisco TrustSec-related functions.

The controller acquires the environment data from the authentication server (Cisco ISE) when the controller first joins a Cisco TrustSec domain by sending a secure RADIUS Access request. The authentication server returns a RADIUS Access-Accept message with attributes, including environment expiry timeout attributes. This is the time interval that controls how often the Cisco TrustSec device must refresh its environment data.

Security Group Access Control List Policy Download

A Security Group is a group of users, endpoint devices, and resources that share access control policies. Security groups are defined by the administrator in the Cisco ISE. As new users and devices are added to the Cisco TrustSec domain, the authentication server assigns these new entities to the appropriate security groups. Cisco TrustSec assigns each of the security group a unique 16-bit number whose scope is global in a Cisco

TrustSec domain. The number of security groups in a wireless device is limited to the number of authenticated network entities. You do not have to manually configure the security group numbers.

After a device is authenticated, the Cisco TrustSec tags any packet that originates from that device with an SGT that contains the security group number of the device. The packet carries this SGT everywhere in the network, in the Cisco TrustSec header.

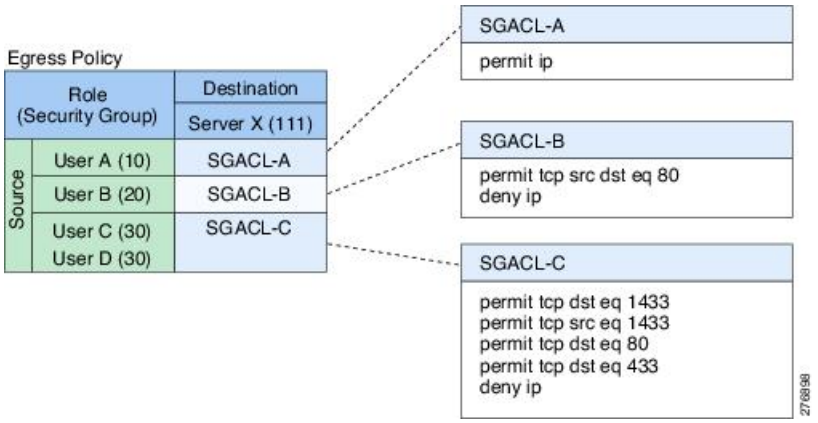
As the SGT contains the security group of the source, the tag can be referred to as the source SGT (S-SGT). The destination device is also assigned to a security group (destination SG) that can be referred to as the destination SGT (D-SGT), although the Cisco TrustSec packet does not contain the security group number of the destination device.

You can control the operations that users can perform based on the security group assignments of users and destination resources, using the Security Group Access Control Lists (SGACLs). Policy enforcement in a Cisco TrustSec domain is represented by a permission matrix, with the source security group on one axis and destination security group numbers on the other axis. Each cell in the matrix body contains an ordered list of SGACLs, which specifies the permissions that must be applied to packets originating from the source security group and destined for the destination security group. When a wireless client is authenticated, it downloads all the SGACLs in the matrix cells.

When a wireless client connects to the network, the client pushes all the ACLs to the controller.

This figure shows an example of a Cisco TrustSec permission matrix with three defined user roles, one defined destination resource, and three SGACL policies that control access to the destination server based on the user roles.

Figure 18: Example of an SGACL Policy Matrix



Cisco TrustSec achieves role-based topology-independent access control in a network by assigning users and devices in the network to security groups and applying access control between the security groups. The SGACLs define access control policies based on the device identities. As long as the roles and permissions remain the same, changes to the network topology do not change the security policy. When a user is added to the wireless group, you simply assign the user to an appropriate security group and the user immediately receives permissions to that group.

The size of ACLs is reduced and their maintenance is simplified with the use of role-based permissions. With Cisco TrustSec, the number of Access Control Entities (ACEs) configured is determined by the number of permissions that are specified, resulting in a much smaller number of ACEs.

Note By default, the following predefined SGACL policies are downloaded:

- Default policy—This is applied when source and destination SGTs are available, but SGACLs are not defined for a cell or column.
- Unknown policy—This is applied when the source SGT is unknown. You can use the session group named Unknown and apply the unknown policy on that traffic.

The following are examples of SGACLs that are on Cisco ISE and downloaded on a controller and tested:

Generic SGACL

- **Web_SGACL**

  permit tcp dst eq 80

  permit tcp dst eq 443

  deny ip
- **PCI_Servers_SGACL**

  deny tcp dst eq 4444

  deny tcp dst eq 4446

  deny tcp dst eq 443

  permit ip
- **PCI_Zone_SGACL**

  deny tcp dst eq 4444

  deny tcp dst eq 4446

  deny tcp dst eq 443

  permit ip
- **Deny_SSH_RDP_Telnet_SGACL**

  deny tcp dst eq 23

  deny tcp dst eq 23

  deny tcp dst eq 3389

  permit ip
- **Deny_JumpHost_Protocols**

  deny tcp dst eq 23

  deny tcp dst eq 23

  deny tcp dst eq 3389

  permit ip

Anti-Malware SGACLs

- **Anti-Malware-ACL**

deny icmp

deny udp src dst eq domain

deny tcp src dst eq 3389

deny tcp src dst eq 1433

deny tcp src dst eq 1521

deny tcp src dst eq 445

deny tcp src dst eq 137

deny tcp src dst eq 138

deny tcp src dst eq 139

deny udp src dst eq snmp

deny tcp src dst eq telnet

deny tcp src dst eq www

deny tcp src dst eq 443

deny tcp src dst eq 22

deny tcp src dst eq pop3

deny tcp src dst eq 123

deny tcp match-all -ack +fin -psh -rst -syn -urg

deny tcp match-all +fin +psh +urg

permit tcp match-any +ack +syn

Collaboration SGACLs

- **rbacl:Gateway_sig**

  permit udp dst eq 5060 log

  permit tcp dst eq 5060 log

  permit tcp dst eq 5061 log

  permit udp dst range 32768 61000

  permit tcp dst range 32768 61000

  deny ip log

- **rbacl:Intra_Jabber**

  permit udp dst range 16384 32767 log

  permit tcp dst range 49152 65535 log

  permit tcp dest eq 37200 log

  deny ip log

- **rbacl:Jabber_sig**

  permit tcp dst eq 6970 log

permit tcp dst eq 6972 log

permit tcp dst eq 3804 log

permit tcp dst eq 8443 log

permit tcp dst eq 8191 log

permit tcp dst eq 5222 log

permit tcp dst eq 37200 log

permit tcp dst eq 443 log

permit tcp dst eq 2748 log

permit tcp dst eq 5060 log

permit tcp dst eq 5061 log

permit tcp dst range 30000 39999 log

permit udp dst range 5070 6070 log

deny ip log

- **rbacl:Phone_sig**

  permit udp dst eq 69 log

  permit tcp dst eq 8080 log

  permit tcp dst eq 2445 log

  permit tcp dst eq 3804 log

  permit tcp dst eq 5060 log

  permit udp dst eq 5060 log

  permit tcp dst eq 5061 log

  permit tcp dst eq 6970 log

  deny ip log

- **rbacl:UC_endpoint_media**

  permit udp dst range 16384 32767 log

  deny ip log

Inline Tagging

Inline tagging is a transport mechanism using which a controller or a Cisco AP understands the source SGT. Transport mechanism is of two types:

- Central switching—For centrally switched packets, controller performs inline tagging for all the packets that are sourced from wireless clients that are associated with the controller by tagging it with the Cisco Meta Data (CMD) tag. For packets inbound from the Distribution System, inline tagging also involves controller stripping off the CMD header from the packet to learn the S-SGT tag. Controller thereafter forwards the packet including the S-SGT for SGACL enforcement.
- Local switching—To transmit locally switched traffic, Cisco AP performs inline tagging for packets that are associated with the Cisco AP and sourced from clients. To receive traffic, Cisco AP handles both

locally switched packets and centrally switched packets, uses an S-SGT tag for packets, and applies the SGACL policy.

With wireless Cisco TrustSec enabled on the controller, the choice of enabling and configuring SXP to exchange tags with the switches is optional. Both wireless Cisco TrustSec and SXP modes are supported; however, there is no use case to have both wireless Cisco TrustSec on AP and SXP to be in the enabled state concurrently.

Policy Enforcement

Cisco TrustSec access control is implemented using ingress tagging and egress enforcement. At the ingress point to the Cisco TrustSec domain, the traffic from the source is tagged with an SGT containing the security group number of the source entity. The SGT is propagated across the domain with the traffic. At the egress point of the Cisco TrustSec domain, an egress device uses the source SGT (S-SGT) and the security group of the destination entity (D-SGT) to determine the access policy to apply from the SGACL policy matrix.

You can apply policy enforcement to both central and local switched traffic on an AP. If wired clients communicate with wireless clients, the Cisco AP enforces the downstream traffic. If wireless clients communicate with wired clients, the Cisco AP enforces the upstream traffic. This way, the Cisco AP enforces traffic in both downstream and wireless-to-wireless traffic. You require S-SGT, D-SGT, and ACLs for enforcement to work. Cisco APs get the SGT information for all wireless clients from the information available on the Cisco ISE server.

Note A Cisco AP must be in either Listener or Both (Listener and Speaker) mode to enforce traffic as the Listener mode maintains the complete set of IP-SGT bindings. After you enable enforcement on a Cisco AP, the corresponding policies are downloaded and pushed to the Cisco AP.

Guidelines and Restrictions on Cisco TrustSec

- The configuration of the default password should be consistent for both the controller and the switch.
- 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.
- Cisco TrustSec (CTS) is not supported when the controller is in FIPS mode.
- Cisco TrustSec is not supported in L3 and Guest Access deployments.
- Cisco TrustSec in Monitor mode is not supported.
- Device or Multicast SGT and server list as part of environment data is not supported.

- Change of Authorization (CoA) for policy and environment data refresh is not supported.
- In a High Availability (HA) setup, environment data, and SGACLs are not synchronized with standby controllers. The PAC information and device ID and password are synchronized. Upon a controller failover, environment data and SGACLs are downloaded from Cisco ISE.

Note In an HA setup, when a client connects to an AP that is associated with the active controller, the AP-SGT information is updated in the standby controller. This AP-SGT mapping is used to download the SGT policy after an HA switchover. The policy is not synchronized with the standby controller. However, the AP-SGT information is used to initiate the policy download after the HA switchover.

Only the active controller can set create an SXP socket connection to the peer; The standby controller does not establish the SXP socket connection. Therefore, the SXP status in the standby controller is 'OFF'.

- When a controller running Release 8.4 or a later release becomes nonoperational, an AP associated with the controller might switch to another controller running Release 8.3 or an earlier release and download the image. Then, the AP cannot communicate with the controller because Release 8.3 and older releases do not support inline tagging. In this case, we recommend that you disable Cisco TrustSec manual configuration mode (**cts manual**) on the AP switchport so that the AP can download the image.
- The **policy static sgt** *tag* **trusted** command, in the Cisco TrustSec manual configuration mode, is used in an inline tagging enabled setup, when the AP switch port is required to trust the SGT tag set by the peer. In case of untagged traffic, the switch port tags all the packets with the value that is configured in this command. Therefore, this configuration must not be used when inline tagging is disabled.
- Static SGACL policy is not supported on controller.
- Policy enforcement is not applied to multicast traffic.
- Inline and SXPv4 are not supported in a FlexConnect split tunneling scenario.
- In a mixed-mode deployment scenario, if a Cisco AP is configured with two SXP peer connections, the password of one peer connection is set to *default* and the password of the other peer connection is set to *none*. In such a scenario, the peer connection with the password set to *none* will not be operational. However, if all the SXP peer connections are configured with the password *none*, the SXP peer connections are operational.
- To have a heterogeneous network consisting of Wave 1 and Wave 2 APs, configure the Cisco 3850 switch SGACL ACEs for TrustSec. If the Cisco 3850 switch is not used for TrustSec, then the network supports only a homogeneous network of either Cisco Wave 1 or Wave 2 APs.

Note ACLs are not applied to clients which are associated to unsupported TrustSec AP devices.

- Cisco TrustSec is not supported for Guest LAN clients.
- Cisco TrustSec is not supported on Outdoor and Industrial Wireless mesh APs.
- Cisco TrustSec is not supported in Cisco Wave 2 APs that are in Flex+Bridge mode.

- PAC provisioning is not supported on Cisco vWLC.
- PAC provisioning is not supported on a IPv6 server.
- Inline tagging and SGACL download and enforcement are not supported on Cisco vWLC.
- SXPv4 Listener and Both modes are not supported in FlexConnect deployments with Cisco vWLC.
- Inline tagging is not supported in Cisco Wave 2 APs that are in Flex+Bridge mode.
- We recommend that you do not use SXPv4 for a NAT scenario (FlexConnect Central DHCP).
- If you encounter the `CTS CORE: AAA-3-AUTH_REQUEST_QUEUE_FAILED` system message, no action is required. This is an expected error log after every controller reboot. This system message is displayed because the Cisco TrustSec core is initialized before AAA.

Cisco TrustSec Feature Support Matrix

Table 12: Cisco TrustSec Feature Support Matrix

AP Mode	SXPv4 Support	Inline Tagging Support	Enforcement Support	Cisco Aironet AP Series	Remarks
Local	No	No	Yes	1700, 2700, 3700	NA
				18*xx*, 38*xx*, 28*xx*	
FlexConnect	Yes	Yes	Yes	1700, 2700, 3700	NA
				18*xx*, 38*xx*, 28*xx*	
Flex+Bridge	Yes	No	Yes	1700, 2700, 3700	NA
	No	No	No	18*xx*, 38*xx*, 28*xx*	Flex+Bridge mode is not supported on these APs.
Mesh	No	No	Yes (Online for indoor mesh)	1700, 2700, 3700	No support for outdoor mesh
	No	No	No	18*xx*, 38*xx*, 28*xx*	Mesh mode is not supported.

Configuring Cisco TrustSec

Configuring Cisco TrustSec on Controller (GUI)

Procedure

Step 1 Choose **Security** > **TrustSec** > **General**.
The **General** page is displayed.

Step 2 Check the **CTS** check box to enable Cisco TrustSec. By default, Cisco TrustSec is in disabled state.

Step 3 Save the configuration.

Configuring Cisco TrustSec on Controller (CLI)

Procedure

- Enable Cisco TrustSec on the controller by entering this command:

  config cts enable

Note If you enable Cisco TrustSec, the SGACL is also enabled in the controller. Also, you will need to manually enable inline tagging.

Configuring Cisco TrustSec Override for an Access Point (CLI)

Procedure

- Enable or disable override of global Cisco TrustSec configuration on a specific AP by entering this command:

  config cts ap override {**enable** | **disable**} *cisco-ap*

SXP

Configuring SXP on Controller (GUI)

Procedure

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 controller. The controller 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 controller 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 controller.
- **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.

Configuring SXP on Controller (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.

Configuring SXP on Cisco Access Points (GUI)

This configuration is applicable to only FlexConnect, Flex+Bridge, Mesh, and Local mode APs.

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs** and the name of the desired access point.

Step 2 Click the **Advanced** tab.

Step 3 In the **Trusted Security** area, click **TrustSec Config**.
The **All APs** > **<ap-name>** > **Trusted Security** page is displayed.

Step 4 In the **Trusted Security** area, check the **SGACL Enforcement** check box.

Step 5 Save the configuration.

Configuring SXP on Cisco Access Points (CLI)

This configuration is applicable to only FlexConnect, Flex+Bridge, Mesh, and Local mode APs.

Procedure

- Enable or disable the SXP for an access point or all access points by entering this command:

  config cts sxp ap {**enable** | **disable**} {*ap_name* | **all**}

- Configure the default password for the SXP connection by entering this command:

  config cts sxp ap default password *password* {*ap-name* | **all**}

- Configure the SXP peer IP address with which a Cisco AP is connected by entering this command:

  config cts sxp ap connection peer *ip-address* **password** {**default** | **none**} **mode** {**both** | **listener** | **speaker**} {*ap-name* | **all**}

- Configure the minimum and maximum time intervals for the SXP connection to be alive by entering this command:

  config cts sxp ap listener hold-time *min max* {*ap-name* | **all**}

- Configure the reconciliation time interval on a Cisco AP by entering this command:

  config cts sxp ap reconciliation period *time-in-seconds* {*ap-name* | **all**}

- Configure the interval between connection attempts by entering this command:

  config cts sxp ap retry period *time-in-seconds* {*ap-name* | **all**}

- Configure the connection hold time by entering this command:

  config cts sxp ap speaker hold-time *hold-time-in-seconds* {*ap-name* | **all**}

Note If a Cisco AP with a DHCP IP is rebooted, associates with the controller after the reboot, and has a different IP address, the SXP connection fails. To overcome this, perform either of the following tasks:

- Define a reserved set of IP addresses in DHCP for the Cisco AP.
- Configure a static IP address for the Cisco AP.

Cisco TrustSec Credentials

Configuring Cisco TrustSec Credentials (GUI)

Procedure

Step 1 Choose **Security** > **TrustSec** > **General**.
The **General** page is displayed.

Step 2 In the **Device ID** field, enter the Cisco TrustSec device ID.

Step 3 In the **Password** field, enter the Cisco TrustSec device password.

Step 4 Check or uncheck the **Inline Tagging** check box to enable or disable inline tagging.

Step 5 In the **Environment Data** area, the following information is displayed:

- **Current State**—Shows whether the environment data is complete or not.
- **Last Status**—Shows the last state of the environment data.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Refresh Env Data** to refresh the environment data.

Configuring Cisco TrustSec Credentials (CLI)

Procedure

- Configure a Cisco TrustSec device ID and password by entering this command:

  config cts device-id *device-id* **password** *password*

Configuring a RADIUS AAA Server (GUI)

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.

Configuring RADIUS AAA Server (CLI)

Procedure

Configure a RADIUS authentication server to enable RADIUS PAC by entering the command:

config radius auth pac *srv-index* **enable**

Here *srv-index* specifies the RADIUS server index between 1 and 32.

Monitoring Environment Data

Monitoring Environment Data (GUI)

Procedure

Step 1 Choose **Security** > **TrustSec** > **General**.
The **General** page is displayed with the following details as part of Environment data: **Current State** and **Last Status**.

Step 2 To view the updated information, click **Refresh Env Data**.

Monitoring Environment Data (CLI)

Procedure

- View Cisco TrustSec environment data by entering this command:

  show cts environment-data

- Refresh Cisco TrustSec environment data by entering this command:

  config cts refresh environment-data

Note You must manually refresh the environment data from Cisco ISE because CoA is not supported in Cisco Wireless Release 8.4.

Configuring a Static Security Group Tag on a WLAN

Configuring a Static Security Group Tag on a WLAN (GUI)

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the WLAN ID.

Step 3 On the **WLANs** > **Edit** page, click the **Advanced** tab.

Step 4 Under the **TrustSec** area, in the **Security Group Tag** field, enter a value between 0 and 65533.

Step 5 Save the configuration.

Configuring a Static Security Group Tag on a WLAN (CLI)

Procedure

- Configure a static Security Group Tag (SGT) on a WLAN by entering this command:

  config wlan security sgt *value wlan-id*

  The valid range for *value* is between 0 and 65533.

Note This command is applicable for local and web authentication of clients in controller. The SGT also applies to clients that are connected to WLANs with AAA override disabled.

Configuring Inline Tagging

Configuring Inline Tagging in Controller (GUI)

Procedure

Step 1 Choose **Security** > **TrustSec** > **General**.
The **General** page is displayed.

Step 2 Check the **Inline Tagging** check box to enable inline tagging. By default, inline tagging is in disabled state.

Step 3 Save the configuration.

Configuring Inline Tagging in Controller (CLI)

Procedure

- Enable or disable inline tagging in the controller by entering this command:

  config cts inline-tag {**enable** | **disable**}

Note Controller performs the task of inline tagging for central switching packets.

Configuring Inline Tagging in Cisco Access Points (GUI)

Before you begin

1. Inline tagging is supported only on APs in FlexConnect mode.
2. By default, inline tagging is in disabled state.

Procedure

Step 1 To configure inline tagging on all APs:

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

b) Under the **TrustSec** area, click **TrustSec Config**.
The **All APs Trusted Security** page is displayed.

c) To enable inline tagging, check the **Inline Tagging** check box.

d) Click **Apply**.

Step 2 To configure inline tagging on a specific AP:

a) Choose **Wireless** > **Access Points** > **All APs**.

b) Click the name of the AP.
The **All APs > Details for <ap-name>** page is displayed.

c) Click the **Advanced** tab.
d) Under the **TrustSec** area, click **TrustSec Config**.
e) In the **Trusted Security** area, check the **Inline Tagging** check box to enable inline tagging.
f) Click **Apply**.

Configuring Inline Tagging in Cisco Access Points (CLI)

Before you begin

1. Inline tagging is supported only on APs in FlexConnect mode.
2. By default, inline tagging is in disabled state.

Procedure

- Enable or disable inline tagging on a specific AP or all APs by entering this command:

  config cts ap inline-tagging {*enable* | *disable*} {*Cisco AP* | **all**}

- See if a configuration is applied to a specific AP by entering this command:

  show ap config general {*Cisco AP*}

- See the status of inline tagging on all FlexConnect APs by entering this command:

  show cts ap summary

Note APs perform the task of inline tagging for local switching packets.

Verifying SGACL Policy Download

Verifying SGACL Policy Download in Controller (GUI)

Procedure

Step 1 Choose **Security** > **TrustSec** > **Policy**.

Step 2 Click a D-SGT.
The **SGT Detail** page is displayed with details of the SGT including the SGACL policy name.

Step 3 Click **Refresh** to refresh the SGT information.

Note
CoA is not supported. Therefore, we recommend that you manually refresh the SGACL policy from the Cisco ISE.

Verifying SGACL Policy Download in Controller (CLI)

Procedure

- View all or specific SGT policy information by entering this command:

  show cts policy {**all** | *sgt_tag*}

- View all or specific SGACL information by entering this command:

  show cts sgacl {**all** | *sgacl name*}

- Check if the SGACL is enabled or disabled for a specific AP by entering this command:

  show ap config general *cisco-ap*

- View the SGACL policy enabled globally by entering this command:

  show cts ap summary

- Refresh all SGTs by entering this command:

  config cts refresh policy sgt all

- Refresh a specific SGT by entering this command:

  config cts refresh policy sgt *sgt-tag*

Note CoA is not supported. Therefore, we recommend that you manually refresh the SGACL policy from Cisco ISE.

Configuring Policy Enforcement

Configuring Policy Enforcement (GUI)

Before you begin

SGACL enforcement is supported only on Cisco 3504, 5520, and 8540 Wireless Controllers.

Procedure

Step 1 To configure policy enforcement in a specific Cisco AP:

a) Choose **Wireless** > **Access Points** > **All APs** to open the **All APs** page.
b) Click the AP name.
The **All APs > Details for <ap-name>** page is displayed.
c) Click the **Advanced** tab.
d) In the **Trusted Security** area, click **TrustSec Config**.
The **All APs > <ap-name> > Trusted Security** page is displayed.
e) In the **Trusted Security** area, check the **SGACL Enforcement** check box to enforce SGACL policies on the AP.

By default, SGACL enforcement is in disabled state.

f) Click **Apply**.

Step 2 To configure policy enforcement in all Cisco APs:

a) Choose **Wireless** > **Access Points** > **Global Configuration**.
b) In the **TrustSec** area, click **TrustSec Config**.
The **All APs Trusted Security** page is displayed.
c) Check the **SGACL Enforcement** check box to enforce SGACL policies on all APs.
d) Click **Apply**.

Configuring Policy Enforcement (CLI)

Procedure

- Enable the SGACL enforcement for a specific AP or all APs by entering this command:

  config cts ap sgacl-enforcement enable {*ap-name* | **all**}

Note If you enable SGACL enforcement for all APs, the configuration is applied on all APs, except the ones for which CTS override is enabled.

Debugging Cisco TrustSec in Controller (CLI)

Procedure

- Configure the debug options for Cisco TrustSec AAA by entering this command:

  debug cts aaa {**all** | **errors** | **events**} {**enable** | **disable**}

- Configure the debug options Cisco TrustSec authorization by entering this command:

  debug cts authz {**all** | **errors** | **events** | **aaa**} {**enable** | **disable**}

- Configure the debug options for Cisco TrustSec policy download over CAPWAP messages by entering this command:

  debug cts capwap {**all** | **errors** | **events** | **messages**} {**enable** | **disable**}

- Configure the debug options for Cisco TrustSec environment data by entering this command:

  debug cts env-data {**all** | **errors** | **events**} {**enable** | **disable**}

- Configure the debug options for Cisco TrustSec HA by entering this command:

  debug cts ha {**all** | **errors** | **events**} {**enable** | **disable**}

- Configure the debug options for Cisco TrustSec key store by entering this command:

  debug cts key-store {**enable** | **disable**}

- Configure the debug options for Cisco TrustSec PAC provisioning by entering this command:

  debug cts provisioning {**all** | **errors** | **events** | **packets**} {**enable** | **disable**}

- Configure the debug options for Cisco TrustSec SXP by entering this command:

  debug cts sxp {**all** | **errors** | **events** | **framework** | **message**} {**enable** | **disable**}

- Configure SGT debugging for up to 10 SGTs by entering this command::

  debug cts sgt *sgt-1…sgt-10*

- Display all the AP-SGT information by entering this command:

  show cts ap sgt-info

Cisco TrustSec Commands on Lightweight APs

Enter these commands in a lightweight AP console:

Procedure

- Show commands:
  a) Check the SXP connection status by entering this command:
     - On Cisco Aironet 1700, 2700, and 3700 Series APs: **show cts sxp connections brief**
     - On Cisco Aironet 18*xx*, 28*xx*, and 38*xx* Series APs: **show cts sxp connections**

  b) Check SXP bindings by entering this command:
     - On Cisco Aironet 1700, 2700, and 3700 Series APs: **show cts sxp sgt-map brief**
     - On Cisco Aironet 18*xx*, 28*xx*, and 38*xx* Series APs: **show cts sxp sgt-map**

  c) Check IP-SGT binding by entering this command:
     - On Cisco Aironet 1700, 2700, and 3700 Series APs for local switching only: **show cts role-based sgt-map all**
     - On Cisco Aironet 18*xx*, 28*xx*, and 38*xx* Series APs for local switching and central switching only: **show cts role-based sgt-map all**

  d) Check SGT for central switching clients by entering this command:

     show controllers {*dot11Radio0|1* | **begin** *SGT*}

  e) Check SGACLs for S-SGT and D-SGT by entering this command:

     show cts role-based permissions [**default** | **from** | **ipv4** | **ipv6** | **to** | *cr*]

  f) Check counter for given source and destination SGT by entering this command:

     show cts role-based counters [**default** | **from** | **ipv4** | **ipv6** | **to** | *cr*]

  g) Check ACEs for a given SGACL by entering this command:

     show access-lists *access-list-name*

- Debug commands:
  a) Debug Cisco TrustSec enforcement by entering this command:

     On Cisco Aironet 18*xx*, 28*xx*, and 38*xx* Series APs: **debug cts enforcement**

b) Debug enforcement related issues, for both central and local switched data traffic. by entering this command:

On Cisco Aironet 1700, 2700, and 3700 Series APs: **debug rbm dp packets**

IPSec Profile

Configuring an IPSec Profile (GUI)

Procedure

Step 1 Choose **Management** > **IPSec** to navigate to the **IPSec Profile Name** page.

Step 2 Click **New** and enter a name for the IPSec profile.

Step 3 In the **IPSec Profile Name** listing, click the newly created IPSec profile name to configure the profile parameters.

Step 4 Enter the **IKE Version**. Supported Internet Key Exchange (IKE) versions are 1 and 2.

Step 5 From the **Encryption** drop-down list, choose from the following encryption types:

- **aes-128-cbc**
- **aes-256-cbc**
- **aes-128-gcm**
- **aes-256-gcm**

Note
The encryption type choices are of either 128 or 256 key lengths and either Cipher Block Chaining mode or Galois/Counter mode.

Step 6 From the **Authentication** drop-down list, choose from the following hash-based message authentication code (HMAC) secure hash algorithm (SHA) options:

- **HMAC SHA1**
- **HMAC SHA256**
- **HMAC SHA384**

Step 7 From the **IKE DH Group** drop-down list, choose from the following Diffie-Hellman groups:

- **Group 14** (2048 bits)
- **Group 19** (256-bit elliptic curve)
- **Group 20** (384-bit elliptic curve)

Step 8 In the **IKE Lifetime (1800-86400)** field, enter a value (in seconds) to specify the timeout interval for IKE. The valid range is 1800 to 86400 seconds, and the default value is 28,800 seconds.

Step 9 In the **IPSec Lifetime (1800-28800)** field, enter a value (in seconds) to specify the timeout interval for IPSec. The valid range is 1800 to 28800 seconds, and the default value is 1800 seconds.

Step 10 From the **IKE Phase 1** drop-down list, choose one of the following options to specify the IKE protocol:

- **Main**

- **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.

Step 11 From the **IKE Peer Identification** drop-down list, choose from the following options to be used:

- **FQDN**
- **User FQDN**
- **CN**
- **IP**

Step 12 In the **IKE Peer Value** field, enter the peer value for IKE.

Step 13 From the **IKE Authentication Mode** drop-down list, choose from the following options:

- **PSK**
- **Certificate**

Step 14 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 15 In the **Shared Secret** and **Confirm Shared Secret** fields, 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 16

Step 17 In the **Shared Secret** and **Confirm Shared Secret** fields, 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 18 Save the configuration.

Configuring an IPSec Profile (CLI)

Procedure

Step 1 Create the IPSec profile by entering this command:

config ipsec-profile {**create** | **delete** } *profile-name*

Step 2 Configure the IPSec profile Internet Key Exchange (IKE) version by entering this command:

config ipsec-profile ike version {**1** | **2** } *profile-name*

Step 3 Configure the IPSec profile encryption by entering this command:

config ipsec-profile encryption {**aes-128-cbc | aes-256-cbc | aes-128-gcm | aes-256-gcm** } *profile-name*

Step 4 Configure the IPSec profile authentication by entering this command:

config ipsec-profile authentication {**hmac-sha1** |**hmac-sha256** | **hmac-sha384** } *profile-name*

Step 5 Configure the IKE Diffie-Hellman group by entering this command:

config ipsec-profile ike dh-group {**group-14** |**group-19** | **group-20** } *profile-name*

Step 6 Configure the IKE lifetime by entering this command:

config ipsec-profile life-time-ike *lifetime-in-seconds profile-name*

The valid range is 1800 to 86400 seconds, and the default value is 28,800 seconds.

Step 7 Configure the IPSec lifetime by entering this command:

config ipsec-profile life-time-ipsec *lifetime-in-seconds profile-name*

The valid range is 1800 to 28800 seconds, and the default value is 1800 seconds.

Step 8 Configure IKE Phase1 mode by entering this command:

config ipsec-profile ike phase1 {**aggressive** |**main** } *profile-name*

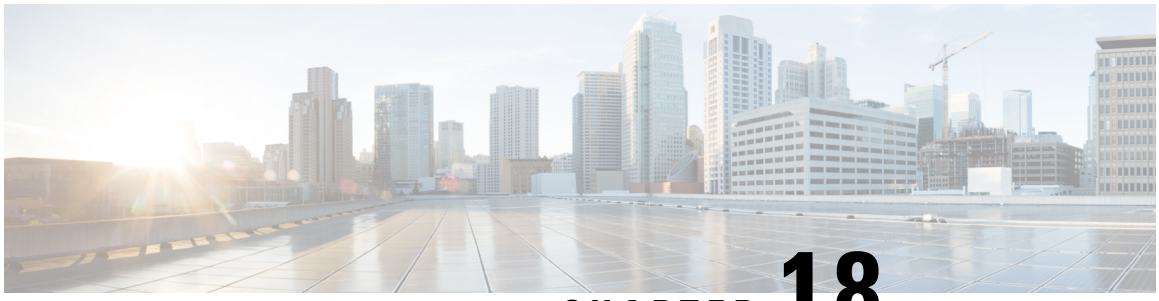
Step 9 Configure the peer identification mode by entering this command:

config ipsec-profile ike peer-identification {**fqdn** |**user-fqdn** | **dn** | **ip** } *profile-name*

Step 10 Configure the IKE authentication method and the shared secret by entering this command:

config ipsec-profile ike auth-mode {{**pre-shared-key** *profile-name* {*ascii* | *hex*} *shared-secret*} | {**certificate** *profile-name*}}

Step 11 Save the configuration.



CHAPTER 18

Cisco Umbrella WLAN (OpenDNS)

- Cisco Umbrella WLAN (OpenDNS), on page 337
- Configuring Cisco Umbrella WLAN (GUI), on page 338
- Configuring Cisco Umbrella WLAN (CLI), on page 339
- Configuring Local Policies for Cisco Umbrella (GUI), on page 340

Cisco Umbrella WLAN (OpenDNS)

The Cisco Umbrella WLAN (OpenDNS) provides a cloud-delivered network security service at the Domain Name System (DNS) level, with automatic detection of both known and emergent threats.

This feature allows you to block sites that host malware, bot networks, and phishing before they actually become malicious.

Cisco Umbrella WLAN provides:

- Policy configuration per user group at a single point.
- Policy configuration per network, group, user, device, or IP address.

  The following is policy priority order:

  1. Local policy
  2. AP group
  3. WLAN

- Visual security activity dashboard in real time with aggregated reports.
- Schedule and send reports through email.
- Support up to 60 content categories, with a provision to add custom allowed list and blocked list entries.

This feature does not work in the following scenarios:

- If an application or host use an IP address directly, instead of using DNS to query domain names.
- If a client is connected to a web proxy and does not send a DNS query to resolve the server address.

Note For more information about integrating this feature, see the *Cisco Umbrella WLAN Integration Guide* at

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-4/b_cisco_umbrella_wlan_integration_guide.html

.

Configuring Cisco Umbrella WLAN (GUI)

Before you begin

- You should have an account with Cisco Umbrella.
- You should have an API token from Cisco Umbrella.

Procedure

Step 1 Choose **Security** > **OpenDNS** > **General**.

The **OpenDNS General Configuration** window is displayed.

Step 2 Check the **OpenDNS Global Status** check box to enable OpenDNS configuration.

Step 3 In the **OpenDns-ApiToken** field, enter the API-token obtained from the OpenDNS Server account.

Step 4 In the **Profile Name** field, enter the profile name that is to be used in the OpenDNS configuration.

Step 5 Click **Add**.

Step 6 Map the profile to the corresponding WLAN or AP group.

a) To map the profile to a WLAN, choose **WLAN** > **WLAN ID** > **Advanced**, and from the **OpenDNS Profile**, select the desired profile.

Note
An administrator can configure OpenDNS in a WLAN in the following modes under the WLAN advanced tab:

- **DHCP Proxy for DNS override** - This is the interface-level configuration, which forms part of the DHCP process to propagate OpenDNS IP address to all WLANs associated to the interface.
- **OpenDNS Mode Force (default)** - This mode is enforced per WLAN, which blocks intentional client activity after client is associated to aWLAN.
- **OpenDNS Mode Ignore (default)** - The controller honors the DNS server used by the client, which could be OpenDNS server or enterprise/external DNS.

b) To map the profile to an AP group, choose **WLANs** > **Advanced** > **AP Groups**, select the corresponding AP group, click the **WLAN** tab, and mouse over the blue button and select **OpenDNS Profile**.

To view OpenDNS mapping, choose **Security** > **OpenDNS** > **General** and click the **Profile Mapped Summary** hyperlink.

Note
Each Cisco Umbrella profile will have a unique OpenDNS-Identity generated on the controller (in the format *Controller name _profile name*). This will be pushed to the associated Cisco Umbrella account in the cloud.

Step 7 Click **Apply**.

What to do next

1. From the Cisco Umbrella dashboard, verify that your controller shows up under **Device Name**, along with their identities controller.
2. Create classification rules for the user roles, for example, rules for employees and nonemployees.
3. Configure policies on the Cisco Umbrella server.

Configuring Cisco Umbrella WLAN (CLI)

This section describes the procedure to configure Cisco Umbrella for a wireless LAN (WLAN) or an access point (AP) group in a WLAN.

Before you begin

- You should have an account with Cisco Umbrella.
- You should have an API token from Cisco Umbrella.

Procedure

Step 1 **config network dns serverip** *server-ip*

Example:

```
(Cisco Controller) > config network dns serverip 208.67.222.222
```

Configures the DNS server IP address of the network.

Step 2 **config opendns enable**

Example:

```
(Cisco Controller) > config opendns enable
```

Enables the Cisco Umbrella global configuration.

Step 3 **config opendns api-token** *api-token*

Example:

```
(Cisco Controller) > config opendns api-token
D72996C18DC334FB2E3AA46148D600A4001E5997
```

Registers the Cisco Umbrella API token on the network.

Step 4 **config opendns profile create** *profilename*

Example:

```
(Cisco Controller) > config opendns profile create profile1
```

Creates an Cisco Umbrella profile that can be applied over a WLAN.

Step 5 **config wlan opendns-profile** *wlan-id profile-name* **enable**

Example:

```
(Cisco Controller) > config wlan opendns-profile wlan1 profile1 enable
```

Applies the Cisco Umbrella profile to a WLAN.

Step 6 **config wlan apgroup opendns-profile** *wlan-id site-name profile-name* **enable**

Example:

```
(Cisco Controller) >config wlan apgroup opendns-profile wlan1 apgrp1 profile1
```

(Optional) Applies the Cisco Umbrella profile to an AP group with the WLAN.

Step 7 **config policy** *policy-name* **create**

Example:

```
(Cisco Controller) > config policy ipad create
```

Creates a policy name.

In controller, policy is generic term that specifies a rule and the associated action when that rule criterion is met for given client.

You can create policy and have rule on that by saying if the rolename from AAA server comes as *employee* take an action to apply Cisco Umbrella profile associated to that policy. Cisco Umbrella profile is applied to the client if the WLAN of that client is mapped for this policy.

Step 8 **config policy** *policy-name* **action opendns-profile-name enable**

Example:

```
(Cisco Controller) > config policy ipad action opendns-profile-name enable
```

Attaches the policy name to the Cisco Umbrella profile.

What to do next

Configure policies in opendns.com.

- Configure granular policies to block sites based on the category of each profile (profiles are listed as identities).
- Add allowed list and blocked list rules for each profile.

Configuring Local Policies for Cisco Umbrella (GUI)

When mapped to local policy, the Cisco Umbrella allows for a granular differentiated user browsing experience based on dynamic evaluation of attributes (user role, device type, and so on).

Use this procedure to configure user role based local policy and tie the corresponding Cisco Umbrella profile to it. This procedure also provides information about how to map a local policy to a WLAN.

Procedure

Step 1 Choose **Security** > **Local Policies** > **New**.

This opens the new policy creation page.

a) In the **Policy Name** field, enter the local policy name.
b) Click **Apply**.

Step 2 From the policies listed under **Policy List**, choose a **Policy Name** to configure the Cisco Umbrella profile.

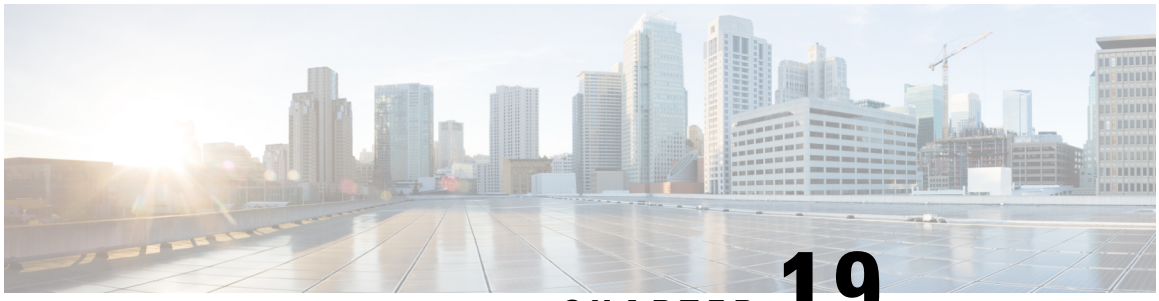
a) From the **Match Criteria** sub-section, enter the Match Role String.
b) From the **Action** sub-section, select the required option from the OpenDNS Profile drop-down list.
c) Click **Apply**.

Step 3 Choose **WLAN** > **WLAN ID** > **Policy Mapping**.

a) In the **Priority Index** field, enter the priority index number.
b) From the **Local Policy** drop-down list, choose a value.
c) Click **Add**.

What to do next

Verify whether the policies you created are working, by connecting a client to the WLAN.



CHAPTER 19

SNMP

- Guidelines and Limitations for SNMP, on page 343
- Configuring SNMP (CLI), on page 343
- SNMP Community Strings, on page 346
- Configuring Real Time Statistics (CLI), on page 347
- Configuring SNMP Trap Receiver (GUI), on page 348

Guidelines and Limitations for SNMP

We recommend that you do not have the SNMP management station in the subnet of dynamic interface or service port of the controller.

If the SNMP management station subnet is the same as that of the dynamic interface, we recommend that you set the SNMP queries to the IP address of the dynamic interface of the controller. Similarly, if the SNMP management station subnet is the same as that of the service port, we recommend that you set the SNMP queries to the IP address of the service port of the controller.

Controller has a limitation where, even if the queries are made to the management IP address, SNMP response packets are sent with the source IP address as the dynamic interface or the service port respectively. For more information, see CSCvk38081.

To avoid AP data mismatch, we recommend retrieving the AP-related details sent to Cisco Catalyst Center (earlier known as Cisco DNA Center) from the controller only after all the APs are in **Run** state.

The controller may fail to sync traps with the configured trap receiver when the AP register SNMP trap is enabled on the controller. The SNMP trap is limited to 1024 message queue size, and the controller might get overwhelmed with the huge number of traps during the AP association/disassociation situation. The workaround is to clear the older trap entries on the controller using the **clear traplog** command.

Configuring SNMP (CLI)

Note Starting from Release 8.3, SNMP over IPSec, and SNMP Traps over IPSec is supported over IPv6 interfaces.

Note To view the controller trap log, choose **Monitor** and click **View All** under "Most Recent Traps" on the controller GUI.

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 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.

- 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*

- 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, you may use the community names to communicate to the controller using SNMP. Therefore, we strongly advise that you change these values.

Changing the SNMP Community String Default Values (GUI)

Procedure

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)

Procedure

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 controller 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)

Procedure

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.

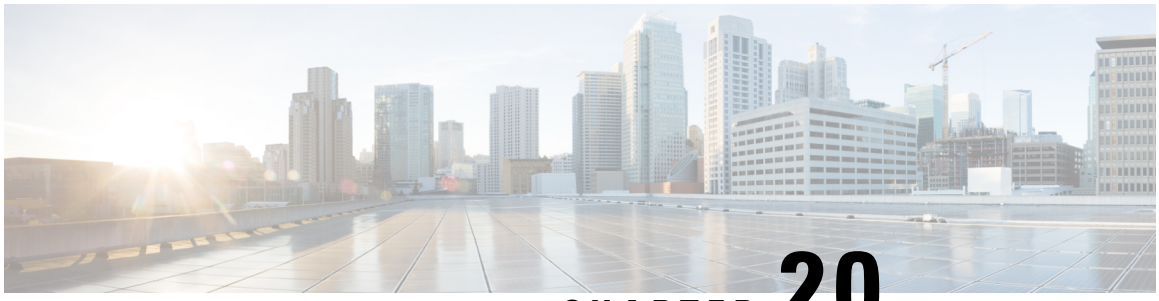
Step 8 Save the configuration.

You can create a maximum of 6 such SNMP trap receivers.

PART III

Mobility

- Overview, on page 353
- Auto-Anchor Mobility, on page 359
- Mobility Groups, on page 369
- Encrypted Mobility Tunnel, on page 379
- Monitoring and Validating Mobility, on page 383



CHAPTER 20

Overview

- Information About Mobility, on page 353

Information About Mobility

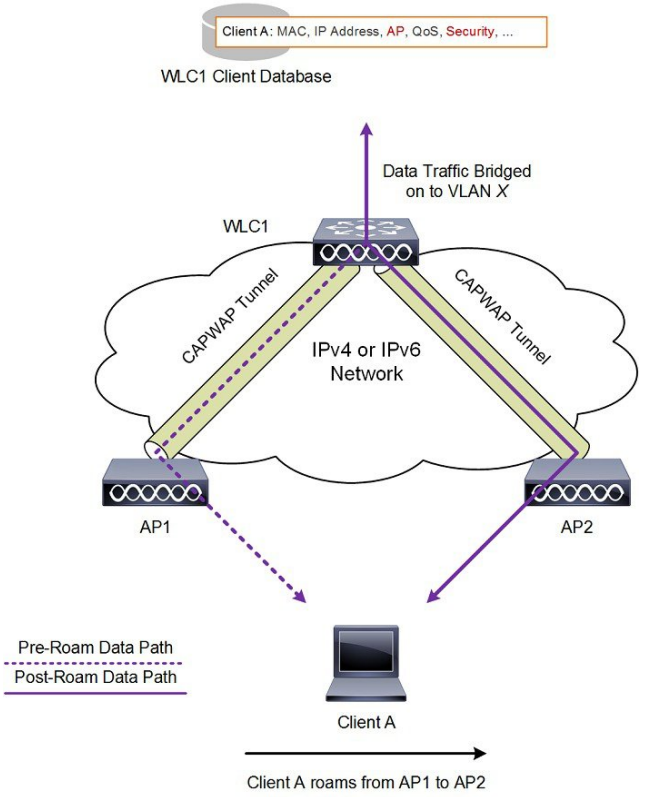
Mobility, or roaming, is a wireless LAN client's ability to maintain its association seamlessly from one access point to another securely and with as little latency as possible. This section explains how mobility works when controllers are included in a wireless network.

When a wireless client associates and authenticates to an access point, the access point's controller places an entry for that client in its client database. This entry includes the client's MAC and IP addresses, security context and associations, quality of service (QoS) contexts, the WLAN, and the associated access point. The controller uses this information to forward frames and manage traffic to and from the wireless client.

Note The information about mobility in this section applies to APs in only Local Mode. For APs in FlexConnect mode, see the FlexConnect section.

The figure below shows a wireless client that roams from one local mode access point to another local mode access point when both access points are joined to the same controller.

Figure 19: Intracontroller Roaming

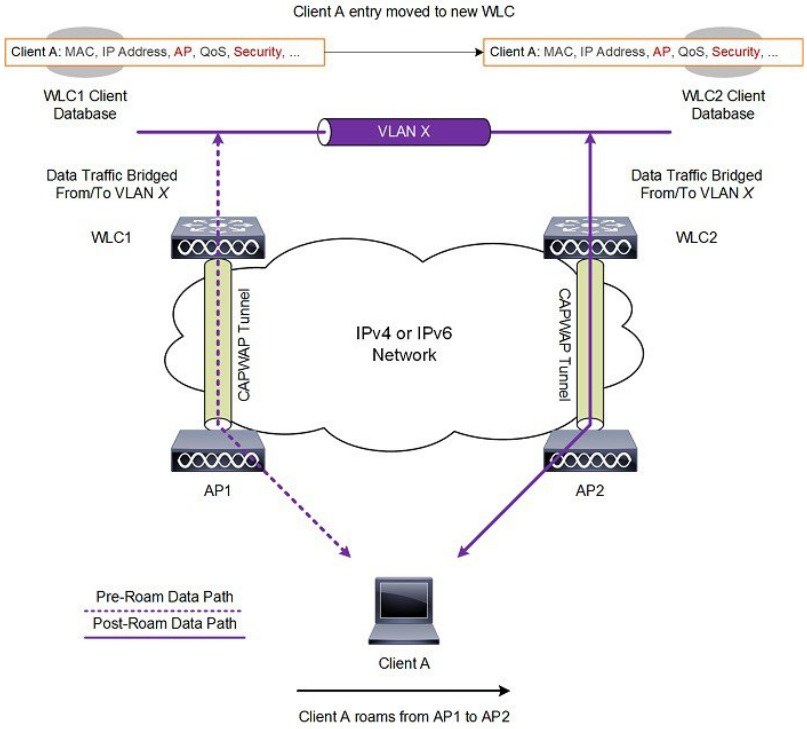


When the wireless client moves its association from one access point to another, the controller simply updates the client database with the newly associated access point. If necessary, new security context and associations are established as well.

The process becomes more complicated, however, when a client roams from an access point joined to one controller to an access point joined to a different controller. It also varies based on whether the controllers are operating on the same subnet.

The figure below shows intercontroller Layer 2 roaming, which occurs when the wireless LAN interfaces of the controllers are on the same IP subnet.

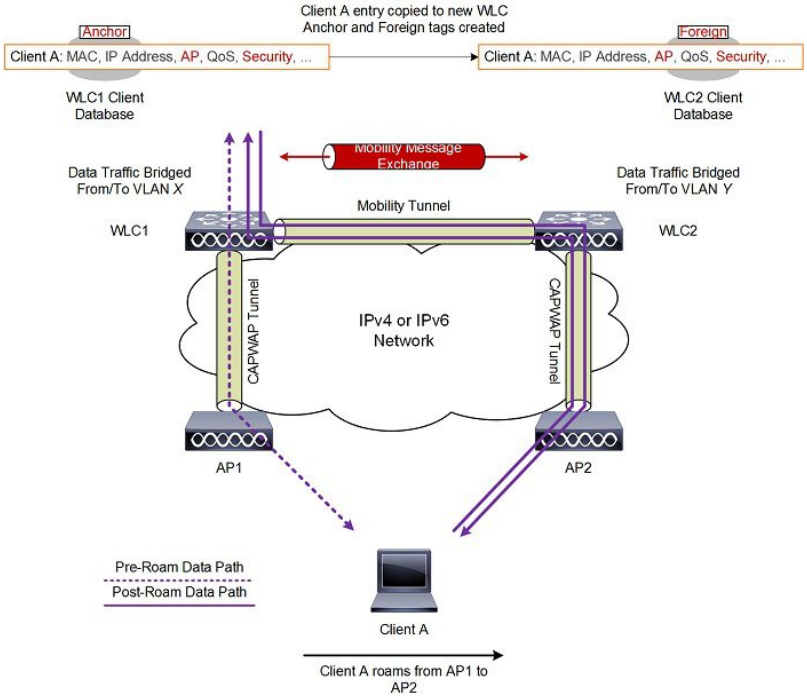
Figure 20: Intercontroller Layer 2 Roaming



When the client associates to an access point joined to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database entry is updated for the new access point. This process remains transparent to the user.

The figure below shows intercontroller Layer 3 roaming, which occurs when the wireless LAN interfaces of the controllers are on different IP subnets.

Figure 21: Intercontroller Layer 3 Roaming

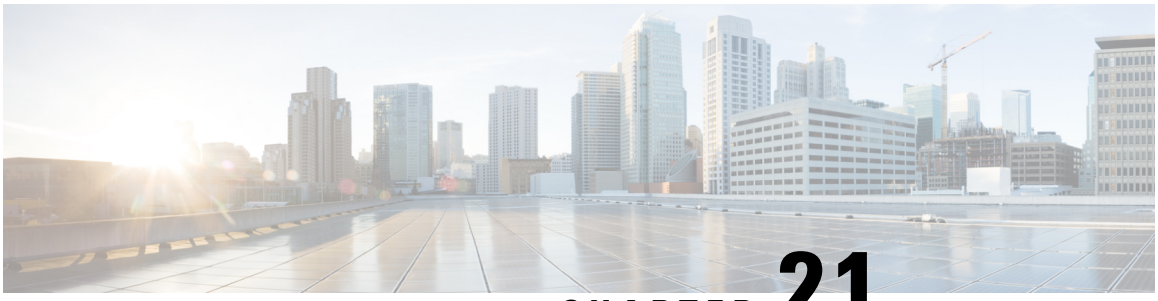


Layer 3 roaming is similar to Layer 2 roaming in that the controllers exchange mobility messages on the client roam. However, instead of moving the client database entry to the new controller, the original controller marks the client with an “Anchor” entry in its own client database. The database entry is copied to the new controller client database and marked with a “Foreign” entry in the new controller. The roam remains transparent to the wireless client, and the client maintains its original IP address.

Guidelines and Restrictions

- If the management VLAN of one controller is present as a dynamic VLAN on another controller, the mobility feature is not supported.
- If a client roams in web authentication state, the client is considered as a new client on another controller instead of considering it as a mobile client.
- When the primary and secondary controller fail to ping each other’s IPv6 addresses, and they are in the same VLAN, you need to disable snooping to get the controller to ping each other successfully.
- Cisco Wireless Controllers (that are mobility peers) must use the same DHCP server to have an updated client mobility move count on intra-VLAN.
- The New Mobility feature is not supported in Release 8.6 and later releases.
- Ensure that the interface name is the same across mobility peers for AAA override to work as expected.
- Up through 8.5, intercontroller roaming was not supported in the following scenarios:
  - Central web authentication (CWA) without 802.1X
  - Web authentication on MAC filter failure

These scenarios are supported with intercontroller roaming beginning with Release 8.6.



CHAPTER 21

Auto-Anchor Mobility

- Information about Auto-Anchor Mobility, on page 359
- Restrictions for Auto-Anchor Mobility, on page 360
- Configuring Auto-Anchor Mobility (GUI), on page 361
- Configuring Auto-Anchor Mobility (CLI), on page 362
- Guest Anchor Priority, on page 364
- Dynamic Anchoring for Clients with Static IP, on page 366

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 designating them as mobility anchors for a WLAN.
- Auto-anchor mobility does not support multiple WLANs with the same SSID name and WLAN ID used is number 17 or higher.
- You can configure multiple controllers as mobility anchors for a WLAN.
- 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 controller deployment, ensure that the foreign controller does not have a WLAN mapped to a VLAN that is associated with the guest anchor controller.

- In Old Mobility, when roaming from foreign to anchor controller, the other foreign controllers in the mobility group do not receive mobile announce messages.

Configuring Auto-Anchor Mobility (GUI)

Procedure

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.

Note
We recommend that you use the default keepalive count and interval values to reduce converge time between the Cisco AireOS Wireless Controllers and Cisco Catalyst 9800 Series Wireless Controllers while setting up a mobility tunnel.

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

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.

  Note
  We recommend that you use the default keepalive count and interval values to reduce converge time between the Cisco AireOS Wireless Controllers and Cisco Catalyst 9800 Series Wireless Controllers while setting up a mobility tunnel.

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.

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

Note
This command output shows the burned-in MAC address.

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.

Guest Anchor Priority

The guest anchor priority feature provides a mechanism that gives "active/standby" load distribution amongst the anchor controllers. This is achieved by assigning a fixed priority to each anchor controller, by distributing the load to highest priority controller and in round-robin fashion if they have the same priority value.

Releases Prior to 8.1	With Release 8.1
All guest clients are load balanced in round robin fashion amongst anchor controllers	All guest clients are sent to anchor controller with highest priority in relation to local internal controller
If an anchor fails, guest clients will be load balanced amongst remaining anchor controllers	If an anchor fails, guest clients will be sent to the next highest priority or round robin if remaining anchors have same priority value

You can configure a priority to the guest anchor when you configure a WLAN. Priority values range from 1 (high) to 3 (low) or primary, secondary or tertiary and defined priority is displayed with guest anchor. Only one priority value is allowed per anchor controller. Selection of guest anchor is round-robin based on a single priority value. If a guest anchor is down, the fallback would be on guest anchors with equal priority. If all guest anchors with same priority value are down, the selection would be on a round-robin basis on next highest priority and so on. Default priority value is 3. If controller is upgraded to Release 8.1, it will be marked with priority 3. Priority configurations are retained across reboots. The priority configuration would be synchronized on HA pair for seamless switchover. Same set of rules apply in determining the anchor controller regardless of IPv4 and/or IPv6 addressing. That is, highest priority value is determinant and not addressing including dual stack case.

Restrictions

- No hard limit on the number of times a priority value is used
- Feature applies only to wireless and "old" mobility model
- Maximum number of supported anchors per WLAN is 24
- Downgrading from Release 8.1 would void this feature since it is not supported on earlier images
- If a guest anchor with higher priority comes up, the existing connections will not shift to the new high priority anchor and only the new connections will go to it
- This feature is applicable when all internal and anchor controllers are using Release 8.1
- There should not be a local address with priority of zero at the Internal/Foreign controller. Priority 0 in the output indicates a local IP address. For example at the anchor controller on DMZ with tunnel termination

Deployment Considerations

- Priority configuration should only be done on foreign controller WLAN. On the mobility list if you are seeing value zero and non-zero that means the same controller is acting as Anchor for few WLANs and foreign controller for few WLAN, if you have controller in DMZ and there is no APs connected to it, then we should not see any non-zero priority for any of its WLANs, as this should be the terminating point for all the clients on the network.

- Ideally we should not see priority zero on foreign controller and non-zero on anchor controller. example: 10.10.10.10(SF) and 20.20.20.20(NY) should not have any priority with zero and DMZ controller 172.10.10.10(SF) and 172.20.20.20(NY) should not have any priority with non-zero values.
- Here priority values zero is not configurable when we select the controller own IP Address as anchor. It will automatically set the priority zero if controller own IP address is selected as anchor.

Examples

- Local anchor controllers may be grouped together with higher priority value than group of remote anchor controllers
- Guest client traffic goes to Anchor controller(s) that is/are local to internal controller rather than remote one(s) due to having higher priority value
- Guest client traffic will be load balanced in round-robin across local anchor controllers since local anchors have same priority value
- If all local anchor controllers fail then traffic will be load balanced in round-robin across remote anchor controller with next priority level

This section contains the following subsections:

Configuring Guest Anchor Priority (GUI)

Procedure

Step 1 Choose **WLANs**.

Step 2 Mouse over the blue down arrow and click **Mobility Anchors**.

Step 3 On the **Mobility Anchors** page, select the mobility anchor from the **Switch IP Address (Anchor)** drop-down list and assign a priority.

Configuring Guest Anchor Priority (CLI)

Procedure

- To configure Guest Anchor priority:
  config wlan mobility anchor add *wlan-id ip-addr* **priority** *prioirity-number*
- To validate proper anchor controller through assigned client address:
  show client summary ip
- To check whether the expected anchor is getting the request:
  debug mobility handoff enable
- To check the anchor priority list of a WLAN:
  test mobility anchor-prioritylist *wlan-id*

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 anchor is responsible for sending the accounting packets AVP attribute values input/outputs to the AAA server as it is the point of accounting with the AAA. However, the values sent will be zero. Therefore, only the foreign can send the actual values to the AAA server.

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 controllers. If the NTP/SNTP servers are different, ensure that the system time on all controllers 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 controller that has the lagging time with NTP/SNTP enabled drops the mobile announce messages.

Configuring Dynamic Anchoring of Static IP Clients (GUI)

Procedure

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 checking the **Static IP Tunneling** check box.

Step 5 Click **Apply** to commit your changes.

Configuring Dynamic Anchoring of Static IP Clients (CLI)

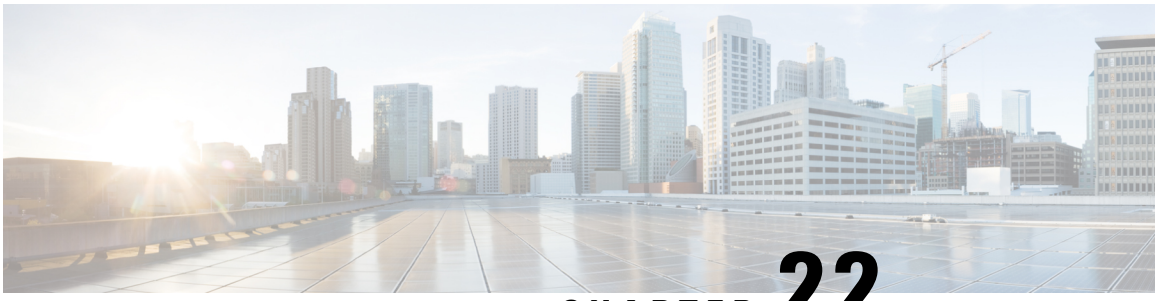
config wlan static-ip tunneling {enable | disable} *wlan_id*— Enables or disables the dynamic anchoring of static IP clients on a given WLAN.

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 22

Mobility Groups

- Information About Mobility Groups, on page 369
- Prerequisites for Configuring Mobility Groups, on page 372
- Configuring Mobility Groups (GUI), on page 373
- Configuring Mobility Groups (CLI), on page 375
- Viewing Mobility Group Statistics (GUI), on page 377
- Viewing Mobility Group Statistics (CLI), on page 378

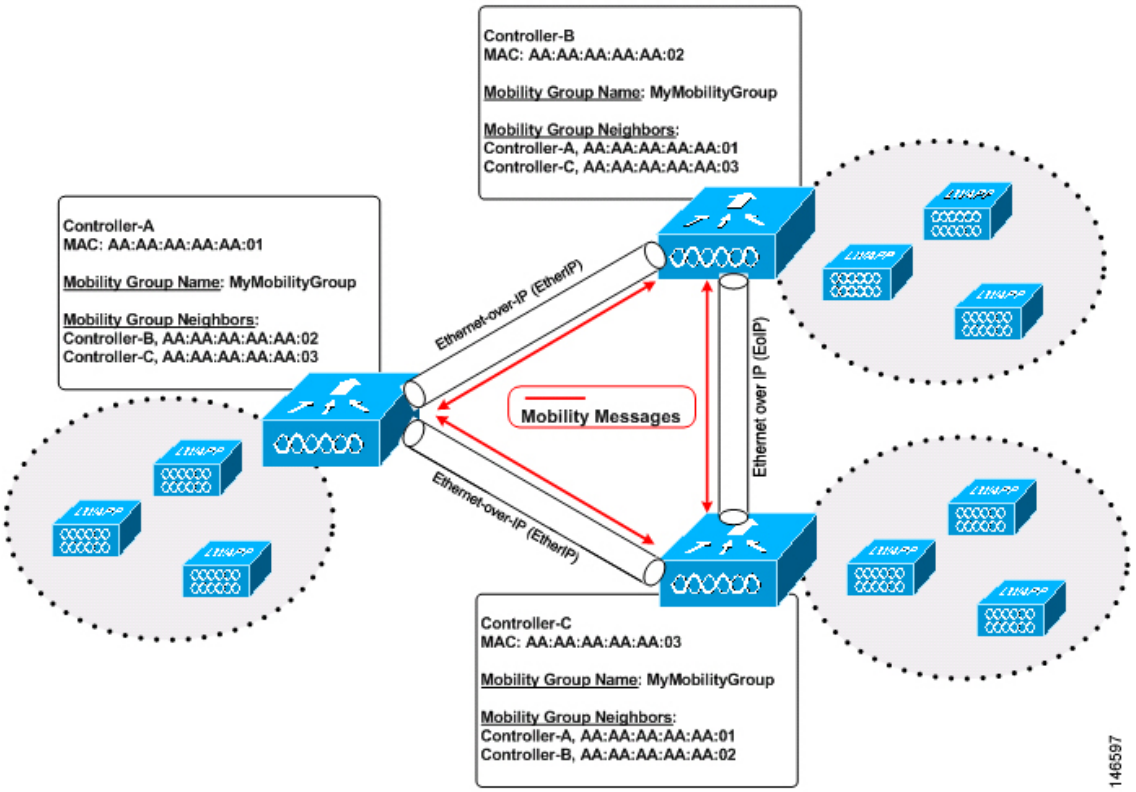
Information About Mobility Groups

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 If migrating APs from one controller to another controller to decommission the old controller, clients that were associated with the first controller before the move might be anchored to the old controller after the move. As a workaround, you must disable the WLANs on the old controller before decommissioning it.

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 as long as the controllers are running compatible AireOS versions. For more information, see the "IRCM Compatibility Matrix for AireOS Releases" section in the Cisco Wireless Solutions Software Compatibility Matrix document.

Figure 22: Example of a Single Mobility Group



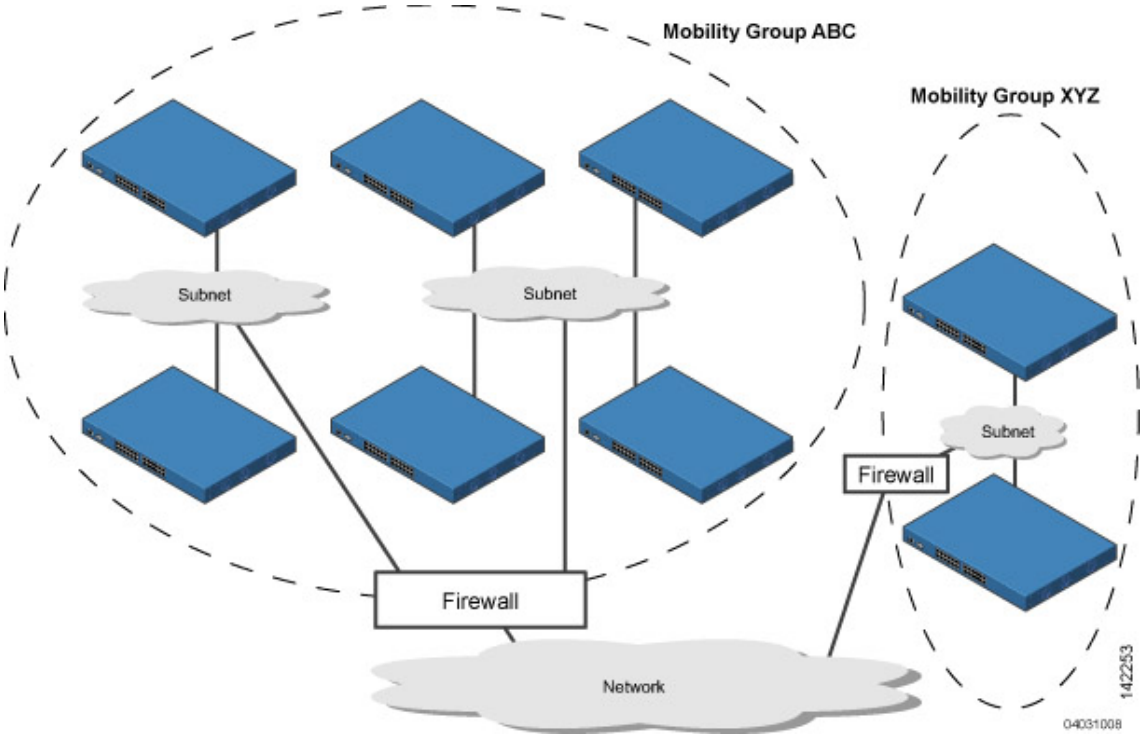
As shown above, each controller is configured with a list of the other members of the mobility group. In this example, client data traffic is tunneled between controllers in Ethernet-over-IP as mobility encryption is not configured. Whenever a new client joins a controller, the controller sends out a 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. You can configure the controller to use multicast to send the Mobile Announce messages. This functionality enables the controller to send only one copy of the message to the network, which destines it to the multicast group that contains all the mobility members. To derive the maximum benefit from multicast messaging, we recommend that you enable multicast messaging for all group members.

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 messages among mobility group members can be transmitted in IPv4 or IPv6, as unicast or multicast. We recommend multicast messaging for large mobility groups.

Figure 23: 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, unless each mobility group member is configured with mobility list entries for the other mobility group members. 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.

A mobility group can have up to 24 members and a mobility list can have up to 72 members. For example, the following combinations 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.

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 using the mping and eping commands.

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.

- If configuring mobility peers that run different software versions, see the "IRCM Compatibility Matrix for AireOS Releases" section in the Cisco Wireless Solutions Software Compatibility Matrix document.

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.
- 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.

- UDP port 5246 and 5247 are for CAPWAP between AP and controller. Encrypted mobility uses UDP 16666 for control and UDP 16667 for data (either encrypted or plain). EoIP IP 97 is for old mobility.

For information about protocols and port numbers that must be used for management and operational purposes, see the Cisco Unified Wireless Network Protocol and Port Matrix document.

Note To view information on mobility support across controllers with different software versions, see 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)

Procedure

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
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)

Procedure

Step 1 Check the current mobility settings by entering this command:

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
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)

Procedure

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)

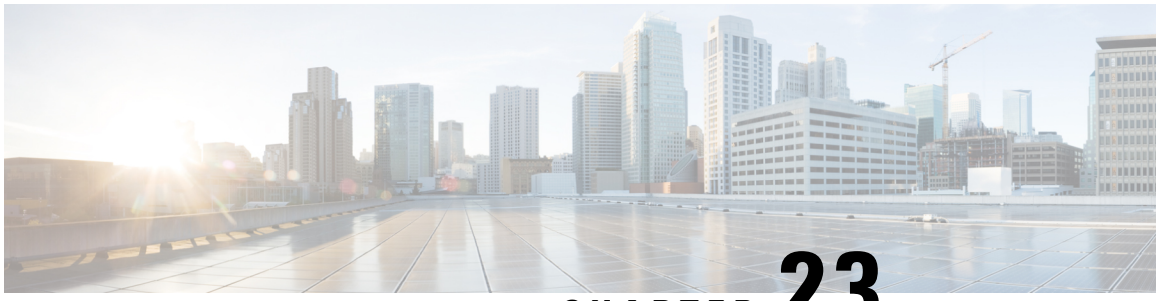
Procedure

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 23

Encrypted Mobility Tunnel

- Information about Encrypted Mobility Tunnel, on page 379

Information about Encrypted Mobility Tunnel

A secure link in which data is encrypted using CAPWAP DTLS protocol can be established between two controllers. This secured link is called Encrypted Mobility Tunnel.

If encrypted mobility tunnel is in enabled state, the data traffic is encrypted and the controller uses UDP port 16667, instead of EoIP, to send the data traffic.

To ensure that controllers with expired MIC certificates are able to join the encrypted mobility tunnel enabled network, an existing CLI is used to disable the MIC certificate date validation.

Note This command disables the date validation check during Cisco AP join and encrypted mobility tunnel creation. When the **config ap cert-expiry-ignore** CLI is enabled, the lifetime check is disabled.

Restrictions for Encrypted Mobility Tunnel

- This feature is supported on Cisco 3504, 5520, and 8540 controllers only.

Note The Cisco 5508 and 8510 Wireless Controllers do not support tunnel encryption protocols. They support IRCM with unencrypted mobility tunnels only.

- Native IPv6 is not supported.
- Mobility Multicast for an encrypted tunnel is not supported.
- The Encrypted Mobility Tunnel feature should be enabled on all the mobility peers in the network to have the tunnel created. The default state is set to disabled.
- If the packets passing through the controller after L3 roaming are greater than the MTU size of the controller in secure mobility, along with secure mobility, data encryption functionality must be enabled for the fragmented packets to be forwarded through a secure mobility tunnel.

- Only MIC certificate is supported to create the tunnel.
- When using Cisco 3504 controller as an anchor, we recommend reducing the client load by 30% of the controller's maximum load capability.

Configuring Mobility Groups for Inter-Release Controller Mobility (IRCM) (GUI)

Procedure

Step 1 Choose **Controller** > **Mobility Management** > **Mobility Groups** to open the **Static Mobility Group Members** page.

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 Click **New** to open the **Mobility Group Member** > **New** page.

Step 3 Add a controller to the mobility group as follows:

a. In the **Member IP Address** text box, enter the management interface IPv4 address of the controller to be added.

Note
IPv6 address is not supported.

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. From the **Secure Mobility** drop-down list, choose **Enabled**.

e. From the **Data Tunnel Encryption** drop-down list, choose **Enabled**.

f. From the **High Cipher** drop-down list, choose **Enabled**.

You must enable **High Cipher** only if you require DTLS v1.2 encryption. The default value is **Disabled**. In disabled state, DTLS v1.0 encryption is enabled.

g. In the **Hash** text box, enter the virtual controller's hash key of the peer mobility controller.

You must configure the hash only if the peer mobility controller is a virtual controller.

h. 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.

Configuring Mobility Groups for Inter-Release Controller Mobility (IRCM) (CLI)

Procedure

Step 1 Add a peer controller in the mobility group by entering this command:

config mobility group member add *peer-mac-addr peer-ip-addr group-name* **encrypt** {**enable** | **disable**}

Step 2 (Optional) Configure the peer controller data traffic encryption by entering this command:

config mobility group member data-dtls *peer-mac-addr* {**enable** | **disable**}

Default value is Enabled.

Step 3 (Optional) Configure high cipher encryption to enable DTLS 1.2 protocol by entering this command:

config mobility group member add *member-switch-mac-addr member-switch-ip-addr grp-name* **encrypt enable high-cipher-option enable**

Default value is Disabled.

Step 4 Configure the SSC hash of the Cisco Catalyst 9800 Series Wireless Controllers by entering this command:

config mobility group member hash *peer-ip-addr 40-digit-ssc-hash-key*

Note
SSC hash is needed on for peers that do not use a MIC certificate. For example: Cisco Catalyst 9800-CL Wireless Controllers.

Step 5 View the peer to peer mobility encryption status by entering this command:

show mobility summary encryption

Step 6 To see the hash key of mobility group members in the same domain, enter this command:

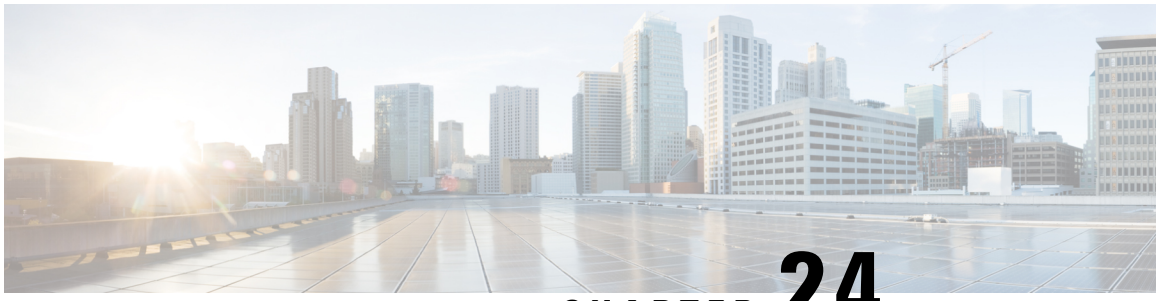
show mobility group member hash

Step 7 View mobility DTLS connection status by entering this command:

show mobility dtls connections

Step 8 View mobility statistics by entering this command:

show mobility statistics



CHAPTER 24

Monitoring and Validating Mobility

- Mobility Ping Tests, on page 383
- WLAN Mobility Security Values, on page 384

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 based on Internet Control Message Protocol (ICMP). The term *ping* is used to indicate an echo request and an echo reply message.

Running Mobility Ping Tests (CLI)

Procedure

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 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.

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 13: 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*

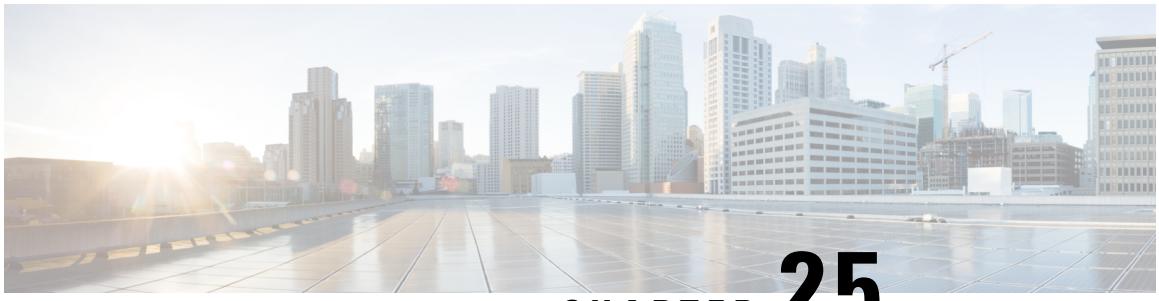
Security Hexadecimal Value	Security Policy
0x00000800	Security_802_11i_NotUsed **Note** Controllers running software release 6.0 or later do not support this security policy.
0x00001000	Security_Web_Passthrough

Note Controllers do not support these security policies: Security_IPSec, Security_IPSec_Passthrough, Security_PPTP, Security_Cranite_Passthrough, Security_Fortress_Passthrough, and Security_L2TP_IPSec.

PART IV

Wireless

- Country Codes, on page 389
- Radio Bands, on page 395
- Radio Resource Management, on page 409
- Wireless Quality of Service, on page 485
- Location Services, on page 531
- Wireless Intrusion Detection System, on page 573
- Advanced Wireless Tuning, on page 619
- Timers, on page 627



CHAPTER 25

Country Codes

- Information About Configuring Country Codes, on page 389
- Restrictions for Configuring Country Codes, on page 390
- Configuring Country Codes (GUI), on page 390
- Configuring Country Codes (CLI), on page 391

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 within that regulatory domain (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 controller. Prior to Release 8.2, you could configure up to 20 country codes per controller; from Release 8.2 onwards, you can configure up to 110 country codes per controller. This multiple-country support enables you to manage access points in various countries from a single controller.

Note

- The 2.4-GHz band radio regulations are the same for the EU and China. Hence, under the 2.4-GHz radio band, it is possible to see -H domain configured APs (China) with the -E AP list in the controller.

- For a complete list of country codes supported per product, see https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.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.

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 radios to join the controller
- J4: Allows 2.4G JPQU and 5G PQU to join the controller.

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)

Procedure

Step 1 Disable the 802.11 networks as follows:

a) Choose **Wireless** > **802.11a/n/ac** > **Network**.
b) Uncheck the **802.11a Network Status** check box.
c) Click **Apply**.
d) Choose **Wireless** > **802.11b/g/n** > **Network**.
e) Uncheck 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)

Procedure

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:

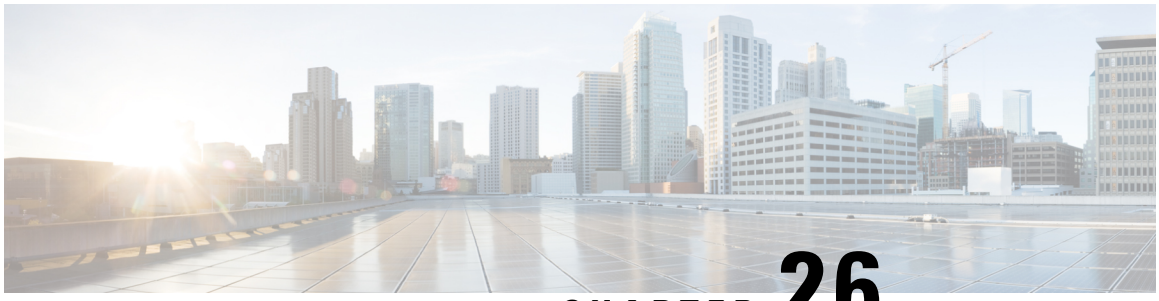
config ap enable *ap_name*

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 26

Radio Bands

- 802.11 Bands, on page 395
- 802.11n Parameters, on page 399
- 802.11ac Parameters, on page 403

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.

This section contains the following subsections:

Configuring the 802.11 Bands (GUI)

Procedure

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 and the recommended 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
DTPC and 801.11h power constraint cannot be enabled simultaneously.

Step 7 Specify the maximum number of allowed clients per radio within this band by entering a value between 1 to 200 in the **Maximum Allowed Client** box. The default value is 200.

Step 8 Select or unselect the **RSSI Low Check** check box to enable or disable the RSSI Low Check feature.

Step 9 (Optional) If you enabled RSSI Low Check, enter the **RSSI Threshold** value.

The default value is –80 dBm.

Step 10 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. At least one data rate must be mandatory.
- **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**—This data rate is not used for communication with associated clients.

Step 11 Click **Apply**.

Step 12 Click **Save Configuration**.

Configuring the 802.11 Bands (CLI)

Procedure

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 Configure the RSSI Low Check feature by entering this command:

config 802.11{**a** | **b**} **rssi-check** {**enable** | **disable**}

Step 8 Configure the RSSI Threshold value by entering this command:

config 802.11{**a** | **b**} **rssi-threshold** *value-in-dBm*

Note
The default value is –80 dBm.

Step 9 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 10 Enable the 802.11a band by entering this command:

config 802.11a enable network

The default value is enabled.

Step 11 Enable the 802.11b band by entering this command:

config 802.11b enable network

The default value is enabled.

Step 12 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 13 Enter the **save config** command to save your changes.

Step 14 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
```

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.

The 802.11n-only access points can filter out clients without high-throughput information element on the association request. The 802.11n-only access points access points reject association requests from clients without high-throughput information element (11n).

In the 802.11n high-throughput mode, there are no 802.11a/b/g stations using the same channel. The 802.11a/b/g devices cannot communicate with the 802.11n high-throughput mode access point, where as the 802.11n-only mode access point uses 802.11a/g rates for beacons or management frames.

Note To disable MCS rates for 802.11n, 802.11ac and 802.11ax, ensure that at least one MCS rate is enabled. To disable 802.11n on the controller to force APs to use only legacy 802.11a/b/g rates, first disable 802.11ax and 802.11ac on the controller for a particular band. Irrespective of the APs mapped to a Custom-RF-Profile, disabling 802.11n globally on the controller applies to all the APs.

Configuring the 802.11n Parameters (GUI)

Procedure

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.

- 16 (22 Mbps)
- 17 (43 Mbps)
- 18 (65 Mbps)
- 19 (87 Mbps)
- 20 (130 Mbps)
- 21 (173 Mbps)
- 22 (195 Mbps)
- 23 (217 Mbps)
- 24 (29 Mbps)
- 25 (58 Mbps)
- 26 (87 Mbps)
- 27 (116 Mbps)
- 28 (173 Mbps)
- 29 (231 Mbps)
- 30 (260 Mbps)
- 31 (289 Mbps)

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 14: Traffic Type Priority Levels

User Priority	Traffic Type
0	Best effort
1	Background
2	Spare
3	Excellent effort
4	Controlled load
5	Video, less than 100-ms latency and jitter
6	Voice, less than 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**}

802.11ac Parameters

The 802.11ac radio module for the Cisco Aironet 3600 Series access point and Cisco Aironet 3700 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 and Cisco Aironet 3700 Series Access Point 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 controller 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.

802.11ac Wave 2 and MU-MIMO

The 802.11ac Wave 2 introduces additional capabilities beyond what were added with Wave 1. It uses MU-MIMO technology and other advancements to help increase wireless performance for applications such as HD video streaming. Wave 2 provides better RF efficiency that Wave 1 provides, in addition to a number of other features that further improve wireless connectivity.

MU-MIMO

MU-MIMO is short for Multi-User, Multiple-Input, Multiple-Output. MU-MIMO is an enhanced form of the MIMO technology that enables multiple independent radio terminals to access a system.

With 802.11n or 802.11ac Wave 1, an access point can transmit multiple spatial streams at the same time, but only directed to a single wireless client. This means only a single device gets data at a time. This is referred to as single-user MIMO (SU-MIMO).

802.11ac Wave 2 allows for MU-MIMO, which enables multiple users to simultaneously receive data from the AP simultaneously using the same channel. With MU-MIMO a Wave 2 capable access point is able to use its antenna resources to transmit to multiple clients, all at the same time and over the same channel. MU-MIMO is used in the downstream direction and requires the wireless clients to also be Wave 2 capable.

More Spatial Streams

802.11ac Wave 2 allows for up to eight spatial streams. However, initial Wave2 implementations will only increase the number of spatial streams from 3 to 4 as compared to Wave 1 implementations. The support of an additional spatial stream allows for additionally increased performance as compared to 3 SS APs.

References

For more information on these technologies, see the following documents on Cisco.com:

- *Cisco 802.11ac Wave 2 FAQs* at http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/802-11ac-solution/q-and-a-c67-734152.html
- *Fundamentals of 802.11ac Wave 2 post on the Cisco Interaction Network* at http://blogs.cisco.com/cin/fundamentals-of-802-11ac-wave-2
- *802.11ac: The Fifth Generation of Wi-Fi* technical white paper at http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103.html

Explicit Compressed Beamforming Feedback

The AP 1850 supports standards-based Explicit Compressed Beamforming Feedback (ECBF) as defined in the 802.11ac standards. With ECBF the client provides estimates of the wireless channel conditions to the access point. As these are based on explicit channel measurements from the client, both the AP and the client must support it. For 802.11ac, the access point's ECBF is typically referred to as Transmit Beamforming or TxBF for short.

While both TxBF and ClientLink 3.0 improve the performance of wireless client devices, ClientLink3.0 provides an additional advantage over TxBF. ClientLink3.0 technology does not depend on any client-side hardware or software capabilities and operates seamlessly in mixed-mode environments where 802.11ac and 802.11a/n clients coexist on the same access point. In comparison, TxBF requires client-side support to take advantage of the performance improvements of beamforming and therefore benefits only 802.11ac clients that support TxBF.

The Cisco 1850 AP supports TxBF but not beamforming to legacy client devices. Therefore, Cisco 1850 AP does not support ClientLink 3.0.

Note ClientLink 3.0 is supported on the Cisco Aironet 2700 and 3700 Series 802.11ac APs.

Note You can disable TxBF only on the APs that support ClientLink 1.0. It cannot be disabled on the APs that supports ClientLink 2.0 and above.

Restrictions for 802.11ac Support

- The 802.11ac module is supported only on the following access points:
  - 1700
  - 1800
  - 2700
  - 2800
  - 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 3504 Wireless Controller
  - Cisco 5520 Wireless Controller
  - Cisco 8540 Wireless Controller
- 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)

Procedure

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 Ensure that all of the 0 to 31 MCS data rate indices are enabled (which is the default setting).

Step 4 Save the configuration.

Configuring MU-MIMO (GUI)

This feature is supported on all the supporting Cisco Wave 2 APs.

Procedure

Step 1 Choose **WLANs** and click the WLAN ID.

Step 2 In the **Advanced** tab, check or uncheck the **11ac MU-MIMO** check box.

Step 3

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 Ensure that all of the 0 to 31 MCS data rate indices are enabled (which is the default setting). In 8.1 and later releases, RF profiles should include MCS 0-31 instead of MCS 0-23 in earlier releases.

Configuring MU-MIMO (CLI)

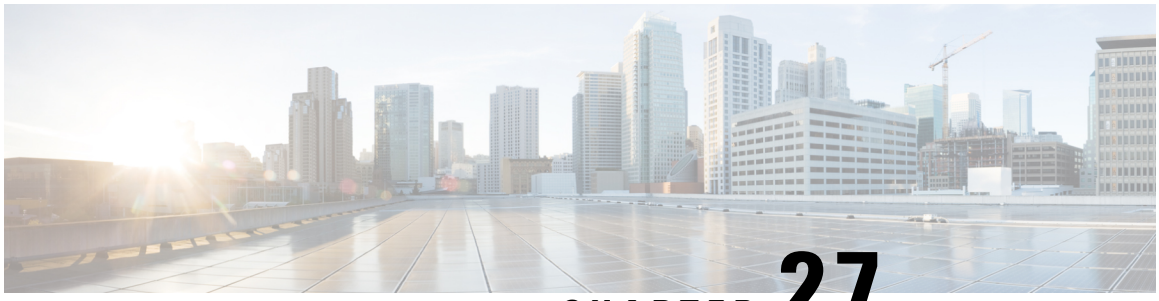
This feature is supported on all the Cisco Wave 2 APs.

Procedure

Step 1 Enable or disable MU-MIMO by entering this command on the controller console:
config wlan mu-mimo {**enable** | **disable**} *wlan-id*

Step 2 See the status of MU-MIMO by entering these commands on the AP console:

- For a WLAN: **show interfaces Dot11Radio** *Dot11-radio-interface-number* **mumimo wlan** *wlan-id*
- For a client: **show interfaces Dot11Radio** *Dot11-radio-interface-number* **mumimo client** *mac-addr*



CHAPTER 27

Radio Resource Management

- Information about Radio Resource Management, on page 409
- Radio Resource Monitoring, on page 410
- Benefits of RRM, on page 410
- Information About Configuring RRM, on page 410
- Configuring RRM (CLI), on page 411
- Viewing RRM Settings (CLI), on page 416
- RF Groups, on page 416
- Off-Channel Scanning Deferral, on page 426
- RRM NDP and RF Grouping, on page 427
- Configuring RRM NDP (CLI), on page 428
- Channels, on page 428
- Overriding RRM, on page 436
- 802.11h Parameters, on page 442
- Transmit Power Control, on page 443
- Coverage hole detection and correction, on page 446
- RF Profiles, on page 447
- XOR Radios and Flexible Radio Assignment, on page 455
- Debug RRM Issues (CLI), on page 460
- CleanAir, on page 461

Information about Radio Resource Management

The Radio Resource Management (RRM) software embedded in the Cisco Wireless Controller acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. RRM enables controllers 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 controllers 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 5-GHz and 2.4-GHz 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.

By default, each radio spends less than 2% of its time off channel.

Note Use off-channel scan deferral to prevent the AP from going off-channel when client traffic is active. For more information, see Off-Channel Scanning Deferral, on page 426.

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: 5 GHz and 2.4 GHz. The RRM algorithms run separately for each radio type (5 GHz and 2.4 GHz). 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.

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.

Configuring RRM (CLI)

Procedure

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 negligible 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.

  Note
  TPCv2 is not supported.

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:

  Note
  In Release 7.6 and later releases, disabling the 802.11 network is not required for this command.

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.

- Configure the Tx-Power Control to be aware of the channel by entering this command:

  config advanced {**802.11a** | **802.11b**} **tpcv1-chan-aware** {**enable** | **disable**}

  Note
  We recommend that you use this feature only on 802.11a (5-GHz) networks.

- 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 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.

- **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 15: 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** | **160** | **best**}—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| 160| best**} 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.
- **160** sets the channel width for the 802.11ac radio to 160 MHz.
- **best** sets the channel width for the 802.11ac radio to best suitable bandwidth.

- Configure slot-specific channel width by entering this command:

  config slot *slot-id* **chan_width***ap-name* {**20** | **40** | **80| 160**}

- **config advanced {802.11a | 802.11b} channel outdoor-ap-dca {***enable* **|** *disable***}**—Enables or disables to the controller 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 controller 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 controller 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 controller 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 controller 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 Configure 802.11a or 802.11b/g network neighbor timeout-factor by entering this command:

config {**802.11a** | **802.11b**} **monitor timeout-factor** *factor-bw-5-to-60-minutes*

If you are using Release 8.1 or a later release, we recommend that you set the timeout factor to default 20. If the access point radio does not receive a neighbor packet from an existing neighbor within 60 minutes when the default NDP interval of 180s is in use, controller deletes the neighbor from the neighbor list.

Note
The Neighbor Timeout Factor was hardcoded to 60 minutes in Release 7.6, but was changed to 5 minutes in Release 8.0.100.0.

Step 9 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 10 Save your settings by entering this command:

save config

Viewing RRM Settings (CLI)

Procedure

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.

RF Groups

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. Separate RF groups exist for 2.4-GHz and 5-GHz networks. Clustering controllers into a single RF group enables the RRM algorithms to scale beyond the capabilities of a single controller.

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 the controller.

RF grouping runs between MCs.

Configuration recommendations:

- List of country code configuration on leader and member controllers should match (should be same).
- RF grouping formation does not happen if:
  - The group leader has IPv4 address and the group member has IPv6 address.
  - The group leader has IPv6 address and the group member has IPv4 address.
- If RF grouping happens between leader and member using IPv6 address, you should also configure the IPv4 address on the group leader.
- We recommend having the same RF profile configurations on the RF group leader and member controllers.
  - Since the RRM algorithms run on the group leader, they refer to the RF profile configurations of the leader controller. For example, if there are additional channels in the member controller allowed channel list, the group leader does not consider them when assigning a channel to the radio. Similarly, if there is a difference in configuration for DBS channel width between the leader and member controller, the algorithm only refers to the configurations of the group leader.
- If any customer premise has more than 20 controllers, we recommend you have a common (non-default) RF network name for a maximum of 20 controllers. The rest of the controllers can be mapped under different RF network names.
- To have better control of the network, making a controller a static leader is preferred.

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

When APs 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

RF Group Leader can be configured in two ways as follows:

Note RF Group Leader is selected based on the controller with the greatest AP capacity (platform limit). If multiple controllers have the same capacity, the leader is selected based on the Group ID, which is a combination of the management IP address, AP capacity, random number, and so on. The one with the highest Group ID is selected as the leader.

- 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 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.

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 Grouping Failure Reason Codes

RF Grouping failure reason codes and their explanations are listed below:

Table 16: RF Grouping Failure Reason Codes

Reason Code	Description
1	Maximum number (20) of controllers are already present in the group.

Reason Code	Description
2	If the following conditions are met: • The request is from a similar powered controller and, • Controller is the leader for the other band, OR • Requestor group is larger.
3	Group ID do not match.
4	Request does not include source type.
5	Group spilt message to all member while group is being reformed.
6	Auto leader is joining a static leader, during the process deletes all the members.
9	Grouping mode is turned off.
11	Country code does not match.
12	Controller is up in hierarchy compared to sender of join command (static mode). Requestor is up in hierarchy (auto mode).
13	Controller is configured as static leader and receives join request from another static leader.
14	Controller is already a member of static group and receives a join request from another static leader.
15	Controller is a static leader and receives join request from non-static member.
16	Join request is not intended to the controller. Controller name and IP do not match.
18	RF domain do not match.
19	Controller received a Hello packet at incorrect state.
20	Controller has already joined Auto leader, now gets a join request from static leader.
21	Group mode change. Domain name change from CLI. Static member is removed from CLI.
22	Max switch size (350) is reached

Additional Reference

Radio Resource Management White Paper: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/b_RRM_White_Paper_chapter_011.html

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.

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)

Procedure

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)

Procedure

Step 1 Create an RF group by entering the **config network rf-network-name name** command:

Note
For the group name, the limit is 19 ASCII characters.

Step 2 See the RF group by entering the **show network summary** 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.

Configuring the RF Group Mode (GUI)

Procedure

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 controller.

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 controller 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 controller optimizes its own access point parameters.

Note
A configured static leader cannot become a member of another controller until its mode is set to **auto**.

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 controller as a static leader, you can add group members from the RF Group Members section as follows:

a. In the **Cisco WLC Name** field, enter the controller that you want to add as a member to this group.

b. In the **IP Address (IPv4/IPv6)** field, 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 Save the configuration.

Configuring the RF Group Mode (CLI)

Procedure

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 controller 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 controller optimizes its own access point parameters.
- *restart*—Restarts the RF group selection.

Note
A configured static leader cannot become a member of another controller until its mode is set to *auto*.

Step 2 Add or remove a controller as a static member of the RF group (if the mode is set to *leader*) by entering 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*

Viewing RF Group Status

Viewing the RF Group Status (GUI)

Procedure

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 controller, the **Update Interval** and the controller name and IP address of the **Group Leader** to this controller.

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

Tip Once a controller 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 controller 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)

Procedure

Step 1 See which controller 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 controller, how often the group information is updated (600 seconds by default), the IP address of the RF group leader, the IP address of this controller, 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 controller is currently the group leader.

Note
A * indicates that the controller has not joined as a static member.

Step 2 See which controller is the RF group leader for the 802.11b/g RF network by entering this command:
show advanced 802.11b group

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 .

Enabling Rogue Access Point Detection in RF Groups (GUI)

Procedure

Step 1 Make sure that each controller 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 controllers 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 controller.

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 controller 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 controller in the RF group.

Note
If rogue access point detection is not enabled on every controller in the RF group, the access points on the controllers with this feature disabled are reported as rogues.

Configuring Rogue Access Point Detection in RF Groups (CLI)

Procedure

Step 1 Make sure that each controller 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 controllers 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 controller.

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 controller in the RF group.

Note
If rogue access point detection is not enabled on every controller in the RF group, the access points on the controllers with this feature disabled are reported as rogues.

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 milliseconds. 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.

Configuring Off-Channel Scanning Deferral for WLANs

Configuring Off-Channel Scanning Deferral for a WLAN (GUI)

Procedure

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)

Procedure

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 between 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 milliseconds (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.

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

Step 1 To configure RRM NDP using the controller 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 controller CLI, enter this command:

show advanced 802.11{**a**|**b**} **monitor**

Channels

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.

Note In a Dynamic Frequency Selection (DFS) enabled AP environment, ensure that you enable the UNII2 channels option under the DCA channel to allow 100-MHz separation for the dual 5-GHz radios.

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.

Invoking channel update will not result in any immediate changes until the next DCA interval is triggered.

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.

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.

Procedure

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 17: DCA Sensitivity Thresholds

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

Step 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 the one managed by the controller 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
The FlexDFS functionality in this context is as follows:

Suppose RADAR is detected on an AP channel and the AP channel width is set to 40 MHz and global width is set to 80 MHz. One of the following scenarios occurs:

- If the RADAR is detected on the primary channel, the channel width changes to the globally configured value, that is 80 MHz, and a new channel is assigned.
- If the RADAR is detected on the secondary channel, the channel width changes to half of the existing width, that is 20 MHz.
- If the RADAR is detected on both the primary and secondary channels, the channel width changes to the globally configured value, that is 80 MHz, and a new channel is assigned.

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
Depending on the countries configured on the controller, only a subset of the channels are available.

Step 14 Click **Apply**.

Step 15 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 16 If you have implemented major changes to your wireless network, such as installing new APs or changing your channel plan, you must now run the startup mode. You can do this in the CLI by entering this command:

config {**802.11a** | **802.11b**} **channel global restart**

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

Procedure

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 controller 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 controller 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 controller 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.

c. In the **Neighbor Timeout Factor** box, enter the NDP timeout factor value in minutes. The valid range is 5 minutes to 60 minutes with the default value being 5 minutes.

If you are using Release 8.1 or a later release, we recommend that you set the timeout factor to default 20. If the access point radio does not receive a neighbor packet from an existing neighbor within 60 minutes when the default NDP interval of 180s is in use, the controller deletes the neighbor from the neighbor list.

Note
The Neighbor Timeout Factor was hardcoded to 60 minutes in Release 7.6, but was changed to 5 minutes in Release 8.0.100.0.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Note

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

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 controller, 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 controller, 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

If you have APs that support flexible radio assignment (FRA), you must first disable FRA and then manually set the XOR radios to the desired band.

Statically Assigning Channel and Transmit Power Settings (GUI)

Procedure

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 controller 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 controller 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 controller 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)

Procedure

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** | **160**}

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 controller would use channel 48 as the extension channel. If you choose a primary channel of 48, the controller 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** | **160** | **best**} 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.
- **160** sets the channel width for the 802.11ac radio to 160 MHz.
- **best** sets the channel width for the 802.11ac radio to best suitable bandwidth.

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 controller 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.

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 controller 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 (CLI)

Procedure

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

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)

Procedure

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)

Procedure

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** {**loud** | **quiet**} | **disable**}

Enter either **quiet** or **loud** for the **enable** parameter. When the quiet mode is enabled, all the clients who can enable 802.11h channel switch announcements should stop transmitting packets immediately because the AP detects that the radar and client devices should also quit transmitting to reduce interference. By default, the Channel Switch 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
```

Transmit Power Control

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

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. We recommend that you select TPCv1; TPCv2 option is deprecated. With TPCv1, you can select the channel aware mode; we recommend that you select this option for 5 GHz, and leave it unchecked for 2.4 GHz.

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.

Configuring Transmit Power Control (GUI)

Procedure

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 controller's dynamic power assignment mode:

- **Automatic**—Causes the controller to periodically evaluate and, if necessary, update the transmit power for all joined access points. This is the default value.
- **On Demand**—Causes the controller to periodically evaluate the transmit power for all joined access points. However, the controller updates the power, if necessary, only when you click **Invoke Power Update Now**.

  Note
  The controller 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 controller 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**.

Coverage hole detection and correction

The RRM coverage hole detection algorithm is a feature in wireless LANs that detects areas of radio coverage with insufficient radio coverage for robust radio performance. This feature alerts you when you need to add or relocate a lightweight AP.

If clients on a lightweight AP are detected at threshold levels such as RSSI, failed client count, percentage of failed packets, and number of failed packets that are lower than those specified in the RRM configuration, the AP sends a "coverage hole" alert to the controller. The alert indicates that clients cannot connect to a usable AP because of poor signal coverage.

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 AP.

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. Increasing downstream transmit power could increase interference in the network.

Configuring Coverage Hole Detection (GUI)

Procedure

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 controller 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 controller 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 controller 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 controller CLI) for a 5-second period, the client is considered to be in a pre-alarm condition. The controller 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 controller 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**.

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.

- DCA—You can configure the following DCA parameters:
  - Avoid foreign AP interference—DCA algorithm bases its optimization on multiple sets of inputs, which include detected traffic and interference from foreign 802.11 traffic access points. Each access point periodically measures interference, noise level, foreign interference, and load and maintains a list of neighbor APs. Foreign AP interference is that which is received from 802.11 non-neighbors (i.e., 802.11 APs which are not in the same RF domain – for instance a foreign 802.11 network). This interference is measured using the same mechanism as the noise level.

    Due to being out of the reach of the radio resource management module of the current deployment, such APs may be disruptive for RRM and hence the user is able to unselect their contribution to DCA in an RF profile to disable this feature.
  - Channel width—You can choose one of the following channel width options to specify the channel bandwidth supported for all 802.11n and 802.11ac radios in the 5-GHz band:
    - 20 MHz—The 20-MHz channel bandwidth (default)

Note The maximum bandwidth allowed for the 2.4-GHz band is 20 MHz.

- 40 MHz—The 40-MHz channel bandwidth
- 80 MHz—The 80-MHz channel bandwidth

- DCA channel list—You can choose a channel set used by DCA to assign one of the channels to an access point radio. The channel set selected for an RF profile must be a subset of the DCA global channel list. The available channels are preselected based on the globally configured countries. DCA compares the metrics measured on these channels and selects the most suitable channel. If the bandwidth is larger than 20 MHz, channel bonding takes place in sequential channels. For example, if the bandwidth is 40 MHz, the selected pair is 36 MHz and 40 MHz. For a higher bandwidth such as 80-MHz, the bandwidths selected are 36, 40, 44, and 48 MHz.
- Auto switch-over on Radar detection—With the enhancements made in DFS architecture, radar trigger on the serving channel AP will move to a new best channel that is confirmed by RRM Dynamic Channel Assignment (DCA) list. The channel width applied to such AP will also follow respective DCA channel width settings configured globally or under RF Profiles (if configured).
- Trap thresholds—The profile threshold for the traps can be configured for the specific AP groups based on the RF profiles.

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.

Configuring an RF Profile (GUI)

Procedure

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 Profile threshold for Traps area, enter the interference percentage, number of clients, noise level, and utilization percentage.

g) In the DCA area, select the Avoid Foreign AP interference **Enabled** check box to avoid foreign AP interference.

h) In the High-Speed Roam area, select the HSR mode **Enabled** check box to optimize high-speed roaming.

i) In the High-Speed Roam area, enter the neighbor timeout factor.

j) In the DCA area, choose one of the following channel width options to specify the channel bandwidth supported for all 802.11n and 802.11 ac radios in the 5-GHz band:

- **20 MHz**—The 20-MHz channel bandwidth (default)
- **40 MHz**—The 40-MHz channel bandwidth
- **80 MHz**—The 80-MHz channel bandwidth

k) In the DCA 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 channel numbers listed are applicable only for that particular RF profile.

The RF profile channel list must be a subset of the global channel list. That is, you may not enable a channel in the RF profile that is not enabled globally.

To configure a DCA channel list, enter this command in the CLI: **config rf-profile channel** {**add** | **delete**} *chan-profile-name*

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)

Procedure

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

Step 14 To configure the DCA parameters for an RF profile:

- To configure foreign AP interference, enter this command:

  config rf-profile channel foreign { **enable** | **disable** } *profile-name*

- To configure channel width, enter this command:

  config rf-profile channel foreign { **enable** | **disable** } *profile-name*

- To configure a DCA channel list, enter this command:

  config rf-profile channel { **add** | **delete** } *chan profile_name*

- To configure trap threshold, enter this command:

  config rf-profile trap-threshold { **clients** | **interference** | **noise** | **utilization** } *profile-name*

  - **clients**—The number of clients on an access point's radio for the trap is between 1 and 200. The default is 12.
  - **interference**—The percentage of interference threshold for the trap is from 0 to 100 percent. The default is 10 percent.
  - **noise**—The noise threshold for the trap is from -127 to 0 dBm. The default is -17 dBm.
  - **utilization**—The percentage of bandwidth being used by an access-point threshold for the trap is from 0 to 100 percent. The default is 80 percent.

Applying an RF Profile to AP Groups (GUI)

Procedure

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

Apply RF profiles to AP groups by entering this command:

config wlan apgroup profile-mapping {**add** | **delete**} *ap-group-name rf-profile-name*

XOR Radios and Flexible Radio Assignment

Cisco Flexible Radio Assignment (FRA) as a feature is a part of the Radio Resource Management (RRM) which takes the advantage of the access point's hardware to analyze NDP measurements and determine the role for the radio on the AP. The feature assigns the role for the radio to be a 2.4-GHz AP, a 5-GHz AP or to monitor the network.

In the traditional legacy dual band APs always had two radio slots, one slot per band and organized by the band they were serving - slot0= 802.11b,g,n, and slot1=802.11a,n,ac.

Note The FRA feature is enabled by default.

The Dual–Band Radio (XOR) offers the ability to serve either the 2.4 or 5-GHz bands or passively monitor both bands on the same AP. The AP models that are offered are designed to support dual 5-GHz band operations with the Cisco APs *i* model supporting a dedicated Macro/Micro architecture and the *e* and *p* models supporting Macro/Macro architecture.

When using FRA with the internal antenna (*i* series models), two 5–GHz radios may be used in a Micro/Macro cell mode. When using FRA with external antenna (*e* and *p* models) the antennas may be placed to enable the creation of two separate macro (wide area cells) or two micro cells (small cells) for HDX or any combination.

Note For *i* model APs the XOR radio when operating in 5 GHz can be set only to the lowest power level.

FRA calculates and maintains a measurement of redundancy for 2.4-GHz radios and represents this as a new measurement metric called COF (Coverage Overlap Factor). When COF is high, FRA marks 2.4GHz radio as redundant. FRA in auto mode can move redundant 2.4GHz radios to 5GHz radio mode or monitor mode. The sensitivity factor controls the threshold at which FRA will move an XOR radio out of 2.4GHz mode. High sensitivity means a lower COF threshold is required to mark a radio as redundant.

This feature is integrated into existing RRM and runs in mixed environments with legacy APs. The AP MODE selection sets the entire AP (slot 0 and slot1) into one of several operating modes including:

- Local Mode
- Monitor Mode
- FlexConnect Mode
- Sniffer Mode
- Spectrum Connect Mode

Before XOR was introduced, changing the mode of the AP propagated the change to the entire AP, both radio slots 0/1. The addition of the XOR radio in the slot0 position provides the ability to operate a single radio interface in many of the previous modes, eliminating the need to place whole AP into a mode. When this concept is applied to a single radio level, it is called “role.” Two such roles can be assigned now:

- Client Serving role
- Monitor role

Advantages of Flexible Radio Assignment

- Introduces concept of Macro/Micro cells for airtime efficiency.
- Enhances the High-Density Experience (HDX) with one AP.
- Allows more bandwidth to be applied to an area within a larger coverage cell.
- Can be used to address nonlinear traffic.
- Permits one AP with one Ethernet drop to function like two 5–GHz APs.
- Creating two diverse 5–GHz cells doubles the airtime.
- XOR radio can be user-selected in either band servicing clients or in monitor mode.
- Reduces 2.4–GHz overcoverage issues.

Additional References

- *Feature Matrix for Wave 2 and 802.11ax (Wi-Fi 6) Access Points*: https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html
- *Flexible Radio Assignment (FRA) and Redundant Radios*: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/b_RRM_White_Paper_chapter_01000.html

Configuring Flexible Radio Assignment-Global (GUI)

Procedure

Step 1 Choose **Wireless** > **Advanced** > **Flexible Radio Assignment** to open the **Flexible Radio Assignment Configuration** page.

Step 2 Select **Enable** to enable Flexible Radio Assignment feature.

- 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 From the Sensitivity drop-down list,

- Low
- Medium
- High

Step 4 From the **Interval** drop-down list, select the interval in hours.

Default is 1 hour.

Step 5 From the **Service Priority** drop-down list choose the priority for the FRA service from the following options:

- Coverage
- Client Aware–Enter the percentage values for the **Client Select** and **Client Reset** fields.
- Service Assurance-Choose the sensor threshold from the following options:
  - Balanced
  - Client-preferred
  - Client-priority
  - Sensor-preferred
  - Sensor-priority

Step 6 Save the configuration.

Configuring Flexible Radio Assignment (CLI)

Procedure

Step 1 Enable or disable FRA by entering this command:

config advanced fra {**enable** | **disabled**}

Step 2 Reset the radio to 2.4 GHz by entering this command:

config advanced fra revert {**all** | `auto-only`} { **static** | **auto**}

Note
Use this command to reset the radio to 2.4-GHz band from 5-GHz band after disabling the FRA feature.

Step 3 Set the FRA interval time in hours by entering this command:

config advanced fra interval

Step 4 Set the FRA coverage overlap sensitivity by entering this command:

config advanced fra sensitivity {**high** | **medium** | **low**}

Step 5 Configure the client aware FRA feature by entering this command:

config advanced fra client-aware {**client-select** | **client-reset**}*percentage*

Valid range is 0 to 100.

Step 6 Configure the FRA sensor service priority by entering this command:

config advanced fra service-priority{**client-aware** | **coverage** | **service-assurance**}

Step 7 Configure the FRA sensor threshold by entering this command:

config advanced fra sensor-threshold{**balanced** | **client-preferred** | **client-priority** | **sensor-preferred** | **sensor-priority**}

Step 8 View the FRA status by entering this command:

show advanced fra

Configuring Flexible Radio Assignment for AP (GUI)

Procedure

Step 1 Choose **Wireless** > **Radio** > **Dual-band radios** to open the **Dual-band radios** page.

Step 2 Hover your cursor over the blue drop-down arrow on the AP of choice and choose **Configure**.

Step 3 In the **802.11a/b/g/n Cisco APs Configure** page, select **Auto** under the Radio Role Assignment section to push FRA to decide the role and the band.

Step 4 In the **802.11a/b/g/n Cisco APs > Configure** page, select **Manual** under the Radio Role Assignment section.

Step 5 Choose the mode for the selected AP from the following options:

- Client Serving–When the radio role is Client Serving, you can set the radio band.
  - 2.4 GHz
  - 5 GHz

- Monitor

Step 6 Save the configuration.

Configuring Auto Radio Role of the XOR Radio (CLI)

Procedure

Step 1 Disable the radio of the XOR radio by entering this command:
config 802.11-abgn disable *ap-name*

Step 2 Change the role of the XOR radio by entering this command:
config 802.11-abgn role *ap-name* **auto**

Step 3 Enable the XOR radio by entering this command:
config 802.11-abgn enable *ap-name*

Configuring Manual Radio Role for the AP (CLI)

Procedure

Step 1 Disable the radio on the AP by entering this command:
config 802.11-abgn disable *ap-name*

Step 2 Change the Role of the AP by entering one of the following commands:

- Change the role to monitor:

  config 802.11-abgn role *ap-name* **monitor**

- Change the role to client-serving:

  config 802.11-abgn role *ap-name* **client-serving**

Step 3 Enable the radio on the AP by entering this command:
config 802.11-abgn enable *ap-name*

Configuring Radio Band for Client-Serving Radio (CLI)

Procedure

Step 1 Disable the radio on the AP by entering this command:
config 802.11-abgn disable *ap-name*

Step 2 Change the band of the AP by entering this command:
config 802.11-abgn band *ap-name* {**2.4GHz** | **5GHz**}

Step 3 Enable the radio on the AP by entering this command:
config 802.11-abgn enable *ap-name*

Debug RRM Issues (CLI)

Procedure

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.

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 controller. The controller controls the access points, collects spectrum data, and forwards information to Cisco Prime Infrastructure or Cisco Connected Mobile Experiences (CMX) 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 controller 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 Cisco Prime Infrastructure and Cisco CMX.

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.

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 controller and this information is used to mitigate interfering channels.

Persistent Device Awareness (PDA)

This relies on detection by a CleanAir AP. The neighbors of the detecting AP can have the PDA information shared through RRM and the channel information biased to help a non-CleanAir AP avoid the interference for a given channel.

Persistent Device Detection

CleanAir-capable Monitor Mode access point collects information about persistent devices on all configured channels and stores the information in the controller. Local/Bridge mode AP detects interference devices on the serving channels only.

Persistent Device 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 controller 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.

Detecting Persistent Sources of Interference

Procedure

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*

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 utilization.
- 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

- 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.
- For 4800 AP slot 1 5 GHz is dedicated and cannot be individually moved to monitor mode. However, slot 0 is XOR and can be moved to monitor as well as 2.4/5 GHz. 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 already available in both 2.4/5GHz. 3700 AP has dedicated 2.4GHz (slot0) and 5GHz (slot1).
- Do not connect access points in SE connect mode directly to any physical port on the controller.
- CleanAir is not supported wherein the channel width is 160 MHz.

Configuring Cisco CleanAir on the Controller

Configuring Cisco CleanAir on Controller (GUI)

Procedure

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 controller from detecting spectrum interference. By default, this feature is in enabled 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 controller 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 controller. 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, except BLE Beacon. 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

APs that are associated with the controller 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 controller or Prime Infrastructure. Filtering allows the system to resume normal performance levels.

Prior to Release 8.7, if CleanAir was enabled, by default, the BLE Beacon was included in the list of interferences to be detected. In 8.7 and later releases, the functionality is changed wherein the BLE Beacon is by default excluded from the list of interferences to be detected. This change in functionality is made to eliminate unwanted off-channel scans to improve performance. If you want the BLE Beacon to be detected, you will have to explicitly add it to the list of interferences to be detected.

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 threshold 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 controller 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 controller 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) To configure rogue duty cycle, check the **Rogue Contribution** check box and then specify the **Rogue Duty-Cycle** in terms of percentage. The default value of **Rogue Duty-Cycle** is 80%.

f) Save the configuration.

Configuring Cisco CleanAir on Controller (CLI)

Procedure

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 controller does not receive any spectrum data. By default, this feature is in enabled 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 with the controller 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 controller or Prime Infrastructure. Filtering allows the system to resume normal performance levels.

Prior to Release 8.7, if CleanAir was enabled, by default, the BLE Beacon was included in the list of interferences to be detected. In 8.7 and later releases, the functionality is changed wherein the BLE Beacon is by default excluded from the list of interferences to be detected. This change in functionality is made to eliminate unwanted off-channel scans to improve performance. If you want the BLE Beacon to be detected, you will have to explicitly add it to the list of interferences to be detected.

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 Configure and monitor Interference Awareness by entering the following commands:

- **config advanced** {**802.11a** | **802.11b**} **channel cleanair-event** {**enable** | **disable**}
- **config advanced** {**802.11a** | **802.11b**} **channel cleanair-event rogue-contribution** {**enable** | **disable**}
- **config advanced** {**802.11a** | **802.11b**} **channel cleanair-event rogue-contribution duty-cycle** *value*
- **show** {**802.11a** | **802.11b**} **cleanair config**
- **debug airewave-director profile enable**
- **debug airewave-director channel enable**

Step 12 Enable persistent devices propagation by entering this command:

config advanced {**802.11a** | **802.11b**} **channel pda-prop** {**enable** | **disable**}

Step 13 Save your changes by entering this command:

save config

Step 14 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 15 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)

Procedure

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.

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)

Procedure

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)
```

Configuring Spectrum Intelligence

Information About Spectrum Intelligence

This feature scans for non-Wi-Fi radio interference on 2.4 and 5 GHz bands. The feature supports client serving mode and monitor mode.

Restrictions on Spectrum Intelligence

- Only the following Cisco APs support Spectrum Intelligence:
  - Cisco Aironet 1800 APs
  - Cisco Aironet 1810 APs
  - Cisco Aironet 1815 APs
  - Cisco Aironet 1832 APs
  - Cisco Aironet 1852 APs
  - Cisco Aironet 1542 APs
- No mitigation of interferer.
- Limited to detect three types of devices.
  - Microwave
  - Continuous wave—video recorder, baby monitor
  - SI-FHSS—Bluetooth, Frequency hopping DECT phones
- Cannot differentiate between devices of the same type.
- Does not report to the CleanAir Infrastructure - it is only reported in the controller.
- When the AP is in Local Mode, it reports the first interference detected.
- When in Monitor Mode, it reports all three types of interference if present.
- Does not provide location as only RSSI is measured at the reporting APs.
- Does not alert through Cisco Prime Infrastructure.
- Does not send information to CMX or MSE (as CleanAir does).
- It cannot provide location of interfering device.

Configuring Spectrum Intelligence – Global (GUI)

Procedure

Step 1 Choose **Wireless** > **802.11a** > **CleanAir** to open the CleanAir page.

Step 2 Check **Spectrum Intelligence** to enable the Spectrum Intelligence feature.

This enables Spectrum Intelligence feature on all the APs which support Spectrum Intelligence.

Step 3 Click **Apply**.

Step 4 To view the APs supporting Spectrum Intelligence, choose **Wireless** > **Access Points** > **Radios** > **802.11a/b** to open the **802.11a/b Radio** page.

The names of the APs that are spectrum intelligence capable have $ as a suffix.

Configuring Spectrum Intelligence per AP (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **Radios** > **802.11a/b** to open the 802.11a/b radio page.

Step 2 The names of the APs that are spectrum intelligence capable have $ as a suffix. Hover your cursor over the blue drop-down arrow in front of the AP name with the $ sign. Click **Configure**.

The Cisco APs > Configure page is displayed.

Step 3 Under the **Spectrum Intelligence** section, from the **Spectrum Intelligence Admin Status** drop-down list, choose **Enable** or **Disable** option.

Step 4 Click **Apply**.

Configuring Spectrum Intelligence (CLI)

Procedure

- Configure spectrum intelligence globally on all spectrum intelligence capable APs or on an individual AP by entering this command:

  config {802.11a | 802.11b} SI {enable | disable} *network* | *ap-name*

- View the global admin status by entering this command:

  show {802.11a | 802.11b} SI config

- View interferences by AP by entering this command:

  show {802.11a | 802.11b} SI device ap *ap-name*

- View interferences by interferer type by entering this command:

show {802.11a | 802.11b} SI device-type *interferer_type_name*

Monitoring Interference Devices

Prerequisites for Monitoring the Interference Devices

You can configure Cisco CleanAir only on CleanAir-enabled access points.

Monitoring the Interference Device (GUI)

Procedure

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)

Detecting Interferers by an Access Point

Procedure

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

Procedure

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
  - **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.

Monitoring Persistent Devices (GUI)

Procedure

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)

Procedure

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_1572_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 2020
```

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 controller GUI and CLI.

Monitoring the Air Quality of Radio Bands (GUI)

Procedure

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)

Viewing a Summary of the Air Quality

Procedure

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

Procedure

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)

Procedure

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)

Procedure

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

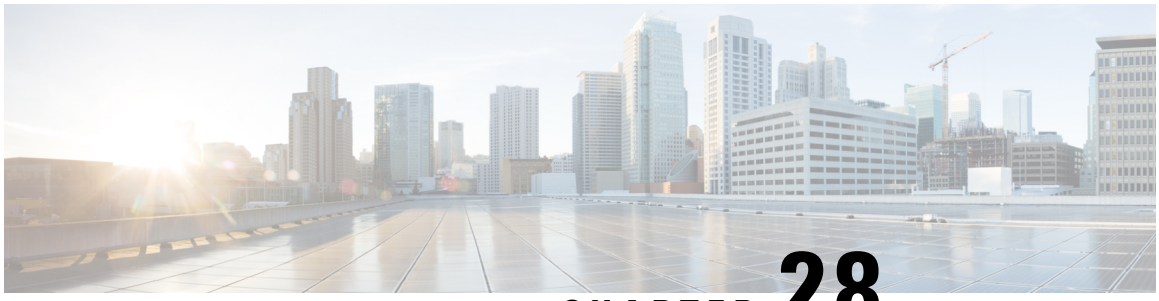
- **wimax-fixed**—A WiMAX fixed device
- **wimax-mobile**—A WiMAX mobile device

- **802.11b**
  - **bt-link**—A Bluetooth link device
  - **bt-discovery**—A Bluetooth discovery device
  - **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 28

Wireless Quality of Service

- Call Admission Control, on page 485
- Application Visibility and Control, on page 502
- NetFlow, on page 514
- QoS Profiles, on page 517
- Cisco Air Time Fairness, on page 524

Call Admission Control

This section contains the following subsections:

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:

Configuring Voice Parameters

Configuring Voice Parameters (GUI)

Procedure

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, 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. The **Voice** tab is displayed by default.

Step 4 (Optional) Check 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** field, 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** field, 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, check the **Expedited Bandwidth** check box. By default, this field is disabled.

Step 9 To enable SIP CAC support, check 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)** field, enter the bandwidth in kilobits per second.

The possible range is 8 to 64.

The default value is 64.

Note
The **SIP Bandwidth (kbps)** field 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)** field is set to 64. If you choose the SIP codec as G.729, the SIP Bandwidth (kbps) field is set to 8.

Step 12 In the **SIP Voice Sample Interval (msecs)** field, enter the value for the sample interval.

Step 13 In the **Maximum Calls** field, 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 Check 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, check 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.

Procedure

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 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.

Step 13 Configure voice automatically for a WLAN by entering this command:

config auto-configure voice cisco *wlan-id* **radio** {**802.11a** | **802.11b** | **all**}

Step 14 Enter the **save config** command to save your settings.

Configuring Video Parameters

Configuring Video Parameters (GUI)

Procedure

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.

Procedure

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)

Procedure

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)

Procedure

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.

Procedure

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)

Procedure

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**}

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)

Procedure

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)

Procedure

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

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)

Procedure

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. The WMM option is default and we recommend this setting if you have SpectraLink phones deployed in your network.
- **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 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. This setting is not recommended because it is deprecated.

  Note
  If you deploy video services, admission control must be disabled.

- **Fastlane**—Enables fastlane EDCA parameters. This setting is recommended for use with Apple client devices.

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

Step 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)

Procedure

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 |fastlane**}

- **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.

- **Fastlane**—Enables Fast Lane EDCA parameters.

Step 4 View the current status of MAC (low latency 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
The low latency MAC option is not supported.

This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight APs. This, in turn 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**.

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:

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.

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).

Procedure

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**

Procedure

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**

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.

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

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

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

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 controller to AP through CAPWAP. It does not change the DSCP of the original packet.

Traffic flows are analyzed and recognized using the NBAR2 engine for CAPWAP data at the controller and for FlexConnect locally switched data, analysis is done at the AP. For more information about the NBAR2 Protocol Library, see http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/

nbar-prot-pack-library.html. The specific flow is marked with the recognized protocol or application, such as WebEx. This per-flow information can be used for application visibility using Flexible NetFlow (FNF).

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

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.

The number of concurrent flows supported for AVC classification on different controller platforms are noted in the following table.

Controller Platform	Flow
Cisco 3504 Wireless Controller	183750
Cisco 5520 Wireless Controller	336,000
Cisco 8540 Wireless Controller	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.

AAA override for AVC profiles

The AAA attribute for client or user profile is configured on the AAA server using authentication from RADIUS server or Cisco ACS or ISE. The AAA attribute is processed during layer 2 or layer 3 authentication by the controller and the same is overridden by what is configured on the WLAN.

The AAA AVC profile is defined as a Cisco AV pair. The string option is defined as **avc-profile-name** and this value has to be configured for any AVC profile available in the controller.

Default DSCP Value for AVC Profile

Prior to Release 8.8 with AVC enabled, you could override DSCP values for only those application flows that were configured on an AVC profile. For the application flows that were not configured, no action was performed and DSCP was left intact. The maximum number of application rules that the AVC profile can contain is 32. For managed service, to control and rewrite DSCP values (example with DSCP 0) for all flows that are not presented on the AVC profile is not possible.

In Release 8.8, the new enhancement includes a new *default-class* rule that you can use to override the DSCP values for all application flows in which AVC rule is not configured. The goal of this enhancement is to protect the network for all flows with unwanted or controlled DSCP values.

This enhancement comes with the following restrictions:

- Only the start of an application flow is captured.
- Supported only for marking. Rate limit and drop are not supported.
- Default DSCP works only if AVC is in enabled state.
- An AVC profile can support up to 32 rules, including the *default-class* rule. If the *default-rule* is configured, you can configure up to 31 rules.
- Multicast and broadcast traffic is not supported.
- IPv6 is not supported in AVC.
- Cascading of rules is not supported, which means that for the same flow, it is not possible to have rate limiting and marking. Therefore, if rate limiting is performed for a flow, *default* marking is not performed on the flow.

This section contains the following subsections:

Restrictions for Application Visibility and Control

- IPv6 packet classification is not supported.
- Layer 2 roaming across controllers is not supported.
- Multicast traffic is not supported.
- Controller GUI support is not present for the AVC Protocol Pack feature.
- You can apply rate limiting to up to 3 applications.
- Each application can be configured with one rule only. An application cannot have both a rate limit and a Mark rule.
- If the standby controller has a different protocol pack version that is installed before pairing, then the active and standby controllers will have different protocol packs versions after pairing, in a HA environment. In the standby controller, the transferred protocol pack takes the preference over the default protocol pack.

  For example, the controller with the software release 8.0 contains Protocol Pack version 9.0 by default. Before pairing, if one of the controllers has a Protocol Pack version 11.0 that is installed, then after pairing one controller contains Protocol Pack version 9.0 and the other controller contains Protocol Pack 11.0 installed.

Configuring Application Visibility and Control (GUI)

Procedure

Step 1 Create and configure an AVC profile by following these steps:

a) Choose **Wireless** > **Application Visibility and Control** > **AVC Profiles**.
b) Click **New** and enter the AVC profile name.
c) Click **Apply**.
d) On the AVC Profile Name page, click the AVC profile name to open the AVC Profile > Edit page.
e) Click **Add New Rule**.
f) Choose the application group and the application name from the respective drop-down lists.

See the list of default AVC applications available by choosing **Wireless** > **Application Visibility and Control** > **AVC Applications**.

g) 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 permit all applications.

h) 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 quality of service 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 the high-quality video applications.
- **Silver (Best Effort)**—Supports the 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.

i) Click **Apply**.
j) Click **Save Configuration**.

Step 2 Associate an AVC profile to a WLAN by following these steps:

a) Choose **WLANs** and click the WLAN ID to open the WLANs > Edit page.
b) In the QoS tab, choose the AVC profile from the AVC Profile drop-down list.
c) Click **Apply**.
d) 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**}

AVC-based Reanchoring

This feature is designed to reanchor clients when they roam from one controller to another controller. Reanchoring of Apple clients prevents depletion of IP addresses available for new clients in controller. The AVC profile-based statistics is used to decide whether the client must be reanchored or deferred. This is useful when the client is actively running voice or video application defined in the AVC rules.

The clients get deauthenticated when they are not transmitting any traffic for applications listed in the AVC rules when they are roaming between controllers.

Guidelines and Restrictions for AVC-based Reanchoring

- This feature is supported only in Central Switch mode.
- Some Apple clients roaming to another controller fails to reassociate with the new controller with the new IP address. These clients do not release the old IP address and therefore do not re-associate with the current controller.
- If the Wi-Fi calling signature in any application is changed and AVC fails to recognize this signature, this rule stops working.
- For the client to roam between controllers:
  - The controllers must be in the same mobility group.
  - Roaming is limited to within the same SSID.
- For the updated configuration to be available via CLI or GUI, we recommend that you refresh the interface. However, this is not required for the updated information to be visible on the Monitoring page in the GUI.

This section contains the following subsections:

Configuring AVC-based Selective Reanchoring (GUI)

Procedure

Step 1 Choose **WLANs** and click the WLAN ID.

Step 2 Click the **QoS** tab.

Step 3 Check the **Application Visibility** check box.

Step 4 Click **Advanced** tab.

Step 5 In the **Mobility** section, check the **AVC Based Reanchor** check box.

Step 6 Click **Apply** to save the configuration.

Step 7 (Optional) To add rules in the AVC profile:

a) Choose **Wireless** > **Application Visibility and Control** > **AVC Profiles** page.

b) Select the AVC profile **AVC_BASED_REANCHOR**.

This profile by default contains Jabber-Audio, Jabber-Video, WebEx, and Wifi calling applications.

c) Click **Add New Rule**.

d) From the **Application Group** drop-down list, choose the application from the various options available.

e) From the **Application Name** drop-down list, choose the application name from the various options available.

f) Click **Apply**.

Note
When enabling AVC-based re-anchoring, the action function is disabled for the application profiles.

Step 8 (Optional) To delete rules from the AVC profile

a) Choose **Wireless** > **Application Visibility and Control** > **AVC Profiles** page.

b) Hover your cursor over the blue drop-down arrow for the rule.

c) Click **Remove**.

Note
The **AVC_BASED_REANCHOR** AVC profile can contain up to 32 applications as rules.

Configuring AVC-based Selective Reanchoring (CLI)

Procedure

Step 1 Enable Application Visibility on a WLAN by entering this command:

config wlan avc *wlan-id* **visibility enable**

Step 2 Enable Selective Reanchoring feature on a WLAN by entering this command:

config wlan mobility selective re-anchoring enable *wlan-id*

Step 3 Disable Selective Reanchoring feature on a WLAN by entering this command:

config wlan mobility selective re-anchoring disable *wlan-id*

Step 4 View the status of Selective Reanchor by entering this command:

show wlan *wlan-id*

Step 5 View the Reanchor statistics by entering this command:

show mobility statistics

Application Visibility Control for FlexConnect

AVC provides application-aware control on a wireless network and enhances manageability and productivity. AVC is already supported on ASR and ISR G2 and controller platforms. The support of AVC embedded within the FlexConnect AP extends as this is an end-to-end solution. This gives a complete visibility of applications in the network and allows the administrator to take some action on the application.

AVC has the following components:

- Next-generation Deep Packet Inspection (DPI) technology, called Network Based Application Recognition (NBAR2), allows for identification and classification of applications. NBAR is a deep-packet inspection technology available on Cisco IOS-based platforms, which supports stateful L4 to L7 classification. NBAR2 is based on NBAR and has extra requirements such as having a common flow table for all IOS features that use NBAR. NBAR2 recognizes application and passes this information to other features such as Quality of Service (QoS), and Access Control List (ACL), which can take action based on this classification.
- Ability to Apply Mark using QoS, Drop and Rate-limit applications.

The important use cases for NBAR AVC are capacity planning, network usage base lining, and better understanding of the applications that are consuming bandwidth. Trending of application usage helps the network administrator to plan for network infrastructure upgrade, improve quality of experience by protecting important applications from bandwidth-hungry applications when there is congestion on the network, capability to prioritize or de-prioritize, and drop some application traffic.

Supported Hardware

- Supported Access Points—All Wave 2 and 802.11ax APs
- Supported Controllers—3504, 5520, 8540, and vWLC
- Supported Modes—FlexConnect and Flex+Bridge mode

Restrictions for AVC for FlexConnect

- IPv6 packet classification is not supported.
- Multicast traffic is not supported.
- Downloading the AVC Protocol Pack is not supported on FlexConnect APs.
- You can apply rate limiting to up to 3 applications.
- Only one rule can be configured per application. An application cannot have both a rate limit as well as a Mark rule.
- A maximum of 31 rules can be configured in a profile. You can configure a maximum of 16 profiles in the complete system.
- AAA override of AVC profiles is not supported.
- By design, WLAN-level FlexConnect AVC stats are not supported.
- When the AP is in a FlexGroup and the FlexGroup does not have FlexConnect AVC configured, then FlexConnect AVC configuration is not pushed to the AP from the controller.
- Netflow Export from controller is not supported.

- In the stats, DHCP information is not supported on the controller.
- Foreign anchor scenario: AVC for FlexConnect statistics can be seen only on the foreign controller.
- FlexConnect Group AVC configuration:
  - WLAN AVC configuration is not inherited when the AP is part of FlexConnect group.
  - It is mandatory to configure AVC for FlexConnect on a FlexConnect Group if the AP is part of the FlexConnect group, if you want to push the AVC for FlexConnect configuration to the AP.
  - If a FlexConnect AP is not part of a FlexConnect group, local switching WLAN AVC configuration is pushed to the FlexConnect AP.

This section contains the following subsections:

Configuring Application Visibility and Control for FlexConnect (GUI)

Procedure

Step 1 To create a FlexConnect AVC profile and add a rule:

a) Choose **Wireless** > **Application Visibility and Control** > **FlexConnect AVC Profiles** and click **New**.
b) Specify the FlexConnect profile name and click **Apply**.
c) Click the profile name and click **Add New Rule**.
d) Specify the **Application Group**, **Application Name**, and **Action** and click **Apply**.

Step 2 To check the visibility globally for all WLANs on a FlexConnect Group, choose **Monitor** > **Applications** > **FlexConnect Groups** and select the FlexConnect group that you created earlier.
This page provides more granular visibility per FlexConnect group and lists the top 10 applications in the last 90 seconds, as well as cumulative stats for the top 10 applications. You can view upstream and downstream statistics individually per FlexConnect group on the same page by clicking the **Upstream** and **Downstream** tabs.

You can set the number of applications that are displayed on this page through the **Max Number of Records** drop-down list. The default value is 10.

Step 3 To specify more granular visibility of the top 10 applications per client on a locally switched WLAN where AVC visibility is enabled, choose **Monitor** > **Applications** > **FlexConnect Groups**, select the FlexConnect group name and click the **Client** tab. Then, click any individual client MAC address entry listed on the page. This page provides further granular statistics per client associated on locally switched WLANs where AVC visibility is enabled on the WLAN itself or on the FlexConnect Group, and lists the top 10 applications in last the 180 seconds as well as cumulative stats for top 10 applications. You can view upstream and downstream stats individually per-client from same page by clicking the **Upstream** and **Downstream** tab. You can set the number of applications that are displayed on this page through the **Max Number of Records** drop-down list. The default value is 10.

Configuration Example

Procedure

Step 1 Create an open WLAN.

An open WLAN has Layer 2 security set to **None**.

Step 2 Enable FlexConnect Local Switching on the WLAN and click **Apply.**

a) On the **WLANs** page, click the WLAN ID.
b) On the **WLANs > Edit** page, click the **Advanced** tab.
c) In the FlexConnect area, select the **FlexConnect Local Switching** check box.

Step 3 Ensure that the APs connected to this WLAN are among the list of supported access points for this feature. Set the APs in FlexConnect mode.

a) Choose **Wireless** > **Access Points** > **All APs**.
b) Click the AP name.
c) From the **AP Mode** drop-down list, select **FlexConnect** and click **Apply**.

Step 4 Create a FlexConnect group and add the AP to the FlexConnect group.

a) Choose **Wireless** > **FlexConnect Groups**.
b) Click **New** and enter the name of the FlexConnect group, and then click **Apply**.
c) On the **FlexConnect Groups > Edit** page, in the FlexConnect APs area, click **Add AP**.
d) You can either select an AP from a list of APs associated with the controller or directly specify the Ethernet MAC address of the AP that is associated with the controller.
e) Click **Add**.

Note
Applications that can be identified, classified, and controlled are listed under **Wireless** > **Application Visibility and Control** > **FlexConnect AVC Applications**. The access points support Protocol Pack version 8.0 and NBAR engine version 16.

Step 5 Create an AVC profile and add a rule.

Note
A FlexConnect AVC profile can have a maximum of 32 rules.

a) Choose **Wireless** > **Application Visibility and Control** > **FlexConnect AVC Profiles** and click **New**.
b) Specify the FlexConnect profile name and click **Apply**.
c) Click the profile name and click **Add New Rule**.
d) Specify the **Application Group**, **Application Name**, and **Action** and click **Apply**.

Step 6 Enable AVC on the FlexConnect group and apply the FlexConnect AVC profile to the FlexConnect group.

a) Choose **Wireless** > **FlexConnect Group** and click the FlexConnect group name.
b) Click the **WLAN AVC Mapping** tab.
c) Specify the WLAN ID and from the **Application Visibility** drop-down list, choose **Enable**.
d) From the **Flex AVC Profile** drop-down list, choose the FlexConnect AVC profile, and click **Add**.
e) Click **Apply**.

Step 7 After Application Visibility is enabled on the FlexConnect Group, you can start different types of traffic (from the associated wireless client) using the applications (already installed) such as Cisco Jabber, Skype, Yahoo Messenger, HTTP, HTTPS/SSL, YouTube, Ping, Trace route.
After traffic is initiated from the wireless client, visibility of different traffic can be observed on a per-FlexConnect Group and per-client basis. This provides a good overview to the administrator of the network bandwidth utilization and type of traffic in the network per-client and per-branch site.

Step 8 To check the visibility globally for all WLANs on a FlexConnect Group, choose **Monitor** > **Applications** > **FlexConnect Groups** and select the FlexConnect group that you created earlier.
This page provides more granular visibility per FlexConnect group and lists the top 10 applications in the last 90 seconds, as well as cumulative stats for the top 10 applications. You can view upstream and downstream statistics individually per FlexConnect group on the same page by clicking the **Upstream** and **Downstream** tabs.

You can set the number of applications that are displayed on this page through the **Max Number of Records** drop-down list. The default value is 10.

Step 9 To specify more granular visibility of the top 10 applications per client on a locally switched WLAN where AVC visibility is enabled, choose **Monitor** > **Applications** > **FlexConnect Groups**, select the FlexConnect group name and click the **Client** tab. Then, click any individual client MAC address entry listed on the page. This page provides further granular statistics per client associated on locally switched WLANs where AVC visibility is enabled on the WLAN itself or on the FlexConnect Group, and lists the top 10 applications in last the 180 seconds as well as cumulative stats for top 10 applications. You can view upstream and downstream stats individually per-client from same page by clicking the **Upstream** and **Downstream** tab. You can set the number of applications that are displayed on this page through the **Max Number of Records** drop-down list. The default value is 10.

Step 10 Click **Clear AVC Stats** to clear all the AVC statistics for a particular client.

Configuring Application Visibility and Control for FlexConnect (CLI)

Procedure

- Configure a FlexConnect AVC profile by entering this command:
  config flexconnect avc profile *profile-name* {**create** | **delete**}
- Add a rule for a FlexConnect AVC profile by entering this command:
  config flexconnect avc profile *profile-name* **rule add application** *app-name* {**drop** | {**mark** *dscp-value* {**upstream** | **downstream**}}}
- Delete a rule for a FlexConnect AVC profile by entering this command:
  config flexconnect avc profile *profile-name* **rule remove application** *app-name*
- Apply rule changes to a FlexConnect AVC profile by entering this command:
  config flexconnect avc profile *profile-name* **apply**
- Apply FlexConnect group AVC profile to a WLAN by entering this command:
  config flexconnect group *group-name* **avc** *wlan-id* **visibility wlan-specific**
- See a summary of FlexConnect AVC profiles or detailed information about one FlexConnect AVC profile by entering this command:
  - **show flexconnect avc profile summary**
  - **show flexconnect avc profile detailed** *profile-name*

Note The FlexConnect AVC profile rules are pushed to the AP only when the rules are in 'Applied' state.

- Troubleshooting command:
  debug flexconnect avc {**event** | **error** | **detail**} {**enable** | **disable**}
- Monitoring commands to be entered on the AP console:
  a) Check whether the FlexConnect AVC profiles are present on the AP by entering this command:
  show policy-map
  b) See statistics for each application in the FlexConnect AVC profile by entering this command:
  show policy-map target
  c) Check the applications present in the FlexConnect AVC profiles by entering this command:
  show class-map
  d) See WLAN and FlexConnect AVC mapping on the AP by entering this command:
  show dot11 qos

Configuration Example

Before you begin

Ensure that you have created an open WLAN.

Procedure

Step 1 Enable FlexConnect local switching on the WLAN:
config wlan flexconnect local-switching *wlan-id*

Step 2 Ensure that the APs connected to this WLAN are among the list of supported access points for this feature. Set the APs in FlexConnect mode.
config ap mode flexconnect submode none

Step 3 Create a FlexConnect group and add the AP to the FlexConnect group:
a) **config flexconnect group** *group-name* **add**
b) **config flexconnect group** *group-name* **ap add** *ap-mac-addr*

Step 4 Create a FlexConnect AVC profile and add a rule:

Note
A FlexConnect AVC profile can have a maximum of 32 rules.

a) **config flexconnect avc profile** *profile-name* **create**
b) **config flexconnect avc profile** *profile-name* **rule add application** *app-name* {**drop** | **mark**}

Step 5 Enable AVC on the FlexConnect group and apply the FlexConnect AVC profile to the FlexConnect group.
a) **config flexconnect group** *group-name* **avc** *wlan-id* **visibility enable**
b) **config wlan avc** *wlan-id* **visibility enable**
c) **config wlan avc** *wlan-id* **flex-profile** *profile-name* **enable**

Step 6 Configure the FlexConnect group AVC to a WLAN in local switching mode.

config flexconnect group *group-name* **avc** *wlan-id* **visibility wlan-specific**

Step 7 After Application Visibility is enabled on the FlexConnect Group, you can start different types of traffic (from the associated wireless client) using the applications (already installed) such as Cisco Jabber, Skype, Yahoo Messenger, HTTP, HTTPS/SSL, YouTube, Ping, Trace route.
After traffic is initiated from the wireless client, visibility of different traffic can be observed on a per-FlexConnect Group and per-client basis. This provides a good overview to the administrator of the network bandwidth utilization and type of traffic in the network per-client and per-branch site.

Step 8 To check the visibility globally for all WLANs on a FlexConnect Group:

show flexconnect avc statistics

Step 9 To see a summary of AVC for FlexConnect profiles or detailed information about one AVC for FlexConnect profile:

- **show flexconnect avc profile summary**
- **show flexconnect avc profile detailed** *profile-name*

Note
The AVC profile rules are pushed to the AP only when the rules are in 'Applied' state.

Step 10 To troubleshoot AVC for FlexConnect:

debug flexconnect avc {**event** | **error** | **detail**} {**enable** | **disable**}

Step 11 Monitoring commands to be entered on the AP console:

a) Check whether the FlexConnect AVC profiles are present on the AP by entering this command:
show policy-map

b) See statistics for each application in the FlexConnect AVC profile by entering this command:
show policy-map target

c) Check the applications present in the FlexConnect AVC profiles by entering this command:
show class-map

d) See WLAN and FlexConnect AVC mapping on the AP by entering this command:
show dot11 qos

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.

NetFlow has added an enhanced template in Release 8.2 using the Version 9 export format, which provides additional 17-field information about the flow. This report is compatible with third-party NetFlow collectors, including Lancope. The minimum supported protocol pack version is 14 with NBAR engine version 23.

The following are the template enhancements in NetFlow Version 9 :

- New features can be added to NetFlow quickly, without breaking existing implementations.
- NetFlow is future-proofed against new or developing protocols, because NetFlow Version 9 can be adapted to provide support for those protocols.
- NetFlow Version 9 is the IETF standard mechanism for information export.
- Third-party business partners who produce applications that provide collector or display services for NetFlow are not required to recompile their applications each time a new NetFlow feature is added.

Table 18: List of data points in a NetFlow template

Existing Template [2]: ipv4_client_app_flow_record	**Enhanced template [3]: ipv4_client_src_dst_flow_record**
applicationTag	applicationTag
ipDiffServCodePoint	staMacAddress
octetDeltaCount	wtpMacAddress
packetDeltaCount	WlanID
postIpDiffServCodePoint	Source IP
staIPv4Address	Dest IP
staMacAddress	Source Port
wlanSSID	Dest Port
wtpMacAddress	Protocol
—	Start Time
—	End Time
—	Direction
—	Packet count
—	Byte count
—	VLAN id

Existing Template [2]: ipv4_client_app_flow_record	Enhanced template [3]: ipv4_client_src_dst_flow_record
—	TOS
—	Client username

[2] Supported on Cisco 5520, 8540 Wireless Controllers
[3] Supported on Cisco 5520 and 8540 Wireless Controllers

Restrictions for Using Netflow

- The enhanced template is supported only on Cisco 3504, 5520, and 8540 controllers.
- NetFlow is not supported on Cisco Virtual Wireless Controller (vWLC).
- FlexConnect mode is not supported.
- IPv6 traffic is not supported.
- Only one collector and exporter each can be configured.

Configuring NetFlow (GUI)

Before you begin

You have to enable AVC before enabling netflow on a WLAN.

Procedure

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
- Client Source and Destination Record—Higher Visibility

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 the new template record by entering this command:

  config flow {**add** | **delete**} **monitor** *monitor-name* **record ipv4_client_src_dst_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**}

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 19: 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
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 most significant 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:

Configuring QoS Profiles (GUI)

Procedure

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)

Procedure

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**}

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.

Procedure

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.

Procedure

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
...
```

Cisco Air Time Fairness

Cisco Air Time Fairness (ATF) for High Density Experience (HDX) allows network administrators to group devices of a defined category and enables some groups to receive traffic from the WLAN more frequently than other groups. Therefore, some groups are entitled to more *air time* than other groups.

Cisco ATF has the following capabilities:

- Allocates Wi-Fi *air time* for user groups or device categories
- Air time fairness is defined by the network administrator and not by the network
- Provides a simplified mechanism for allocating air time
- Dynamically adapts to changing conditions in a WLAN
- Enables a more efficient fulfillment of service-level agreements
- Augments standards-based Wi-Fi QoS mechanisms

By enabling network administrators to define what *fairness* means within their environments with regard to the amount of *on air* time per client group, the amount of traffic is also controlled.

To control air time on a percentage basis, the air time, which includes both uplink and downlink transmissions of a client/SSID, is continuously measured.

Only air time in the downlink direction, that is AP to client, can be controlled accurately by the AP. Although air time in the uplink direction, that is client to AP, can be measured, it cannot be strictly controlled. Although the AP can constrain air time for packets that it sends to clients, the AP can only measure air time for packets that it *hears* from clients because it cannot strictly limit their air time.

Cisco ATF establishes air time limits (defined as a percentage of total air time) and to apply those limits on a per SSID basis, where the SSID is used as a parameter to define a client group. Other parameters can be used as well to define groups of clients. Furthermore, a single air time limit (defined as a percentage of total air time) can be applied to individual clients.

If the air time limit for an SSID (or client) is exceeded, the packets that are in the downlink direction are dropped. Dropping downlink packets (AP to client) frees up air time whereas dropping uplink packets (client to AP) does not do anything to free up air time because the packet has already been transmitted over the air by the client.

Client Fair Sharing

With Cisco Wireless Release 8.2, Cisco Air Time Fairness can be enforced on clients that are associated with an SSID/WLAN. This ensures that all clients within an SSID/WLAN are treated equally based on their utilization of the radio bandwidth. This feature is useful in scenarios where one or a few clients could use the complete air time allocated for an SSID/WLAN, thereby depriving Wi-Fi experience for other clients associated with the same SSID/WLAN.

- The percentage of air time to be given to each client is recomputed every time a client connects or disconnects.
- Client fair sharing is applicable to only downstream traffic.
- Clients can be categorized into the following usage groups at the policy level: low, medium, and high.
- Client-based ATF metrics accumulation is performed in the transmit complete routine. This allows the air time that is unused by clients in low-usage or medium-usage groups to be accumulated to a common share pool bucket where the high-usage clients can be replenished.

Supported Access Point Platforms

Cisco ATF is supported on the following access points:

- Cisco Aironet 1570 Series Access Points
- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 3700 Series Access Points

Note Cisco ATF is supported only on Local and FlexConnect mode APs.

Cisco ATF Modes

Cisco ATF operates in the following modes:

- Monitor mode in which users can do the following:
  - View the air time
  - Report air time usage for all AP transmissions
  - View reports

    - per SSID/WLAN
    - per AP Group
    - per AP
    - per client
  - Report air time usage at periodic intervals
  - Block ACKs are not reported
  - No enforcement as part of Monitor mode
- Enforce Policy mode in which users can do the following:
  - Enforce air time based on configured policy
  - Enforce air time on
    - a WLAN
    - All APs connected within a controller's network
    - an AP group
    - an AP
    - a client
  - An AP can have multiple WLANs with multiple policies (1:16)
  - Strict Enforcement per WLAN—Air time used by the WLANs on a radio is strictly enforced up to the configured limits in the policies
  - Optimal Enforcement per WLAN—Share unused air time from other SSIDs
  - The sum of all policies should amount to 100 percent; there can be no oversubscription.

Restrictions on Cisco Air Time Fairness

- ATF can be implemented only on data frames that are in the downstream direction.
- When ATF is configured in per-SSID mode, all of the WLANs must be disabled before you can enter any ATF configuration commands. The WLANs can be enabled after all of the ATF commands have been entered.

Cisco Air Time Fairness (ATF) Use Cases

Public Hotspots (Stadium/Airport/Convention Center/Other)

In this instance a public network is sharing a WLAN between two (or more) service providers and the venue. Subscribers to each service provider can be grouped and each group can be allocated a certain percentage of air time.

Education

In this instance, a university is sharing a WLAN between students, faculty, and guests. The guest network can be further partitioned by service provider. Each group can be assigned a certain percentage of air time.

Enterprise/Hospitality/Retail

In this instance, the venue is sharing a WLAN between employees and guests. The guest network can be further partitioned by service provider. The guests could be sub-grouped by tier of service type with each subgroup being assigned a certain percentage of air time, for example a paid group is entitled to more air time than the free group.

Time Shared Managed Hotspot

In this instance, the business entity managing the hotspot, such as a service provider or an enterprise, can allocate and subsequently lease air time to other business entities.

The following are the high-level steps to configure Cisco ATF:

1. Enable Monitor mode to determine network usage (optional)
2. Create Cisco ATF policies
3. Add WLAN ATF policies per network, AP group, or AP. Policies set in AP or AP group override per network polices.
4. Determine if optimization should be enabled.
5. Periodically check Cisco ATF statistics.

Related Documentation

- Air Time Fairness(ATF) Phase1 and Phase 2 Deployment Guide
- Feature Matrix for Cisco Wave 2 Access Points and Wi-Fi 6 (802.11ax) Access Points

This section contains the following subsections:

Configuring Cisco Air Time Fairness (GUI)

Configuring Cisco ATF Monitor Mode (GUI)

Procedure

Step 1 Choose **Wireless** > **ATF** > **Monitor Configuration**.

Step 2 On the **ATF Monitor Mode Configuration** page, choose an AP, AP group, or an entire network. If you choose the entire network, specify the radio type(s).

Step 3 Click **Enable**.

Step 4 Save the configuration.

Configuring Cisco ATF Policy (GUI)

Procedure

Step 1 Choose **Wireless** > **ATF** > **Policy Configuration**.

Step 2 On the **ATF Policy Configuration** page, specify an ID, name, and a weight to the ATF policy, and click **Create**.

Weighted ratio is used instead of percentages so that the total can exceed 100. The minimum weight that you can set is 10.

Step 3 Check the **Client Fair Sharing** check box to apply Client Fair Sharing on the policy.

Step 4 Save the configuration.

Configuring Cisco ATF Enforcement SSID (GUI)

Procedure

Step 1 Choose **Wireless** > **ATF** > **Enforcement SSID Configuration**.

Step 2 On the **ATF Enforcement SSID Configuration** page, apply the ATF policy created to an AP, an AP group, or the entire network with the radio type specified.

Step 3 Choose the enforcement type as either **Optimized** or **Strict**.

Step 4 Click **Enable**.

Step 5 Enforce an ATF policy on a WLAN by selecting the WLAN and the ATF policy and clicking **Add**.

Step 6 Save the configuration.

Monitoring ATF Statistics (GUI)

Procedure

To monitor per WLAN per AP ATF statistics with percentage of used time, choose **Wireless** > **ATF** > **ATF Statistics**. Select the AP name in the drop-down list to view the statistics.

- abs—Number of air time units being used per SSID
- Relative Time—Percentage of time used per SSID
- Total Air time—Total air time used per SSID

Configuring Cisco Air Tme Fairness (CLI)

Procedure

- Configure Cisco ATF at the network level (global) by entering these commands:
  - **config atf 802.11**{**a** | **b**} **mode disable**
  - **config atf 802.11**{**a** | **b**} **mode monitor**
  - **config atf 802.11**{**a** | **b**} **mode enforce-policy**
  - **config atf 802.11**{**a** | **b**} **optimization** {**enable** | **disable**}
- Configure Cisco ATF on a per AP group basis by entering these commands:
  - **config wlan apgroup atf 802.11**{**a** | **b**} **mode disable** *ap-group-name*
  - **config wlan apgroup atf 802.11**{**a** | **b**} **mode monitor** *ap-group-name*
  - **config wlan apgroup atf 802.11**{**a** | **b**} **mode enforce-policy** *ap-group-name*
  - **config wlan apgroup atf 802.11**{**a** | **b**} **optimization** {**enable** | **disable**} *ap-group-name*
- Configure Cisco ATF on a per AP radio basis by entering these commands:
  - **config ap atf 802.11**{**a** | **b**} **mode disable** *ap-name*
  - **config ap atf 802.11**{**a** | **b**} **mode monitor** *ap-name*
  - **config ap atf 802.11**{**a** | **b**} **mode enforce-policy** *ap-name*
  - **config ap atf 802.11**{**a** | **b**} **optimization** {**enable** | **disable**} *ap-name*
- Configure ATF policies by entering these commands:
  - **config atf policy create** *policy-id policy-name policy-weight*
  - **config atf policy modify** {**weight** *policy-weight policy-name*} | {**client-sharing** {**enable** | **disable**} *policy-name*}
  - **config atf policy delete** *policy-name*
- Configure WLAN with a policy ID by entering this command:
  - **config wlan atf** *wlan-id* **policy** *policy-id*
- Configure AP group-level override for Cisco ATF policy on a WLAN by entering these commands:
  - **config wlan apgroup atf 802.11**{**a** | **b**} **policy** *ap-group-name wlan-id policy-name* **override** {**enable** | **disable**}
- Configure AP-level override for Cisco ATF policy on a WLAN by entering these commands:
  - **config ap atf 802.11**{**a** | **b**} **policy** *wlan-id policy-name ap-name* **override** {**enable** | **disable**}
- Monitor Cisco ATF configurations by entering these commands:
  - **show atf config all**
  - **show atf config ap-name** *ap-name*
  - **show atf config apgroup** *ap-group-name*
  - **show atf config 802.11**{**a** | **b**}
  - **show atf config policy**
  - **show atf config wlan**
  - **show atf statistics ap** *ap-name* **802.11**{**a** | **b**} **summary**
  - **show atf statistics ap** *ap-name* **802.11**{**a** | **b**} **wlan** *wlan-id*

- **show atf statistics ap** *ap-name* **802.11**{**a** | **b**} **policy** *policy-name*

CHAPTER 29

Location Services

- Cisco Hyperlocation, on page 531
- FastLocate for Cisco Wave 2 Access Points, on page 535
- Optimizing RFID Tracking on Access Points, on page 536
- Location Settings, on page 538
- Probe Request Forwarding, on page 543
- CCX Radio Management, on page 544
- Mobile Concierge, on page 548
- CMX Cloud Connector, on page 565
- NMSP by AP Groups with Subscription List from CMX, on page 569

Cisco Hyperlocation

The Cisco Hyperlocation radio module provides the following:

- WSM Radio Module functions that are extended to:
  - 802.11ac
  - Wi-Fi Transmit
  - WSM and RRM channel scanning that is extended to 20-MHz, 40-MHz, and 80-MHz channel bandwidth.
- Expanded location functionality:
  - Low latency location optimized channel scanning
  - 32-antenna angle of arrival (AoA)

Note The download BlockAckReq (BAR)/ Block Ack (BA) uses 1/3 of airtime in the worst case scenario when there is only one AP to do the AoA location.

In a typical AoA location usage, there are 4 to 5 participating APs. These APs send BAR/BA in a round robin fashion and only 5 to 6 percent airtime is used. For each 250 ms of dwell time, the primary AP schedules a 4ms-burst of BAR/BA every 9 ms. Therefore, sufficient airtime is available to support voice and video unless there is a case of extreme overload.

The Cisco Hyperlocation Radio Module is supported on Cisco Aironet 3600 and 3700 Series Access Points.

For more information about Cisco Hyperlocation, see the following documents:

- Cisco Hyperlocation Solution
- Cisco CMX 10.2 Configuration Guide to enable Cisco Hyperlocation
- Cisco CMX 10.2 Release Notes

Guidelines and Restrictions for Cisco Hyperlocation

- Hyperlocation configurations are not supported on Cisco APs in Sniffer mode.
- Cisco Hyperlocation in enabled state has an impact on performance where both radios of APs that do not have Cisco Hyperlocation module go off-channel for about 100 milliseconds every 3 seconds.
- When Hyperlocation is enabled, a burst of BARs are sent for location purposes. This takes about 6 percent to 10 percent of airtime.
- If submode wIPS is in enabled state, it is not possible to enable Hyperlocation or FastLocate.

This section contains the following subsections:

Cisco Hyperlocation in a High Availability Environment

The global and per AP-group Cisco Hyperlocation configuration is mirrored from primary to secondary controller. The secondary controller updates only the internal state and does not forward any configuration information to the APs.

For MSE message encryption, the controller generates an encryption key and sends it to the APs and to the MSE, which uses it for encryption and decryption as end clients. The secondary controller does not generate an encryption key and the AP and MSE use the actual key shared by the primary controller.

Cisco Hyperlocation Client Debug Tracing

The Cisco Hyperlocation Debug Client Tracing feature provides the ability to specify a client MAC address for detailed hyperlocation tracing. Enable this feature using the **test dot11 halo-client-trace client-mac** command. To disable this feature, use the **test dot11 halo-client-trace 0000.0000.0000** command.

Configuring Cisco Hyperlocation

Configuring Cisco Hyperlocation for all APs (GUI)

This section provides instructions to configure Cisco Hyperlocation for all APs, a specific AP, and a group of APs that have the Cisco Hyperlocation radio module and are associated with controller.

Procedure

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration**.

Step 2 In the **Hyperlocation Config Parameters** section:

a) Check the **Enable Hyperlocation** check box.

Based on AP and installed module, checking the **Enable Hyperlocation** check box enables different location service (PRL-based or AoA-based).

b) Enter the **Packet Detection RSSI Minimum (dBm)** value.

This is the minimum level at which a data packet can be heard by the WSM modules for use in location calculations. The default value is –100 dBm.

We recommend that this value be increased if you want to have only strong signals used in calculating locations.

c) Enter the **Scan Count Threshold for Idle Client Detection** value.

The Scan Count Threshold represents the number of off-channel scan cycles the AP will wait before sending a Block Acknowledgment Request (BAR) to idle clients. The default value of 10 corresponds to approximately 40s, depending on the number of channels in the off channel scan cycle.

d) Enter the IPv4 address of the NTP server.

This is the IPv4 address of the NTP server that all APs that are involved in this calculation need to synchronize to.

We recommend that you use the same NTP server as is used by the general controller infrastructure. The scans from multiple AP need to be synchronized for the location to be accurately calculated.

Step 3 Save the configuration.

Configuring Cisco Hyperlocation for an AP (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs**.

Step 2 On the **All APs** page that is displayed, click the name of the access point for which you want to configure Cisco Hyperlocation.

Step 3 Click the **Advanced** tab.

This opens the window.

Step 4 In the **Hyperlocation Configuration** section, from the **Enable Hyperlocation** drop-down list, choose **AP Specific** and then check the check box next to the drop-down list to enable Cisco Hyperlocation for the AP.

Step 5 Save the configuration.

Configuring Cisco Hyperlocation for an AP Group (GUI)

Procedure

Step 1 Choose **WLANs** > **Advanced** > **AP Groups**.

Step 2 Click the AP group name.

Step 3 Click the **Location** tab.

Step 4 In the **HyperLocation Config Parameters** section, check the **Enable Hyperlocation** check box to enable Hyperlocation for the AP group.

Step 5 Enter the **Packet Detection RSSI Minimum (dBm)** value.

This is the minimum level at which a data packet can be heard by the WSM modules for use in location calculations. The default value is –100 dDm.

We recommend that this value be increased if you want to have only strong signals used in calculating locations.

Step 6 Enter the **Scan Count Threshold for Idle Client Detection** value.

The Scan Count Threshold represents the number of off-channel scan cycles the APs will wait before sending a Block Acknowledgment Request (BAR) to idle clients. The default value of 10 corresponds to approximately 40s, depending on the number of channels in the off channel scan cycle.

Step 7 Enter the IPv4 address of the NTP server.

This is the IPv4 address of the NTP server that all APs that are involved in this calculation need to synchronize to.

We recommend that you use the same NTP server as is used by the general controller infrastructure. The scans from multiple APs need to be synchronized for the location to be accurately calculated.

Step 8 Save the configuration.

Configuring Cisco Hyperlocation for all APs (CLI)

Procedure

- Configure Cisco Hyperlocation for all APs by entering this command:
  config advanced hyperlocation {**enable** | **disable**}
- Configure the IP address of the NTP server by entering this command:
  config advanced hyperlocation ntp *ipv4-addr*
- Reset threshold value in scan cycles after trigger by entering this command:
  config advanced hyperlocation reset-threshold *value*

- Configure the threshold value below which RSSI is ignored while sending to controller by entering this command:
  config advanced hyperlocation threshold *value*
- Configure the number of scan cycles between PAK RSSI location trigger by entering this command:
  config advanced hyperlocation trigger-threshold *value*
- See a summary of Cisco Hyperlocation global configuration by entering this command:
  show advanced hyperlocation summary

Configuring Cisco Hyperlocation for an AP (CLI)

Procedure

- Configure Cisco Hyperlocation for a specific AP by entering this command:
  config advanced hyperlocation {**enable** | **disable**} *ap-name*

Configuring Cisco Hyperlocation for an AP Group (CLI)

Procedure

- Configure Cisco Hyperlocation for an AP group by entering this command:
  config advanced hyperlocation apgroup *group-name* {**enable** | **disable**}

FastLocate for Cisco Wave 2 Access Points

Current Wi-Fi location technology relies on mobile devices sending received signal strength indication (RSSI) or location information, based on probe request messaging, to the Wave 2 APs. The information is sent on most channels and received by neighbor Wave 2 APs on different channels, which helps in estimating the location.

Device probing frequency varies from 10 seconds to 5 minutes depending on client, OS, driver, battery, current, and client activity. This results in inadequate data points to represent real-world movement.

Using FastLocate, it is possible to get received signal strength indication (RSSI) or location information using data packets received by APs for higher location refresh rates. Using data packets, location-based services (LBS) updates are initiated by the network and are available more frequently. For more information, see the CMX FastLocate Deployment Guide.

For information about which Wave 2 APs support FastLocate, see https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html.

When FastLocate is enabled, the XOR radios of these Wave 2 APs act as the WSSI module and transform into a monitoring role and off-channel scanning mode. The XOR radios scan through all the 2.4-GHz channels and 5-GHz channels in a linear fashion, with each channel scanned for 150 milliseconds. This period is called the dwell time. The XOR radios of these Wave 2 APs are synchronized with the NTP server. All the data packet RSSI records that are collected during one-off channel dwell is packaged in a specific packet format and sent to controller at the end of the dwell time using fastpath. controller in turn forwards this data to Cisco CMX.

Configuring FastLocate on Cisco Wave 2 APs (GUI)

Before you begin

- Ensure that the Cisco Wave 2 APs are part of an AP group and a WLAN is assigned to the AP group.
- Ensure that global Hyperlocation is disabled.

Procedure

Step 1 Set the radio role assignment for the XOR radios of the Wave 2 APs to Auto and Client Serving:

a) Choose **Wireless** > **Access Points** > **Dual-Band Radios**.
b) On the **Dual-Band Radios** page, hover the cursor over the blue drop-down arrow for the Wave 2 AP and click **Configure**.
c) On the **802.11a/b/g/n Cisco APs > Configure** page and in the **Radio Role Assignment** section, choose **Auto** and **Client Serving**.
d) Click **Apply**.

Step 2 Choose **WLANs** > **Advanced** > **AP Groups** and click the name of the AP group that consists of the Wave 2 APs for which you have to configure FastLocate.

Step 3 On the **AP Groups > Edit** page, click the **Location** tab.

Step 4 Check the **Enable Hyperlocation** check box.

Step 5 Enter the **Packet Detection RSSI Minimum** value.

This is the minimum level at which a data packet can be heard by the AP modules for use in location calculations. The default value is –100 dBm.

Step 6 Enter the **Scan Count Threshold for Idle Client Detection** value.

The Scan Count Threshold represents the number of off-channel scan cycles the AP will wait before activating the idle clients once. The default value of 10 corresponds to approximately 40s, depending on the number of channels in the off-channel scan cycle.

Step 7 Enter the IPv4 address of the NTP server.

We recommend that you use the same NTP server as is used by the general controller infrastructure. The scans from multiple AP need to be synchronized for the location to be accurately calculated.

Step 8 Save the configuration.

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)

Procedure

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)

Procedure

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

Location Settings

Configuring Location Settings (CLI)

The controller determines the location of client devices by gathering received signal strength indication (RSSI) measurements from access points all around the client of interest. The controller can obtain location reports from up to 16 access points for clients, RFID tags, and rogue access points.

Improve location accuracy by configuring the path loss measurement (S60) request for normal clients or calibrating clients by entering this command:

config location plm *?*

where *?* is one of the following:

- **client** {**enable** | **disable**} *burst_interval*—Enables or disables the path loss measurement request for normal, noncalibrating clients. The valid range for the *burst_interval* parameter is 1 to 3600 seconds, and the default value is 60 seconds.
- **calibrating** {**enable** | **disable**} {**uniband** | **multiband**}—Enables or disables the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio or on the associated 802.11a/b/g radio.

If a client does not send probes often or sends them only on a few channels, its location cannot be updated or cannot be updated accurately. The **config location plm** command forces clients to send more packets on all channels. When a CCXv4 (or higher) client associates, the controller sends it a path loss measurement request, which instructs the client to transmit on the bands and channels that the access points are on (typically, channels 1, 6, and 11 for 2.4-GHz-only access points) at a configurable interval (such as 60 seconds) indefinitely.

These four additional location CLI commands are available; however, they are set to optimal default values, so we do not recommend that you use or modify them:

- Configure the RSSI timeout value for various devices by entering this command:

  config location expiry *?*

  where*?* is one of the following:

  - **client** *timeout*—Configures the RSSI timeout value for clients. The valid range for the *timeout* parameter is 5 to 3600 seconds, and the default value is 5 seconds.
  - **calibrating-client** *timeout*—Configures the RSSI timeout value for calibrating clients. The valid range for the *timeout* parameter is 0 to 3600 seconds, and the default value is 5 seconds.
  - **tags** *timeout*—Configures the RSSI timeout value for RFID tags. The valid range for the *timeout* parameter is 5 to 300 seconds, and the default value is 5 seconds.
  - **rogue-aps** *timeout*—Configures the RSSI timeout value for rogue access points. The valid range for the *timeout* parameter is 5 to 3600 seconds, and the default value is 5 seconds.

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

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

- Configure the RSSI half life for various devices by entering this command:

  config location rssi-half-life *?*

  where *?* is one of the following:

  - **client** *half_life*—Configures the RSSI half life for clients. The valid range for the *half_life* parameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.
  - **calibrating-client** *half_life*—Configures the RSSI half life for calibrating clients. The valid range for the *half_life* parameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.

- **tags** *half_life*—Configures the RSSI half life for RFID tags. The valid range for the *half_life* parameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.
- **rogue-aps** *half_life*—Configures the RSSI half life for rogue access points. The valid range for the *half_life* parameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.

  Some client devices transmit at reduced power immediately after changing channels, and RF is variable, so RSSI values might vary considerably from packet to packet. The **config location rssi-half-life** command increases accuracy by averaging nonuniformly arriving data using a configurable forget period (or half life).

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

- Configure the NMSP notification threshold for RSSI measurements by entering this command:

  config location notify-threshold *?*

  where *?* is one of the following:

  - **client** *threshold*—Configures the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the *threshold* parameter is 0 to 10 dB, and the default value is 0 dB.
  - **tags** *threshold*—Configures the NMSP notification threshold (in dB) for RFID tags. The valid range for the *threshold* parameter is 0 to 10 dB, and the default value is 0 dB.
  - **rogue-aps** *threshold*—Configures the NMSP notification threshold (in dB) for rogue access points. The valid range for the *threshold* parameter is 0 to 10 dB, and the default value is 0 dB.

Note We recommend that you do not use or modify the **config location notify-threshold** command.

- Configure the algorithm used to average RSSI and signal-to-noise ratio (SNR) values by entering this command:

  config location algorithm *?*

  where *?* is one of the following:

  - **simple**—Specifies a faster algorithm that requires low CPU overhead but provides less accuracy.
  - **rssi-average**—Specifies a more accurate algorithm but requires more CPU overhead.

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

Viewing Location Settings (CLI)

To view location information, use these CLI commands:

- View the current location configuration values by entering this command:

  show location summary

- See the RSSI table for a particular client by entering this command:

  show location detail *client_mac_addr*

- See the location-based RFID statistics by entering this command:

  show location statistics rfid

- Clear the location-based RFID statistics by entering this command:

  clear location statistics rfid

- Clear a specific RFID tag or all of the RFID tags in the entire database by entering this command:

  clear location rfid {*mac_address* | **all**}

- See whether location presence (S69) is supported on a client by entering this command:

  show client detail *client_mac*

  When location presence is supported by a client and enabled on a location appliance, the location appliance can provide the client with its location upon request. Location presence is enabled automatically on CCXv5 clients.

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

NMSP manages communication between the Cisco Connected Mobile Experience (Cisco CMX) and the controller for incoming and outgoing traffic. If your application requires more frequent location updates, you can modify the NMSP notification interval (to a value between 1 and 180 seconds) for clients, active RFID tags, and rogue access points and clients.

NMSP uses 128_CBC_SHA cipher to communicate with the MSE or the CMX device.

Note The TCP port (16113) that the controller and Cisco CMX communicate over must be open (not blocked) on any firewall that exists between the controller and the Cisco CMX for NMSP to function.

Procedure

Step 1 Set the NMSP notification interval value for clients, RFID tags, and rogue clients and access points by entering these commands, where *interval* is a value between 1 and 180 seconds:

- **config nmsp notification interval rssi clients** *interval*

- **config nmsp notification interval rssi rfid** *interval*
- **config nmsp notification interval rssi rogues** *interval*

Step 2 See the NMSP notification intervals by entering this command:

show nmsp notification interval

Information similar to the following appears:

```
NMSP Notification Interval Summary

                                  RSSI Interval:
 Client.......................................... 2 sec
 RFID............................................ 2 sec
 Rogue AP........................................ 2 sec
 Rogue Client.................................... 2 sec

Spectrum Interval:
 Interferer device............................... 2 sec
```

Viewing NMSP Settings (CLI)

To view NMSP information, use these CLI commands:

- See the status of active NMSP connections by entering this command:

  show nmsp status

- See the NMSP capabilities by entering this command:

  show nmsp capability

- See the NMSP counters by entering this command:

  show nmsp statistics {**summary** | **connection**}

  where

  - **summary** shows the common NMSP counters.
  - **connection** shows the connection-specific NMSP counters.

- See the mobility services that are active on the controller by entering this command:

  show nmsp subscription {**summary** | **detail** | **detail** *ip_addr*}

  where

  - **summary** shows all of the mobility services to which the controller is subscribed.
  - **detail** shows details for all of the mobility services to which the controller is subscribed.
  - **detail** *ip_addr* shows details only for the mobility services subscribed to by a specific IP address.

- Clear all NMSP statistics by entering this command:

clear nmsp statistics

Debugging NMSP Issues

Use these commands if you experience any problems with NMSP:

- Configure NMSP debug options by entering this command:

  debug nmsp *?*

  where *?* is one of the following:

  - **all** {**enable** | **disable**}—Enables or disables debugging for all NMSP messages.
  - **connection** {**enable** | **disable**}—Enables or disables debugging for NMSP connection events.
  - **detail** {**enable** | **disable**}—Enables or disables debugging for NMSP detailed events.
  - **error** {**enable** | **disable**}—Enables or disables debugging for NMSP error messages.
  - **event** {**enable** | **disable**}—Enables or disables debugging for NMSP events.
  - **message** {**tx** | **rx**} {**enable** | **disable**}—Enables or disables debugging for NMSP transmit or receive messages.
  - **packet** {**enable** | **disable**}—Enables or disables debugging for NMSP packet events.

- Enable or disable debugging for NMSP interface events by entering this command:

  debug dot11 nmsp {**enable** | **disable**}

- Enable or disable debugging for IAPP NMSP events by entering this command:

  debug iapp nmsp {**enable** | **disable**}

- Enable or disable debugging for RFID NMSP messages by entering this command:

  debug rfid nmsp {**enable** | **disable**}

- Enable or disable debugging for access point monitor NMSP events by entering this command:

  debug service ap-monitor nmsp {**enable** | **disable**}

- Enable or disable debugging for wIPS NMSP events by entering this command:

  debug wips nmsp {**enable** | **disable**}

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)

Procedure

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 Configure the backoff parameters for probe queue in a Cisco AP by entering this command:

config advanced probe backoff {**enable** | **disable**}

- **enable**(default)—Choose this parameter to use increased backoff parameters for probe response.
- **disable**—Choose this parameter to use default backoff parameter value for probe response.

Step 4 Enter the **save config** command to save your changes.

Step 5 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
```

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 controller 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)

Procedure

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 controller 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 controller 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)

Procedure

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 controller 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 controller 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

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) (GUI)

Procedure

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 Check 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) Check 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** field, 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) Check 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** field, 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** field, 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** field, 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*

Online Sign Up

Online Sign Up (OSU) is a process in which a mobile device is registered with a service provider, enabling users to select a plan to obtain network access. After the sign-up, the device receives the users' credentials to connect to the network. A network architecture for OSU is given below, which consists of a service provider network and a hotspot:

The service provider network consists of an OSU server, an Authentication, Authorization and Accounting (AAA) server, and (access to) a Certification Authority (CA). These devices may be co-located or separate.

The hotspot has its own OSU, which is optional, and a AAA server. The hotspot is configured to allow only HTTPS traffic to OSU servers. An OSU server registers new customers and provides security credentials to their mobile devices. It can also be used to initially provision devices of existing customers. The AAA server of the service provider is used to authenticate subscribers based on the information received from the OSU server.

The OSU process ensures that:

- A user is communicating with the intended service provider network and OSU server.
- The communication is protected between the mobile device and OSU server.
- Poor security practices of one service provider affecting other service providers are reduced.

The controller should support the following requirements:

- Hotspot 2.0 Indication Element
- OSU Service Provider List
- Icon Request and Response Access Network Query Protocol (ANQP) Element
- OSU Server-Only Authenticated L2 Encryption Network (OSEN)
- Wireless Network Management (WNM) Notification Subscription Remediation Request
- WNM Notification Deauth Imminent Request

- Basic Service Set (BSS) Transition Management Request Frame - Session URL
- QoS Map Set
- Extended Capability Bit Support:
  - WNM Notification
  - QoS Map Set

Hotspot 2.0 Indication Element

This element (using vendor-specific information) enables the controllers and mobile devices to indicate that they are HotSpot (HS) 2.0 capable. All the beacon and probe response frames from HS 2.0 controllers contain this HS 2.0 indication element. For mobile devices, the association and re-association request frames contain the HS 2.0 indication element.

OSU Service Provider List

This element provides information for the entities offering OSU service. The following information is provided for each OSU provider:

- A friendly name (in one or more human languages)-Name of the OSU provider in human language, which matches the name drawn from the OSU server certificate exactly.
- The Network Access Identifier (NAI) used to authenticate to the OSU (if configured for OSEN).
- The icons and Uniform Resource Identifier (URI) of the OSU server.

Note The controller supports a maximum of 16 service providers per OSU-SP list.

The Icon Request or Response ANQP Element

This element provides a filename for the (icon) download request from the mobile device, which is one of the filenames included in the OSU providers list element. The maximum file size for the icon is 65535 octets; the file type should be a valid image type, for example, PNG, JPEG, and so on. The file type restriction is not applicable for controllers and supports a maximum of 16 icons.

OSEN

The OSEN element is used to advertise and select an OSEN-capable network.

WNM Notification Subscription Remediation Request

The WNM notification request is sent from a controller to a mobile device to indicate that subscription remediation is required when the AAA server indicates to controller of this requirement through the RADIUS Access-Accept message. After the authentication is complete, the controller sends WNM notification to the mobile device, using the URL of the Subscription Remediation server as the server URL.

WNM Notification Deauth Imminent Request

A home SP uses the Deauthentication Imminent Notice to inform the mobile device when it is no longer authorized to use the service due to a temporary condition in the network that requires deauthentication, for example, congestion in the Wi-Fi AN or congestion on a mobile core network element. The notice also provides information on the time that must elapse before the AAA server permits the mobile device to reauthenticate again on the same Basic Service Set (BSS) or Extended Service Set (ESS). Following this, the mobile device should not try to reauthenticate to the same BSS or ESS until the expiry of the reauthentication delay.

BSS Transition Management Request Frame - Session URL

The controller uses the BSS Transition Management Request frame to inform the mobile device of the impending session expiry. It also provides an URL to the user detailing on how to extend the session. The controller gets the information about session warning time and URL from the AAA server through the Access-Accept message.

Extended Capability Bit Support

This element has two sections, WNM Notification and QoS Map Set, which are explained in the previous sections.

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)

Procedure

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)

Procedure

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 In the **Domain ID** field, enter the domain identifier.

Step 5 In the **OSU SSID** field, enter the OSU SSID.

Step 6 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 7 In the **Online Sign Up List** area, perform the following tasks:

a) From the **OSU Index** drop-down list, choose the OSU index you want to use.

b) From the **Lang Code** drop-down list, choose the language code you want to use, and select whether its in ASCII or HEX format from the next drop down list.
c) In the **SP Name** field, enter the service provider name.
d) In the **Description** field, enter the description.
e) Click **Add** to add the parameters to the list.

Step 8 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 9 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 10 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 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.

Procedure

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 20: Venue Group Mapping

Venue Group Name	Value	Venue Type for Group
UNSPECIFIED	0	
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

Venue Group Name	Value	Venue Type for Group
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
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

Venue Group Name	Value	Venue Type for Group
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
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 controller 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.

Procedure

Step 1 Save the icon file on an TFTP, SFTP, or an FTP server.

Step 2 Download the icon file to the controller by entering these commands:

a) **transfer download datatype icon**

b) **transfer download start**

Configuring ICONs

Note The character '?' is not supported in the command values.

- To download an icon from the TFTP server or FTP server into the controller, enter this command:

  configure icon parameters

- To configure icon parameters, enter this command:

  config icons file-info *filename file-type lang-code width height*

- To delete an icon from flash, enter this command:

  config icons delete {*filename* | **all**}

- To display icon parameters, enter this command:

  show icons summary

This section contains the following subsections:

Downloading an ICON File (GUI)

Procedure

Step 1 Copy the **ICON** file to the default directory on your server.

Step 2 Choose **Commands** > **Download File**.

The **Download File to Controller** window is displayed.

Step 3 From the **File Type** drop-down list, choose ICON.

Step 4 From the **Transfer Mode** drop-down list, choose from one of the following options:

- **TFTP**
- **FTP**
- **SFTP**

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 fields should work correctly without any adjustment. However, you can change these values.

Step 6 Enter the maximum number of times the TFTP server can attempt to download the certificate in the Maximum Retries field, and the amount of time (in seconds) that the TFTP server can attempt to download the certificate in the **Timeout** field.

Step 7 In the **File Path** field, enter the directory path of the icon file.

Step 8 In the **File Name** field, enter the name of the icon 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 in to the FTP server.
b) In the **Server Login Password** field, enter the password to log in to the FTP server.
c) In the **Server Port Number** field, enter the port number in the FTP server through which the download occurs. The default value is 21.

Step 10 Click **Download** to download the login ICON file to the controller.

A message is displayed indicating the status of the download.

Step 11 Click **Apply**.

Configuring an ICON (GUI)

Procedure

Step 1 Choose **Controller** > **Icons**.

The **Icon Configuration** window is displayed.

Step 2 In the **Filename** field, enter the filename for the icon.

Step 3 In the **File Type** field, enter the file type of the icon.

Step 4 In the **Lang Code** field, enter the language code.

Step 5 In the **Width** field, enter the width of the icon.

Step 6 In the **Height** field, enter the height of the icon.

Step 7 Click **Add**.

Step 8 Click **Apply**.

Configuring OSEN Support (CLI)

Note The character '?' is not supported in the command values.

- To enable or disable OSEN on a given WLAN, enter this command:

  config wlan security wpa osen {**enable** | **disable**} *wlan-id*

- To display OSEN details on a given WLAN, enter this command:

  show wlan *wlan-id*

This section contains the following subsection:

Configuring OSEN Details (GUI)

Procedure

Step 1	Choose **WLAN** to open the **WLANs** window.
Step 2	Click the WLAN ID to open the Edit page pertaining to the selected WLAN.
Step 3	Click the **Security** tab and then the **Layer 2** tab.
Step 4	From the **Layer 2 Security** drop-down list, choose **WPA+WPA2**.
Step 5	Under **WPA+WPA2 Parameters**, check the **OSEN Policy** check box to enable OSEN.
Step 6	Check the **OSEN Encryption** check box to enable OSEN encryption, and check the **TKIP** check box to enable TKIP.
Step 7	Click **Apply**.

Configuring OSU (CLI)

Note The character '?' is not supported in the command values.

- To configure an (OSU) Service Set Identifier (SSID) name, enter this command:

  config wlan hotspot hs2 osu legacy-ssid {**wlan-id** | **ssid-name**}

- To create an OSU service provider name, enter this command:

  config wlan hotspot hs2 osu sp create *wlan-id osu-index lang-code ascii/hex friendly-name*[*description*]

  The following options are available:

  - *wlan-id*—The WLAN ID on which you want to configure the operator-name.
  - *osu-index*—The osu index of the operator. The range is 1 to 32.
  - *lang-code*—The language used.
  - *ascii/hex*—.
  - *friendly-name*—The name of the 802.11an operator.
  - *description*—The language used.

- To delete an OSU service provider, enter this command:

  config wlan hotspot hs2 osu sp delete *wlan-id osu-index lang-code*

- To configure a domain ID, enter this command:

config wlan hotspot hs2 domain-id {**wland** | **domain-id**}

- To create an OSU URL, enter this command:

  config wlan hotspot hs2 osu sp uri add *wlan-id osu-index uri*

- To delete an OSU URL, enter this command:

  config wlan hotspot hs2 osu sp uri delete *wlan-id osu-index*

- To configure an OSU method list, enter this command:

  config wlan hotspot hs2 osu sp method add *wlan-id osu-index method-pri* [*method-sec*]

- To delete an OSU method list, enter this command:

  config wlan hotspot hs2 osu sp method delete *wlan-id osu-index method*

- To configure an OSU icon file on a given WLAN, enter this command:

  config wlan hotspot hs2 osu sp icon-file add *wlan-id osu-index icon-filename*

Note Yous should first configure icon parameters using the **config icon** *icon-filename* command.

- To delete an OSU icon file from a given WLAN, enter this command:

  config wlan hotspot hs2 osu sp icon-file delete *wlan-id osu-index icon-filename*

- To configure an OSU NAI, enter this command:

  config wlan hotspot hs2 osu sp nai add *wlan-id osu-index nai*

- To delete an OSU NAI, enter this command:

  config wlan hotspot hs2 osu sp nai delete *wlan-id osu-index*

- To display the OSU details configured on a given WLAN, enter this command:

  show wlan *wlan-id*

Configuring OSU Details (GUI)

Procedure

Step 1 Choose **WLAN**.

It opens the WLANs window.

Step 2 Hover your mouse over the blue drop-down arrow corresponding to the desired WLAN on which you want to configure the OSU parameters and choose **802.11u**.

The **802.11u Parameters** window appears.

Step 3 In the **WLAN > 802.11u Parameters** window, enable 802.11u.

Step 4 In the Service Provider Name field, enter the name of the service provider.

The **OSU Index** field displays the OSU index that you are editing.

The **Language Code** field displays the language code associated with the OSU Index.

Step 5 In the **Description** field, enter the description for the OSU.

Step 6 In the **URI** field, enter the URI details.

Step 7 In the **NAI** field, enter the NAI details.

Step 8 In the **Icon Filename** field, enter the filename for the icon associated with the service provider.

Step 9 From the **Method** drop-down list, choose the association method.

Step 10 Click **Apply**.

Configuring WAN Metrics

Note The character '?' is not supported in the command values.

- To configure downlink WAN metrics, enter this command:

  config wlan hotspot hs2 wan-metrics downlink *wlan-id dlink-speed dlink-load*

- To configure uplink WAN metrics, enter this command:

  config wlan hotspot hs2 wan-metrics uplink *wlan-id ulink-speed ulink-load*

- To configure the link status of WAN metrics, enter this command:

  config wlan hotspot hs2 wan-metrics link-status *wlan-id link-status*

- To configure the load measurement duration WAN metrics, enter this command:

  config wlan hotspot hs2 wan-metrics lmd *wlan-id ilmd-val*

CMX Cloud Connector

Cisco CMX Cloud Connector is a Software-as-a-Service (SaaS) product aimed to provide in-venue analytics which seamlessly integrates with the Cisco wireless infrastructure. This product provides secured guest-access solutions to visitors through custom portal. To list some of the features of Cisco CMX Cloud, it analyzes guest activity to provide better engagement, and track assets.

The Cisco CMX Cloud Connector comprises the following packages:

- Cisco CMX Connect
- Cisco CMX Connect with Cisco CMX Presence Analytics

Cisco CMX Connect provides a customizable, seamless, location-aware guest-captive portal that on-boards customers with free Wi-Fi internet access.

Cisco CMX Presence Analytics is a comprehensive analytics and engagement platform that detects the presence of visitors through their mobile devices, using Cisco access points. It eliminates the need for maps, thus enabling faster deployment, easy-to-use and quicker insights.

Cisco CMX Presence Analytics provides customer insights to customer-facing enterprises like retail, hospitality, education, sports, and entertainment, healthcare, airport sectors, and so on. This caters to the needs of businesses with smaller sites and wireless deployments that are not designed for location accuracy.

The incoming connections from Mobility Service Engine (MSE) or CMX to controller are restricted to four TCP/TLS connections. One outgoing HTTPS connection is used to connect controller to CMX cloud, with the controller acting as HTTPs client. The controller uses the preinstalled GeoTrust CA certificate to authenticate CMX Cloud server.

In the controller, when an HTTP proxy server is configured, it can send the NMSP data over this proxy server to the CMX Cloud as the fifth data consumer.

When multiple MSE or CMX devices are used, we recommend you to distribute the subscriptions for services like client measurements, Intrusion Detection System (IDS), RFID, and so on, across different NMSP connections.

As an example, four NMSP connections are distributed among the following services:

- WIPS Server
- Client and Rogues
- RFID
- Halo Traffic Control

The NMSP protocol is used to export the following data from controller to CMX server:

- Client Information
- Client RSSI measurements
- Client traffic stats
- RFID Tag information and measurements
- AP Radio information
- Rogue AP
- Client information
- RSSI measurements

This section contains the following subsections:

Prerequisites for CMX Cloud Connector

- You must have a CMX account at http://www.cmxcisco.com.
- Configure the DNS name in the controller.

  For more information, see https://support.cmxcisco.com/hc/en-us.
- Configure the IP address of the DNS server on the controller to allow it to resolve the configured cloud URL.

Restrictions for CMX Cloud Connector

- Incoming TCP/TLS connections from MSE are limited to four to reduce duplication of NMSP data.
- One CMX cloud URL can be configured in a controller.
- wIPS service is not supported on HTTPS connection.

Configuring CMX Cloud Connector (GUI)

Configure the CMX cloud server in a controller.

Note To change either the ID token or the URL, you need to disable the CMX service, update the fields, and enable the service.

Procedure

Step 1 Choose **Management** > **Cloud Services** > **CMX**.
Step 2 Set the Service Status as **Disabled**.
Step 3 Click **Apply**.
Step 4 Choose **Cloud Services** > **Server**.
Step 5 Enter the server URL in the **URL** box.
Step 6 Enter the **ID-Token** in the Id-token box.
Step 7 Click **Apply**.
Step 8 Choose **Cloud Services** > **CMX**.
Step 9 Set the Service Status as **Enabled**.
Step 10 Click **Apply**

Configuring CMX Cloud Connector (CLI)

Procedure

Step 1 Configure the CMX Cloud Services by entering this command:

config cloud-services cmx {**enabled | disabled**}

Note
To apply any changes that are made to the cloud URL or dependant configurations, disable and re-enable the CMX cloud-service. The following are the dependent configurations:

- Cloud URL

- Cloud Id-token
- DNS server IP
- HTTP proxy

Step 2 Configure the Cloud Server URL by entering this command:
config cloud-services server url *url*

Step 3 Configure the Cloud Server Id-Token by entering this command:
config cloud-services server id-token *id-token*

Step 4 View CMX Cloud Services summary by entering this command:
show cloud-services cmx summary

Step 5 View the CMX cloud services statistics by entering this command:
show cloud-services cmx statistics

Step 6 View the status of active NMSP connections by entering this command:
show nmsp status

Step 7 View the mobility services summary by entering this command:
show nmsp subscription summary

Installing CMX-Serv CA Certificate on a Controller (CLI)

Procedure

Step 1 Download the CMX server CA certificate by entering this command:
transfer download datatype cmx-serv-ca-cert

Step 2 Specify the transfer mode that is used to download the config file by entering this command:
transfer download mode {**ftp** | **tftp**| **http**| **stftp**}

Step 3 Specify the name of the certificate file to be downloaded by entering this command:
transfer download filename*cert-file-name*

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:
transfer download serverip *server-ip-address*

Step 5 (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 6 Begin the certificate transfer by entering this command:

transfer download start

Enter **Y** to confirm upload.

Step 7 Reboot the device by entering this command:

reset system

NMSP by AP Groups with Subscription List from CMX

Use this feature to send only the required Network Mobility Services Protocol (NMSP) data to CMX (applicable to both on-premises and cloud-based CMX). CMX can subscribe to NMSP data of specific APs or AP groups based on the active services in controller.

This feature helps in load balancing where APs are distributed across different CMX servers to optimize the data flow load.

The CMX server creates a CMX AP group giving it a unique name and groups the APs under it.

Note The CMX AP Group is the list of Cisco APs managed by the CMX for location services. This AP group is not the same as the controller AP group.

Guidelines and Restrictions for NMSP by AP Groups with Subscription List from CMX

- This feature is supported with Cisco CMX Release 10.5 and later releases.
- The following services are supported:
  - Client
  - Probing client filtering
  - Hyperlocation

    Cisco APs, which are a part of two different maps that are managed by two different CMX servers, sync with the latest CMX server only.
- Only the services that are in enabled state in the controller are available for NMSP subscription.

Monitoring NMSP by AP Groups with Subscription List from CMX (GUI)

Procedure

Step 1 Choose **Monitor** > **Cloud Services** > **CMX** to open the **CMX Monitor** page.

This page displays the connected CMX Servers, the subscribed services, and the group subscriptions.

Step 2 Click **See Groups** under **Group Subscriptions** section to view the AP group's subscribed services and the AP Monitor Service configuration details.

Step 3 Click **List of APs** under **AP Subscriptions** section of the **Group Subscriptions** page to view the list of APs subscribed by a CMX server under this AP group.

Monitoring NMSP by AP Groups with Subscription List from CMX (CLI)

Procedure

- View the mobility services summary by entering this command:

  show nmsp subscription summary

  Information similar to the following is displayed:

```
Mobility Services Subscribed:
Index Server IP Services
----- --------- --------
1 209.165.200.225 RSSI, Info, Statistics, AP Monitor, AP Info
2 209.165.200.225 RSSI, Statistics, AP Info
```

- View the mobility services that are subscribed in detail by entering this command:

  show nmsp subscription detail { **detail | group | summary** }

  Information similar to the following is displayed:

```
Mobility Services Subscribed by 209.165.200.225
Services Sub-services
-------- ------------
RSSI Tags,
Statistics Tags,
AP Info Subscription
```

- View mobility services group subscription summary of all CMX connections by entering this command:

  show nmsp subscription group summary

  Information similar to the following is displayed:

```
NMSP connection ip..................... 209.165.200.225
Groups subscribed by this CMX server:
=====================================
No groups subscribed by this CMX server
NMSP connection ip..................... 209.165.200.225
Groups subscribed by this CMX server:
```

```
=======================================
CMX_209.165.200.225
```

- View the services that are subscribed for an AP group by a CMX connection by entering this command:

  show nmsp subscription group detail services *cmx_ipadd grp-name*

  Information similar to the following is displayed:

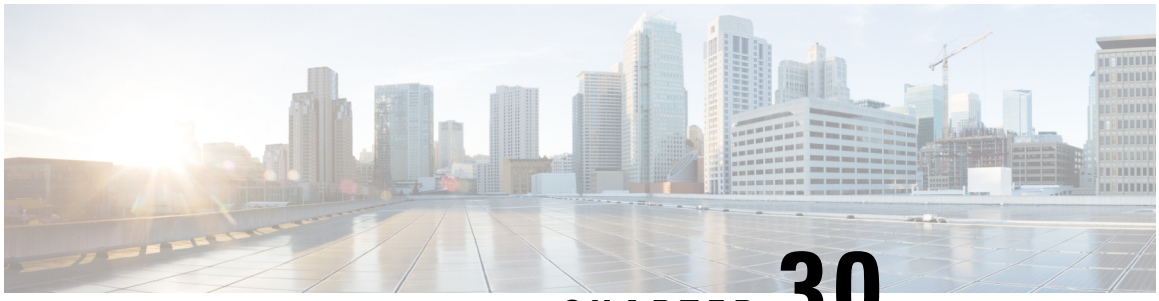
```
CMX connection ip.......................... 209.165.200.225
CMX group name............................. CMX_209.165.200.225
Services Sub-services
-------- ------------
RSSI Mobile Station,
Info Mobile Station,
Statistics Mobile Station,
AP Monitor Subscription

AP Monitor Service Configuration:
Halo UDP Server IP Address..................... 209.165.200.225
Halo UDP Server Port........................... 5003
```

- View the AP MAC list that is subscribed for an AP group by a CMX connection by entering this command:

  show nmsp subscription group detail ap-list *cmx_ipadd grp-name*

  Information similar to the following is displayed:

```
CMX connection ip.......................... 209.165.200.225
CMX group name............................. CMX_209.165.200.225
AP-LIST
====================
00:ae:e5:db:af:56
```



CHAPTER 30

Wireless Intrusion Detection System

- Protected Management Frames (Management Frame Protection), on page 573
- Rogue Management, on page 576
- Rogue Access Point Classification, on page 582
- Intrusion Detection System Signatures, on page 597
- Cisco Intrusion Detection System, on page 605
- Wireless Intrusion Prevention System, on page 609

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 send 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 send 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

The 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

Additional Reference: Configure 802.11w Management Frame Protection on Controller

This section contains the following subsections:

Configuring Infrastructure MFP (GUI)

Procedure

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).
e) Click **Apply** to commit your changes.

Step 5 Save the configuration.

Related Topics

Configuring Protected Management Frames (802.11w) (GUI), on page 919

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.

Related Topics

Configuring Protected Management Frames (802.11w) 802.11w (CLI), on page 919

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.

Rogue Management

Rogue APs are 802.11 devices that can be detected by your network's APs but are not members of the same RF group. Rogue clients are clients that are associated with such APs.

Rogue detection is the method by which APs monitor the channels for rogue APs and clients. Such monitoring is performed by a monitor mode radio and also can be performed by a serving mode radio based upon the RRM monitoring configuration. For more information, see Radio Resource Management, on page 409.

Rogue containment is performed by an AP engaging in denial of service (DoS) attack on what it considers to be a rogue device.

Caution Performing rogue containment might be illegal if the target of the attack is a device that you do not own. Enable rogue containment only if none of your APs can transmit radio signals outside of your property.

Rogue Location Discovery Protocol (RLDP) is a method by which a monitor mode or serving AP acts as a client of a rogue AP and attempts to associate with it in an attempt to determine whether that AP is on your organization's network. For this to work, the rogue SSID has to be open and providing DHCP addresses.

Note RLDP is supported only in Cisco IOS-based Wave 1 APs.

A rogue detector mode AP aims to correlate rogue information heard over the air with ARP information obtained from the wired network. Rogue detector mode in APs are supported only in Cisco IOS-based Wave 1 APs.

For a detailed overview on rogue management, see Rogue Management in an Unified Wireless Network.

Configuring Rogue Detection (GUI)

Procedure

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 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 4 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 5 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 6 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 7 In the **Rogue Detection Report Interval** text box, enter the time interval, in seconds, at which APs send the rogue detection report to the controller. 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 8 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 9 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 10 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**.

- **Auto Containment only for Monitor mode APs**—Configure the monitor mode access points for auto-containment.
- **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 11 Click **Apply**.

Step 12 Click **Save Configuration**.

Configuring Rogue Detection (CLI)

Procedure

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 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 3 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 4 Enable or disable ad hoc rogue detection and reporting by entering this command:

config rogue adhoc {**enable** | **disable**}

Step 5 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 6 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 7 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 8 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 9 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.

Step 10 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 11 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 12 Save your changes by entering this command:

save config

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 controller flash memory; however, the database is not updated. When HA switchover occurs, the rogue list from the previously standby controller 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 21: 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.
- The status change of a rogue device to contain or alert does not work when you move it between different class types until you move the class type of the rogue to unclassified.
- 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.
- When a rogue BSSID is submitted for a containment on Cisco Catalyst 9800 Series Wireless Controller, if the controller has enough resources, it will contain. The APs that detect the particular contained rogue AP starts broadcasting the DEAUTH packets.

  Wireless client connected to the contained rogue BSSID will disconnect once DEAUTH packets are received. However, when the client assumes being in a connected state, repeatedly tries to reconnect and the wireless client's user browsing experience would be badly affected.

  Also, in a high RF environment like that of a stadium, though DEAUTH packets are broadcasted, client does not receive all of them because of RF disturbance. In this scenario, the client may not be fully disconnected but will be affected badly.

- The rouge AP manual classification limit has been enhanced from 625 to 10,000 configurations at a time. The rouge client manual classification limit has been enhanced from 625 to 10,000 configurations at a time.

Configuring Rogue Classification Rules (GUI)

Procedure

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 controller and a trap receiver such as Cisco Prime Infrastructure.
- **Global**—Notifies only a trap receiver such as Cisco Prime Infrastructure.
- **Local**—Notifies only controller.
- **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**.

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.

Procedure

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)

Procedure

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**} *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**} *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**} *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**} *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.

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.

Caution Performing rogue containment might be illegal if the target of the attack is a device that you do not own. Enable rogue containment only if none of your APs can transmit radio signals outside of your property.

- 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

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”
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.

Uploading or Downloading IDS Signatures

Procedure

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.

Configuring IDS Signatures (GUI)

Procedure

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)

Procedure

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)

Procedure

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.

Related Topics

Wireless LAN Controller IDS Signature Parameters

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*

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)

Procedure

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.

Controller 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)

Procedure

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)

Procedure

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)

Procedure

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.

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 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 22: Trap Controls and Descriptions

Type	Trap Control	Description
General	Config Save	Notification that is sent when the controller configuration is modified.
AP	Auth Failure	Trap sent when an AP authorization fails
	AP Interface Up/Down	Trap sent when an AP interface (A or B) comes up
	Mode Change	Trap sent when an AP mode is changed
	AP Register	Trap sent when an AP registers with a switch
	Neighbor AP Signal	Trap sent when an AP detects a neighbor AP signal

Type	Trap Control	Description
Client	802.11 Association	Associate notification that is sent when a client sends an association frame
	Enhanced 802.11 Association	Associate notification that is sent when a client sends an enhanced 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
	Enhanced 802.11 Deauthentication	Deauthenticate notification that is sent when a client sends an enhanced 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
	Enhanced Authentication	Notification that is sent when a client has successfully gone through enhanced authentication
	MaxClients Limit Reached Threshold	Notification that is sent when the maximum number of clients, defined in the **Threshold** field, is 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.

Type	Trap Control	Description
	802.11 Assoc 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
	WebAuth User Login	Trap sent for web authentiction user login
	WebAuth User Logout	Trap sent for web authentiction user logout
	Neighbor Client Detection	Trap sent for neighbor client detection
AAA	User Authentication	This trap informs that a client RADIUS authentication failure has occurred
	RADIUS Servers Not Responding	This trap is to indicate that RADIUS servers are not responding to authentication requests sent by the RADIUS client
802.11 Security Traps	WEP/WPA Decrypt Error	Notification sent when the controller detects a WEP decrypting error
	IDS Signature Attack	Trap sent for IDS signature attacks
	MFP	Trap sent for management frame protection (protected management frames)
Rogues	Rogue AP	Whenever a rogue AP is detected, this trap is sent with its MAC address; when a rogue AP that was detected earlier no longer exists, this trap is sent.
Management	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.
	Multiple Users	Multiple users have logged in using the same ID
	Strong Password	Trap sent for strong password check

Type	Trap Control	Description
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

Type	Trap Control	Description
Mesh	Child Excluded Parent	Notification that is sent when a defined number of failed association to the controller occurs through a parent mesh node
	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
	Authfailure Mesh	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
	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
	Excessive Association	Notification sent when cumulative association counter at parent mesh node exceeds the value configured
	Default Bridge Group Name	Notification sent when the MAP mesh node joins its parent using the default bridge group name

For more information about trap logs, see *Cisco Wireless Controller Trap Logs* at https://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-system-message-guides-list.html.

wIPS Support for 40 and 80 MHz

Release 8.2 introduces wIPS support for 40 and 80 MHz range. This feature detects alarms in the 40 and 80 MHz range (if RRM channel scanning is selected) and provides information to the Cisco Prime Infrastructure. The channel-width information is derived from the packet data rate and sent to the wIPS module that stores

the channel width per alarm. Using the **show capwap am alarm** *alarm-id* command, you can view the channel width in which the attack has occured.

The wIPS alarm report contains the *channel-width* of the attack and device capability (11a/b/g/n/ac). No wIPS specific configuration is required to enable this feature. The only prerequisite is that RRM scanning should be enabled for this feature to work properly.

Restrictions for wIPS

- wIPS ELM is not supported on the following APs:
  - 702i
  - 702W
- Request to Send (RTS) and Clear to Send (CTS) frames are not forwarded to driver if RTS and CTS are for the BSSID of the AP.
- 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)

Procedure

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)

Procedure

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

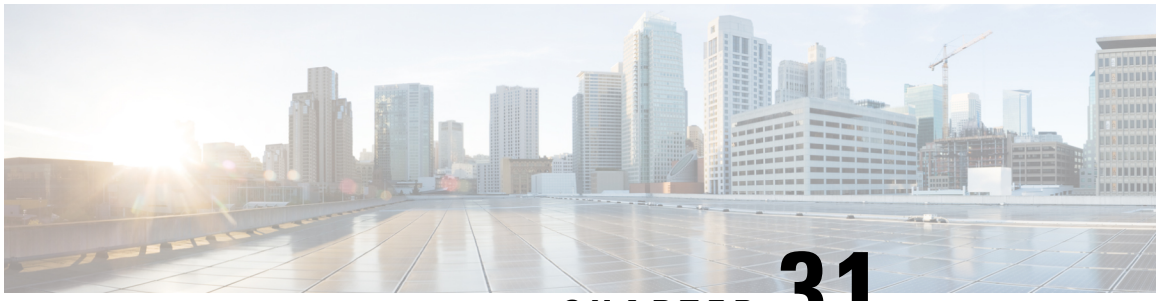
- Clear the wIPS statistics in the controller by entering this command:

  clear stats wps wips

Cisco Adaptive wIPS Alarms

The controller supports five Cisco Adaptive wIPS alarms that serve as notifications for potential threats. You must enable these alarms based on your network topology using Cisco Prime Infrastructure. For more details on this, see the Cisco Prime Infrastructure User Guide.

- Device not protected by VPN—The controller generates an alarm when a wireless client and access point does not communicate over secure VPN, as all controller traffic must be routed through a VPN connection.
- WPA Dictionary Attack—The controller generates an alarm when a dictionary attack on the WPA security key occurs. The attack is detected before the initial handshake message between the client and the access point.
- WiFi Direct Session Detected—The controller generates an alarm when Wifi direct sessions of clients are detected with Wifi direct and prevents enterprise vulnerability.
- RSN Info Element Out-of-Bound Denial-of-Service—The controller generates an alarm when there are large values for RSN information element that results in an access point crash.
- DS Parameter Set DoS—The controller generates an alarm when confusion exists in the channel for the client while multiple channels overlap.



CHAPTER 31

Advanced Wireless Tuning

- Aggressive Load Balancing, on page 619
- Reanchoring of Roaming Voice Clients, on page 621
- SpectraLink NetLink Telephones, on page 623
- Receiver Start of Packet Detection Threshold, on page 624

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 FlexConnect APs do support client load balancing.

Note For a FlexConnect AP the association is locally handled. The load-balancing decisions are taken at the controller. A FlexConnect AP initially responds to the client before knowing the result of calculations at the controller. 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)

Procedure

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)

Procedure

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*

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.

This section contains the following subsections:

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.

Configuring Reanchoring of Roaming Voice Clients (GUI)

Procedure

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)

Procedure

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

SpectraLink NetLink Telephones

For the best integration with the Cisco Wireless 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.

Enabling Long Preambles (GUI)

Procedure

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)

Procedure

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.

Receiver Start of Packet Detection Threshold

Receiver Start of Packet Detection Threshold (Rx SOP) determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. As the Wi-Fi level increases, the radio sensitivity

decreases and the receiver cell size becomes smaller. Reduction of the cell size affects the distribution of clients in the network.

Rx SOP is used to address clients with weak RF links, sticky clients, and client load balancing across access points. Rx SOP helps to optimize the network performance at high-density deployments.

Note Rx SOP configuration is not applicable to 3rd radio module pluggable on 3600 AP.

Guidelines and Restrictions for RxSOP

- Configure this feature only if you have performed a complete site survey throughout your entire coverage area so that you know the RSSI at which all clients' signal levels are received at each AP.
- For information about support on various Wave 2 APs, see Feature Matrix for Wave 2 and 802.11ax (Wi-Fi 6) Access Points.
- RxSOP configurations are supported only in Local, FlexConnect, Bridge, and Flex+Bridge modes.

  RxSOP configurations are not supported in the FlexConnect+PPPoE, FlexConnect+PPPoE-wIPS, and FlexConnect+OEAP submodes.

Configuring Rx SOP (GUI)

Procedure

Step 1 Choose **Wireless > Advanced > Rx SOP Threshold** to configure the high, medium, and low Rx SOP threshold values for each 802.11 band. The table below shows the Rx SOP threshold values for high, medium and low levels for each 802.11 band.

Table 23: Rx SOP Thresholds

802.11 Band	High Threshold	Medium Threshold	Low Threshold
5 GHz	-76 dBm	-78 dBm	-80 dBm
2.4 GHz	-79 dBm	-82 dBm	-85 dBm

Step 2 Choose **Wireless > RF Profiles** to configure the Rx SOP threshold value for an RF profile. The RF profiles page is displayed.

a) Click an RF profile to open the RF Profile > Edit page.
b) In the **High Density** tab, choose the Rx SOP threshold value from the **Rx SOP Threshold** drop-down list.

What to do next

Verify information about Rx SOP thresholds for an 802.11 band by using the**show** {**802.11a** | **802.11b**} **extended** command.

Configuring RxSOP (CLI)

Procedure

Step 1 Configure RxSOP threshold values for each 802.11 band by entering this command:

config {**802.11a | 802.11b** } **rx-sop threshhold** {**high | medium | low | default | custom**}

You can configure the RxSOP thresholds for an access point or on all access points in an 802.11 band.

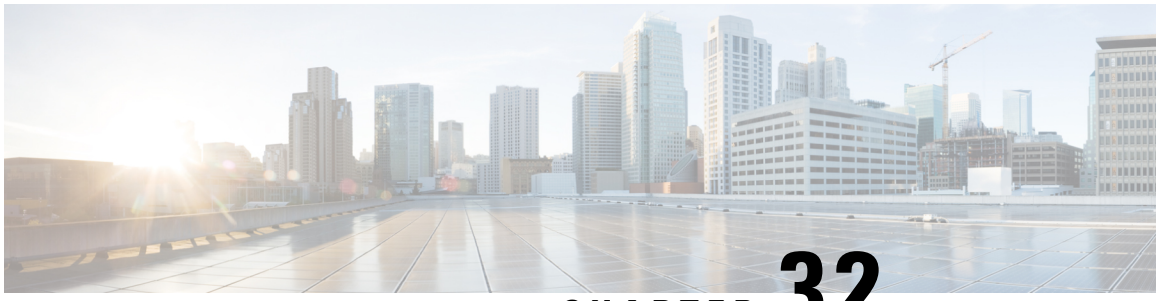
Step 2 Configure RxSOP threshold values for an RF profile by entering this command:

config rf-profile rx-sop threshold {**high | medium | low | default | custom**} *profile_name*

Step 3 View information about RxSOP thresholds for an 802.11 band by entering this command:

show {**802.11a** | **802.11b**} **extended**

```
(Cisco Controller) > show 802.11a extended
Default 802.11a band Radio Extended Configurations:
    Beacon period: 100, range: 0 (AUTO);
    Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
    RX SOP threshold: -76; CCA threshold: 0 (AUTO);

AP3600-XALE3  34:a8:4e:6a:7b:00
    Beacon period: 100, range: 0 (AUTO);
    Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
    RX SOP threshold: -76; CCA threshold: 0 (AUTO);
AP54B4  3c:ce:73:6c:42:f0
    Beacon period: 100, range: 0 (AUTO);
    Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
    RX SOP threshold: -76; CCA threshold: -80;
```



CHAPTER 32

Timers

- Information about Wireless Timers, on page 627
- Configuring Wireless Timers (GUI), on page 627
- Configuring Wireless Timers (CLI), on page 628

Information about Wireless Timers

This feature allows you to set the authentication timeout duration for the client's first attempt to associate with the controller. After the client is authenticated, the controller uses the default 10-second timeout duration.

In a situation where clients seek other APs due to an AP failure causing a gap in the wireless coverage area, the AP after it reassociates sends reports on the client's connectivity to the controller. Based on these AP reports, the controller increases the transmit power of the AP to reduce the coverage gap. This feature addresses the need for AP statistics report to be sent to the controller at an interval of 60 seconds. This report is sent from the controller to the accounting server every 60 seconds. This helps reduce the delay in accounting data usage by a device.

Restrictions for Wireless Timers

The AAA interim accounting interval must be a multiple of the RRM CHD Report interval. The tolerance for odd **AP CHD report** value is 30 seconds.

For example, if **AP CHD report** value is 60 seconds, then the **AAA accounting interim interval value id** is in multiples of 60, 120, 180 seconds, and so on.

Configuring Wireless Timers (GUI)

Procedure

Step 1 Choose **Wireless** > **Timers** to open the **Timers** page.

Step 2 Enter the value in **802.11 Authentication Response Timeout (seconds)** field.

Step 3 Configure the minimum interval setting for volume metering.

a) Enter the value in seconds in the **RRM CHD Report Interval** field. The range is between 60 and 90 seconds. Default is 90 seconds.
b) Choose **WLANs** > **WLAN ID** > **Security** > **AAA Servers** to open the WLAN AAA server page.
c) Enter the **Interim Interval** value in **RADIUS Server Accounting**.

Note
Ensure that the duration is in multiples of the RRM CHD Report Interval seconds. Valid range is between 0 to 3600 seconds.

Example:

If **RRM CHD Report Interval** is set to 60 seconds, then enter the **Interim Interval** value as 60, 120, 180, 240, and so on, seconds.

Step 4 Click **Apply**.

Configuring Wireless Timers (CLI)

Procedure

- Configure the 802.11 authentication response timeout by entering this command:

  config advanced timers auth-timeout *seconds*

  The default value is 10 seconds.

- Configure the minimum interval setting for volume metering by entering these commands:
  a) Configure the AP coverage Report duration by entering this command:

     config advanced timers ap-coverage-report *interval-seconds*

     Range is between 60 and 90 seconds.

  b) Configure the RADIUS Server Accounting interim interval by entering this command:

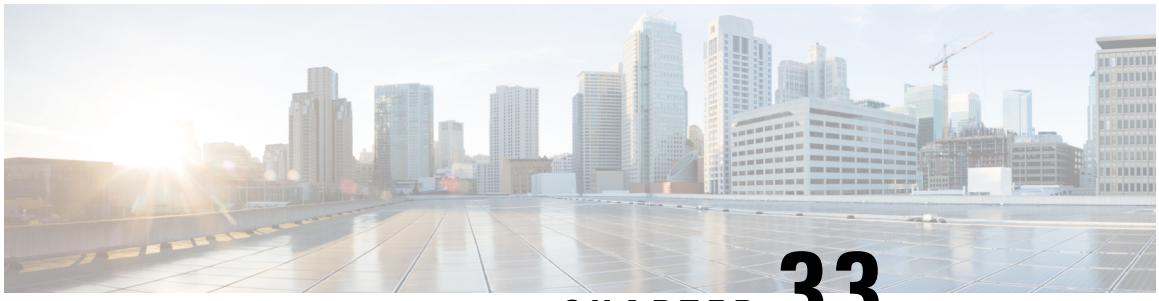
     config wlan radius_server acct interim-update *interval*

     Valid range is between 0 to 3600 seconds.

PART V

Access Points

- AP Power and Uplink LAN Connections, on page 631
- AP Connectivity to Controller, on page 655
- Managing APs, on page 705



CHAPTER 33

AP Power and Uplink LAN Connections

- Power over Ethernet, on page 631
- Cisco Discovery Protocol, on page 634
- Cisco Wave 2 AP's USB Port as Power Source , on page 641
- Viewing AP Serviceability (AP CLI), on page 643
- Cisco 700 Series Access Points, on page 644
- Converting Cisco Wave 2 AP AUX Port to Downlink LAN (RLAN) Port (CLI), on page 651

Power over Ethernet

This section contains the following subsections:

Configuring Power over Ethernet (GUI)

Procedure

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.

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 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*

- 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.
```

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 We recommend 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 3504 Wireless Controller
  - Cisco 5520 Wireless Controller
  - Cisco 8540 Wireless Controller
  - CAPWAP-enabled access points
- 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.
- LLDP is enabled on the APs by default and cannot be disabled.

Configuring the Cisco Discovery Protocol

Configuring the Cisco Discovery Protocol (GUI)

Procedure

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)

Procedure

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)

Procedure

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)

Procedure

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

Cisco Wave 2 AP's USB Port as Power Source

Cisco Aironet 2800 and 3800 Series APs have a USB port that can act as a source of power for some USB devices. The power can be up to 2.5W; if a USB device draws more than 2.5W of power, the USB port shuts down automatically. The port is enabled when the power draw is 2.5W and lower.

Note The controller records the last five power-overdrawn incidents in its logs.

Caution When unsupported USB device is connected to the Cisco AP, the following message is displayed:

```
The inserted USB module is not a supported device. The behavior of this
USB device and the impact to the Access Point is not guaranteed. If Cisco
determines that a fault or defect can be isolated due to the use of
third-party USB modules installed by a customer or reseller, Cisco may
withhold support under warranty or support program under contract. In the
course of providing support for Cisco networking products, the end user
may be required to install Cisco-supported USB modules in the event Cisco
determines that removing third-party parts will assist Cisco in diagnosing
root cause for troubleshooting purposes. Cisco also reserves the right
to charge the customer per then-current time and material rates for
services provided to the customer when Cisco determines, after having
provided such services, that an unsupported device caused the root cause
of the defective product
```

Configuring Cisco Aironet AP's USB Port as Power Source (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs** > **access point name** > **Advanced** tab to open the **Advanced** page.

Step 2 Check the **USB Module Status** check box to enable the USB port.

Note
When the USB device draws power exceeding 2.5W, the USB port is disabled. The status shows the status as Disabled due to over current.

Note
Custom configurations on the *default-group* are not saved and are valid till the next controller reboot only.

Step 3 [Optional] Check the **Override** check box to enable the USB Module on the particular AP or uncheck to apply the AP group setting to the AP.

Step 4 Click **Apply**.

Step 5 Choose the **Inventory** tab to open the **All APs** > **Details** for (Inventory) page.

This page shows the connected USB Module details.

Configuring a Cisco AP Group to Use the Cisco AP's USB Port as Power Source (GUI)

Procedure

Step 1 Choose **WLANs** > **Advanced** > **AP Groups** > **AP_group_name** > **Ports/Module** tab.

Step 2 Check the **USB Module** check box in the **External Module** section to enable on all the APs in this Cisco AP group.

Step 3 Choose **Wireless** > **Access Points** > **All APs** > **Access Point name** > **Advanced** tab to open the **Advanced** page.

Step 4 [Optional] Check the **Override** check box to toggle the override state of USB Module setting on a particular AP or uncheck to apply the AP group setting to the AP.

Step 5 Check the **USB Module Status** to view the **USB Module Operations State** of the port.

Note
When the USB device draws power exceeding 2.5W, the USB port is disabled. The status shows the status as Disabled due to over current.

Step 6 Choose the **Inventory** tab to open the **All APs** > **Details** for (Inventory) page.

This page shows the connected USB Module details.

Configuring Cisco Aironet APs USB Port as Power Source (Controller CLI)

Procedure

- Enable or disable the USB port on an AP by entering this command:

  config ap usb-module {**enable | disable**} *ap-name*

- Enable or disable the USB port, overriding the AP group setting by entering this command:

  config ap usb-module over-ride {**enable | disable**} *ap-name*

- Enable or disable the USB port on all the APs belonging to a specific AP group by entering this command:

  config wlan apgroup port usb-module *ap-group-name* {**enable | disable**}

Note Custom configurations on the *default-group* are not saved and are valid till the next controller reboot only.

- View the inventory details on all APs or a specific AP by entering this command:

  show ap inventory {**all | ap_name**}

Viewing Cisco Aironet APs USB Port as Power Source (AP-CLI)

Procedure

- View the USB Inventory by entering this command:

  show inventory

- View the USB port status by entering this command:

  show interfaces usb

Viewing AP Serviceability (AP CLI)

This section lists the Cisco Wave 2 AP supported CLIs you can use to view the serviceability parameters.

Procedure

- View the last recorded power level (per antenna RSSI) from the antenna by entering this command:

  show controllers dot11Radio *radio(0-1)* **antenna**

- View the details of the client such as rate selection, streams by entering this command:

  show controllers dot11Radio *radio(0-1)* **client** *MAC-address*

Cisco 700 Series Access Points

The Cisco Aironet 700 Series is a compact access point that delivers secure and reliable wireless connections. The main features are:

- Simultaneous dual band, dual radio with support for 2.4GHz and 5GHz.
- Optimized antenna and radio designs: Consistent network transmit and receive for optimized rate versus range.
- Radio resource management (RRM): Automated self-healing optimizes the unpredictability of RF to reduce dead spots and help ensure high-availability client connections.
- Cisco BandSelect improves 5-GHz client connections in mixed-client environments.
- Advanced security features including Rogue Detection, wIPS and Context-Aware.

Configuring Cisco 700 Series Access Points

The Cisco 700 series access points has four LAN ports. The configuration of these ports is stored in a file on flash. The AP retrieves the configuration when restarted. The AP then shares the information with Controller after joining so that Controller can display the updated information.

Note The AP deletes the saved port information and applies the default configuration when the controller clears all the existing configuration on the AP. All LAN ports are disabled by default.

Enabling the LAN Ports (CLI)

Procedure

- Enable or disable a LAN port on the access point by entering this command:
  config ap lan port-id *port-id* {**enable** | **disable**} *ap-name*
- See the port information by entering this command:
  showap lan port-id *port-id ap-name*
- See the port summary information by entering this command:
  showap lan port-summary *ap-name*

Enabling 702W LAN Ports

All ports are mapped to the same access VLAN that the AP's switch port is configured to. Alternatively, the ports are mapped to the native VLAN if port is a trunk. It is possible to enable or disable the ports and map them to specific VLANs if needed. This allows traffic to be separated not only between wireless and wired networks, but also among the four Ethernet ports.

Procedure

Step 1 Enable or disable a LAN port on the access point by entering this command:
config ap lan port-id *port-id* { **enable** | **disable**} *ap-name*

Step 2 Configure the port ID by entering this command:
config ap lan port-id *port-id ap-name*

Step 3 Configure VLAN for the AP by entering this command:
config ap lan enable access vlan *vlan-id port-id ap-name*

Remote LAN Support for Wired Ports on Cisco Aironet 702W APs

A remote LAN (RLAN) in Cisco Aironet 702W access points (APs) are used for authenticating wired clients using Cisco Wireless LAN Controller. You can set the various IEEE 802.1X authentication modes for the LAN ports in Cisco 702W APs by configuring them in RLAN.

The IEEE 802.1X authentication message exchange between a client and an authentication server is carried out locally in APs. All IEEE 802.1X configurations are carried out through controller. Both port control and restrictions are considered locally in APs.

Role of Controller

Controller acts as an authenticator, and Extensible Authentication Protocol (EAP) over LAN (EAPOL) messages from the wired client reaches controller through an AP, and controller communicates with the configured authentication, authorization, and accounting (AAA) server.

Role of an AP

An AP acts as a relay in tunneling the authentication packets from a wired client to controller using the Control and Provisioning of Wireless Access Points (CAPWAP) tunnel. After a port is authenticated, the AP is responsible for port control and monitoring.

LAN ports for an AP are configured in controller and then pushed to the corresponding AP.

Initially, the AP configures the IEEE 802.1X port if the client that joins the AP passes the EAPOL packets to the controller.

IEEE 802.1X Authentication Modes

This topic describes the different IEEE 802.1X authentication modes.

Single-Host Mode

If the single-host authentication mode is configured in an AP and the port link state is up, the AP detects the client by sending the EAPoL frame. If the client leaves or is replaced with another client, the AP changes its port link state to down, making the port unauthorized.

The single-host configuration mode is configured using the existing RLAN configurations in the controller.

Multi-Host Mode

If the multi-host authentication mode is configured, only one client can be authenticated for all the clients to gain network access in that port. If the port becomes unauthorized, the switch denies access to all the attached clients.

Violation Mode

When a security violation occurs, a port is protected based on the following configured violation actions:

- Shutdown—Disables the port.
- Replace—Removes the current session and initiates authentication for the new host. This is the default behavior.
- Protect—Drops packets with unexpected MAC addresses without generating a system message.

In the single-host authentication mode, a violation is triggered when more than one device is detected in data VLAN. In a multi-host authentication mode, a violation is triggered when more than one device is detected in data VLAN or voice VLAN.

Note Security violation cannot be triggered in the multi-host authentication mode.

Configuring Preauthentication Open (CLI)

- The preauthentication open option allows unrestricted traffic on an AP LAN port initially, and is restricted only by other access restrictions.
- The preauthentication open feature is not supported in Cisco Aironet 1810 OEAPs.

Procedure

config remote-lan pre-auth {**enable | disable**} *remote-lan-id* **vlan** *vlan-id*

Example:

```
config remote-lan pre-auth enable 8 vlan vlan2
```

Configures preauthentication open on a VLAN.

Configuring IEEE 802.1X Authentication Modes (CLI)

You can configure three different authentications modes:

- **Single-host**
- **Multi-host**
- **Violation-mode**

Procedure

Perform one of the following tasks to configure authentication:

- **config remote-lan host-mode singlehost** *remote-lan-id*

  Example:

  ```
  (Cisco Controller) > config remote-lan host-mode singlehost 7
  ```

  Configures a remote LAN single-host mode. In single-host mode, violation is triggered when more than one device is detected in data VLAN.

- **config remote-lan host-mode multihost** *remote-lan-id*

  Example:

  ```
  (Cisco Controller) > config remote-lan host-mode multihost 8
  ```

  Configuresa remote LAN multi-host mode. In multi-host mode, a violation is triggered when more than one device is detected in data or voice VLAN. Note that security violation cannot be triggered in multi-host mode.

- **config remote-lan violation-mode** {**protect** | **replace** | **shutdown**}*remote-lan-id*

  Example:

  ```
  (Cisco Controller) > config remote-lan violation-mode protect 7
  ```

  Configures violation mode for remote LAN.

Enabling IEEE 802.1X Authentication in Controller (GUI)

Procedure

Step 1 Choose **WLANs**.

The **WLANs** window is displayed.

Step 2 Click the ID number of the corresponding WLAN.

The **WLANs > Edit** window is displayed.

Step 3 Click the **Security** > **Layer 2** tab.

Step 4 From the **Layer 2 Security** drop-down list, choose **802.1X**.

The IEEE 802.1X parameters are displayed.

a) Select **Host Mode** from the drop-down list.
b) Select **Violation Mode** from the drop-down list.

c) Select the **Pre Authentication** check box and enter pre-authentication VLAN identifier in the Pre Auth Vlan field.

Step 5 Click **Apply**.

Enabling IEEE 802.1X Authentication (CLI)

Enable IEEE 802.1X authentication using the existing remote LAN configuration. After configuring the remote LAN in controller, apply the configuration to the AP group and then push to the individual APs present in that AP group.

Procedure

Step 1 **config remote-lan security 802.1x** {**enable** | **disable**} *remote-lan-id*

Example:

```
(Cisco Controller) > config remote-lan security 802.1X enable 7
```

Configures the security policy for a remote LAN.

Step 2 **config remote-lan apgroup add** *ap-group*

Example:

```
(Cisco Controller) > config remote-lan apgroup add apgroup1
```

Adds a WLAN AP group for a remote LAN.

Mapping an RLAN to an AP Port in Controller (GUI)

Perform this procedure to map an RLAN to an AP port. This task can be performed either per AP or per AP group.

Procedure

Step 1 Choose **WLANs > Advanced > AP Groups**.

The AP Groups window is displayed.

Step 2 Click the corresponding AP Group Name.

The **AP Group > Edit** window is displayed.

Step 3 Click on **WLANs** tab, and then click **Add New**.

The **Add New** area is displayed.

Step 4 Use the drop-down list from WLAN SSID to select the RLAN to be added.

Step 5 From the **Interface/Interface Group** drop-down list, to choose the group it belongs to.The default choice is **management**.

Step 6 Click **Add**.

Step 7 Click the **Ports/Module** tab.

Step 8 In the **LAN Ports** area, use the drop-down to add the RLAN to the LAN port.

Step 9 Click **Apply**.

Mapping an RLAN to an AP Port in Controller (CLI)

Map the LAN ports in an AP to the remote LAN that is configured, for authentication to take place. Perform the port-level configurations through the LAN port configuration in the AP group level.

Procedure

config remote-lan apgroup port port-sardinia *port-id*

Example:

```
(Cisco Controller) > config remote-lan apgroup port port-sardinia 1 apgroup1 remote-lan
```

Assigns a remote LAN to a LAN port in an AP group.

Mapping an RLAN to an AP Port in Controller per AP (GUI)

Perform this procedure to map an RLAN to an AP port. This task can be performed either per AP or per AP group.

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs**.

The **All APs** window is displayed.

Step 2 Click the corresponding AP.

The **AP Details** window is displayed.

Step 3 Click the **Interfaces** tab.

Step 4 In the **LAN Ports** area, set the port state to Enable, and check the **VLAN** check box, and enter the RLAN WLAN ID in the **VLAN ID** field.

Step 5 From the **Layer 2 Security** drop-down list, choose **802.1X**.

The IEEE 802.1X parameters are disaplyed.

Step 6 From the **Key Size** drop-down list, choose the key size for IEEE 802.1X data encryption.

Note

If a preauthentication VLAN is required, enable **Pre Authentication** and enter the Pre Auth VLAN identifier.

Mapping a RLAN to an AP External Port in Controller (GUI)

Perform this procedure to map an RLAN to an AP port. This task can be performed either per AP or per AP group.

Procedure

Step 1 Choose **WLANs** > **Advanced** > **AP Groups**.

The AP Groups window is displayed.

Step 2 Click the corresponding AP Group Name.

The **AP Group** > **Edit** window is displayed.

Step 3 Click on **Ports/Module** tab.

Step 4 Use the RLAN drop-down list to select the RLAN to be mapped.

Step 5 Check the **External Module** check box.

Note
Custom configurations on the *default-group* are not saved and are valid till the next controller reboot only.

Step 6 Click **Apply**.

Mapping a RLAN to an AP External Port in Controller (CLI)

Map the external module in an AP to the remote LAN at the AP group level.

Procedure

config remote-lan apgroup port ext-module *default-group* {**enable** | **disable**}

Example:

```
(Cisco Controller) > config remote-lan apgroup port ext-module default-group enable
```

Enables the external module of the AP in an ap group in the remote LAN .

Note
Custom configurations on the *default-group* are not saved and are valid till the next controller reboot only.

MAB Authentication Support for AP Port LAN Client in Cisco Aironet 702w Access Points

MAC Authentication Bypass (MAB) feature enables port-based access control using the MAC address of an endpoint. An MAB-enabled port can be enabled or disabled based on the MAC address of the device it connects to. MAB is useful when the clients does not recognize EAP packets and is mainly for non-802.1x clients.

This feature is supported in Cisco Aironet 702w access points on the Remote LAN (RLAN).

Configuring MAB Support on AP Port LAN Clients (GUI)

Before you begin

This feature is supported only on Cisco Aironet 702w access points that supports RLAN feature.

Procedure

Step 1 Choose **WLANs** to open the WLANs window.

Step 2 Click the ID number of the desired WLAN to open the **WLANs > Edit** window.

Step 3 Choose the **Security** > **Layer 2** tab.

Step 4 Check the **MAB Mode** check box.

Enables port-based access control using the MAC address of an endpoint.

Configuring MAB Support for AP Port LAN Clients (CLI)

Procedure

config remote-lan mab {**enable** | **disable**} *remote-lan-id*

Example:

```
config remote-lan mab enable 8
```

Enables port-based access control using the MAC address of an endpoint.

Converting Cisco Wave 2 AP AUX Port to Downlink LAN (RLAN) Port (CLI)

Some Wave 2 APs' second Ethernet port, also called the AUX port, is used as a link aggregation (LAG) port, by default. It is possible to use this LAG port as a LAN port when LAG is disabled. When the AUX port is configured as a Downlink LAN (RLAN) Port, you can either use the AP group setting to configure the Downlink LAN (RLAN) Port for a group of APs, or use the LAN override functionality to configure the Downlink LAN (RLAN) Port for each AP separately. This Cisco Wave 2 AP AUX port to Downlink LAN (RLAN) Port conversion feature is supported only in the following APs:

- Cisco Aironet 1850 Series AP
- Cisco Aironet 2800 Series AP
- Cisco Aironet 3800 Series AP
- Cisco Aironet 4800 Series AP

Note After global AP LAG is enabled, the CAPWAP connection with the AP is deleted; that is, the connection is deleted from the database in the controller. This results in AP disjoining and then rejoining the controller. The connection is explicitly deleted from the database in the controller.

After global AP LAG is disabled, for the APs that do not have LAG enabled, their connection is deleted from the database in the controller. This results in APs to disjoin and rejoin the controller.

After global AP LAG is disabled, the APs that have LAG enabled are rebooted.

Procedure

Step 1 By default, the APs are in LAG mode. Check the status of an AP by entering this command:

show ap config general *ap-name*

Note
The `AP LAG Configuration Status` line in the output shows the current LAG status.

Step 2 If LAG mode in the AP is enabled, disable LAG mode by entering this command:

config ap lag-mode support disable *ap-name*

Step 3 Create a remote LAN (RLAN) and enable it by entering these commands:

a) **config remote-lan create** *rlan-id rlan-name*
b) **config remote-lan enable** *rlan-id*

Step 4 Create an AP group for the RLAN that you created by entering this command:

config wlan apgroup add *apgroup-name description*

Step 5 Add the RLAN and the AP to the AP group by entering these commands:

a) **config wlan apgroup interface-mapping add** *apgroup-name rlan-id interface-name*
b) **config ap group-name** *group_name Cisco_AP*

The AP is rebooted after these commands are entered.

Step 6 After the AP is rebooted, assign the RLAN to the Downlink LAN (RLAN) Port (LAN 1) in the AP group by entering this command:

config wlan apgroup port lan *1 apgroup-name* **remote-lan** *rlan-id*

Note
In the supported APs, only LAN 1 can be used.

Step 7 Enable the Downlink LAN (RLAN) Port (LAN 1) for a group of APs in the AP group or for an individual AP by entering these commands:

- For a group of APs in the AP group:

  config wlan apgroup port lan *1 apgroup-name* **enable**

- For an individual AP:

  a. **config ap lan over-ride enable** *ap-name*

  b. **config ap lan port-id** *1* **enable**

Step 8 Connect a client to the AP through the AUX port.

Re-enabling LAG Mode on Cisco Wave 2 APs (CLI)

Procedure

Step 1 Disable the Downlink LAN (RLAN) Port (LAN 1) in the AP group by entering this command:

config wlan apgroup port lan *1 apgroup-name* **disable**

Step 2 Disable the RLAN on the Downlink LAN (RLAN) Port (LAN 1) in the AP group by entering this command:

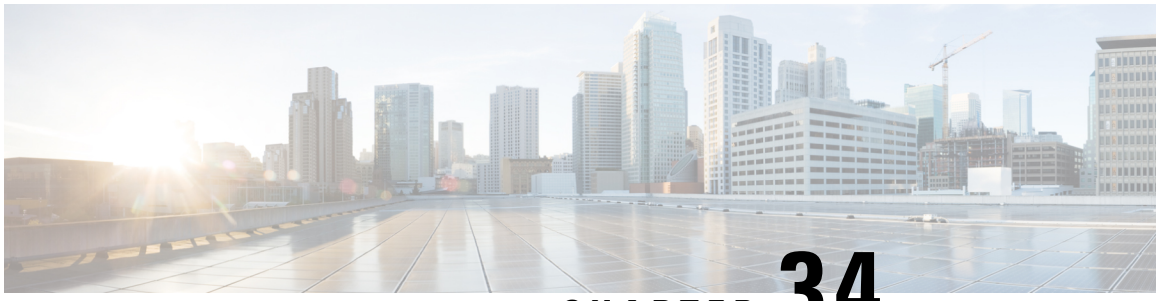
config wlan apgroup port lan *1 apgroup-name* **remote-lan none**

Step 3 If LAN is enabled for an individual AP, disable the LAN override for the AP by entering this command:

config ap lan over-ride disable *ap-name*

Step 4 Enable LAG mode on the AP by entering this command:

config ap lag-mode support enable *ap-name*



CHAPTER 34

AP Connectivity to Controller

- CAPWAP, on page 655
- Preferred Mode, on page 660
- IPv6 CAPWAP UDP Lite, on page 662
- Data Encryption, on page 664
- VLAN Tagging for CAPWAP Frames from Access Points, on page 668
- Discovering and Joining Controllers, on page 669
- Authorizing Access Points, on page 680
- AP Wired 802.1X Supplicant, on page 688
- Configuring a Static IP Address on a Lightweight Access Point, on page 696
- Troubleshooting the Access Point Join Process, on page 699

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 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

- 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 APs, the AP fails to join the controller.
- The sender fragments the IPv6 UDP packets, which are then reassembled at the end device. APs do not support IPv6 reassembly and therefore IPv6 UDP packets are not recognized in the AP datapath.

  This issue does not impact IPv6 TCP because of TCP design. The MSS parameter is a part of the options in the TCP initial handshake that specifies the largest amount of data that a TCP speaker can receive in a single TCP segment. Each direction of TCP traffic uses its own MSS value because this is a receiver-specified value.
- Do not use the following IP addresses with Cisco Wave 2 APs in the network to avoid the AP from dropping packets:
  - 10.128.128.126
  - 10.128.128.127
  - 10.128.128.128
  - 6.0.0.7

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.

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. Specifically for Cisco OEAPs, the least latency controller join feature can be used to guide the AP's controller selection.

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)

Procedure

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)

Procedure

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*

Preferred Mode

Preferred mode allows an administrator to configure CAPWAP L3 transport (IPv4 and IPv6) through which APs join the controller (based on its primary/secondary/tertiary configuration).

There are two levels of preferred mode

- AP Group specific
- Global Configuration

Guidelines for Configuring Preferred Mode

The following preferred mode configurations are available:

- AP-Group specific preferred mode is pushed to an AP only when the preferred mode of AP-Group is configured and the AP belongs to that group.
- Global preferred mode is pushed to default-group APs and to those AP-Groups on which the preferred mode is not configured.
- By default, values of preferred mode for AP-Group and Global is set to un-configured and IPv4 respectively.
- If an AP, with an configured preferred mode, tries to join the controller and fails, then it will fall back to choose AP-manager of the other transport and joins the same controller. When both transports fail, AP will move to next discovery response.
- In such a scenario, Static IP configuration will take precedence over prefer mode. For example:
  - On the controller, the preferred mode is configured with an IPv4 address.
  - On the AP, Static IPv6 is configured using CLI or GUI.
  - The AP will join the controller using IPv6 transport mode.
- The controllers CLI provides an XML support of preferred mode.

Configuring CAPWAP Preferred Mode (GUI)

Procedure

Step 1 Choose **Controller** > **General** to open the Global Configuration page. Select the **CAPWAP Preferred Mode** list box and select either IPv4 or IPv6 as the global CAPWAP Preferred mode.

Note
By default, the controller is configured with an CAPWAP preferred mode IPv4 address.

Step 2 Choose **WLAN** > **Advanced > APGroup > General Tab** and select the **CAPWAP Preferred Mode** checkbox to configure an AP-Group with an IPv4 or IPv6 CAPWAP Preferred Mode.

Step 3 Choose **Wireless** > **ALL APs** > **General Tab** to check the APs CAPWAP setting. Refer to the **IP Config** section to view if the AP's CAPWAP Preferred Mode is applied globally or for an AP-Group.

Step 4 Choose **Monitor** > **Statistics** > **Preferred Mode** to help users to check if the preferred mode command is pushed successfully to an AP.

- Preferred mode of Global/AP Groups: The name of the AP that is configured with either IPv4, IPv6 or global.
- Total: The total count of APs configured with preferred mode.
- Success: Counts the number of times the AP was successfully configured with the preferred mode.
- Unsupported: APs that are not capable of joining in with IPv6 CAPWAP.
- Already Configured: Counts the attempts made to configure an already configured AP.
- Per-AP Group Configured: Preferred mode configured on per AP-Group.
- Failure: Counts the number of times the AP was failed to get configured with the preferred mode.

Configuring CAPWAP Preferred Mode (CLI)

Procedure

Step 1 Use this command to configure preferred mode of AP-Group and all APs. Global preferred mode will not be applied on APs whose AP-Group preferred mode is already configured. On successful configuration, the AP will restart CAPWAP and join with the configured preferred mode after choosing a controller based on its primary/secondary/tertiary configuration.

config ap preferred-mode {**ipv4** | **ipv6**} {*apgroup-name* | **all**}

Step 2 Use this command to disable (un-configure) the preferred mode on the AP.

config ap preferred-mode disable *apgroup-name*

Note
APs that belong to *apgroup-name* will restart CAPWAP and join back the controller with global preferred mode.

Step 3 Use this command to view the statistics for preferred mode configuration. The statistics are not cumulative but will be updated for last executed configuration CLI of preferred mode.

show ap prefer-mode stats

Step 4 Use this command to view the preferred mode configured for all AP-Groups.

show wlan apgroups

Step 5 Use this command to view the global preferred mode configured.

show network summary

Step 6 Use this command to view to check if the preferred mode command is pushed to an AP from global configuration or from an AP-Group specific configuration.

show ap config general *ap-name*

```
(Cisco Controller) >show ap config general AP-3702E

Cisco AP Identifier.............................. 2
Cisco AP Name.................................... AP-3702E
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...................................... bc:16:65:09:4e:fc
IPv6 Address Configuration....................... SLAAC
IPv6 Address..................................... 2001:9:2:35:be16:65ff:fe09:4efc
IPv6 Prefix Length............................... 64
Gateway IPv6 Addr................................ fe80::a2cf:5bff:fe51:c4ce
NAT External IP Address.......................... None
CAPWAP Path MTU.................................. 1473
Telnet State..................................... Globally Enabled
Ssh State........................................ Globally Enabled
Cisco AP Location................................ default location
Cisco AP Floor Label............................. 0
Cisco AP Group Name.............................. default-group
Primary Cisco Switch Name........................ amb
Primary Cisco Switch IP Address.................. 9.2.35.25
.....................................
.....................................
.....................................
.....................................
.....................................
Ethernet Port Speed.............................. Auto
AP Link Latency.................................. Disabled
Rogue Detection.................................. Enabled
AP TCP MSS Adjust................................ Disabled
IPv6 Capwap UDP Lite............................. Enabled
Capwap Prefer Mode............................... Ipv6 (Global Config)
Hotspot Venue Group.............................. Unspecified
Hotspot Venue Type............................... Unspecified
DNS server IP ..................... Not Available
```

IPv6 CAPWAP UDP Lite

The UDP Lite feature, which is an enhancement to the existing IPv6 functionality, supports the UDP Lite protocol. This feature is only applicable to the IPv6 addresses of the controller and APs. IPv6 mandates complete payload checksum for UDP. The UDP Lite feature minimizes the performance impact on the controller and AP by restricting the checksum calculation coverage for the UDP Lite header to 8 bytes only.

This feature impacts intermediate firewalls to allow UDP Lite protocol (protocol ID of 136) packets. Existing firewalls might not provide the option to open specific ports on UDP Lite protocol. In such cases, the administrator must open up all the ports on UDP Lite.

Configuring UDP Lite Globally (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points > Global Configuration** to open the Global Configuration page.

Step 2 Under the **Global UDP Lite** section, select the **UDP Lite** checkbox to enable UDP Lite globally.

Note
IPv6 UDP Lite is not applicable for APs connected with CAPWAPv4 tunnel. They are applicable only for APs joining the controller using CAPWAPv6 tunnel.

Step 3 Click **Apply** to set the global UDP Lite configuration.

Step 4 If desired, you can choose to override the global UDP Lite configuration by unselecting the Global IPv6 UDP Lite mentioned in Step 2.

Note
Switching between UDP and UDP Lite causes the AP to disjoin and rejoin.

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

Configuring UDP Lite on AP (GUI)

Procedure

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

Step 2 Select an **AP Name** with an IPv6 address and click on it to open the **Details** page of the selected AP.

Step 3 Under the **Advanced** tab, select the **UDP Lite** checkbox to enable UDP Lite for the selected AP.

Note
This field is displayed only for APs that have joined the controller over CAPWAPv6 tunnel. The Web UI page does not display this field for APs joining the controller over the CAPWAPv4 tunnel .

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

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

Configuring the UDP Lite (CLI)

Procedure

Step 1 Use this command to enable UDP Lite globally.

config ipv6 capwap udplite enable *all*

Step 2 Use this command to enable UDP Lite on a selected AP.

config ipv6 capwap udplite enable *ap-name*

Step 3 Use this command to disable UDP Lite globally.

config ipv6 capwap udplite disable *all*

Step 4 Use this command to disable UDP Lite on a selected AP.

config ipv6 capwap udplite disable *ap-name*

Step 5 Use this command to view the status of UDP Lite on a controller.

show ipv6 summary

```
(Cisco Controller) >show ipv6 summary

Global Config.............................. Disabled
Reachable-lifetime value................... 300
Stale-lifetime value....................... 86400
Down-lifetime value........................ 30
RA Throttling.............................. Disabled
RA Throttling allow at-least............... 1
RA Throttling allow at-most................ 1
RA Throttling max-through.................. 10
RA Throttling throttle-period.............. 600
RA Throttling interval-option.............. passthrough
NS Mulitcast CacheMiss Forwarding.......... Disabled
NA Mulitcast Forwarding.................... Enabled
IPv6 Capwap UDP Lite....................... Enabled
Operating System IPv6 state ............... Disabled
```

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

Note Cisco Wave 1 APs supports TLS v1.0 only.

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.

Cipher Suites Supported by APs

- Cipher suites supported by Cisco Aironet 4800, 3800, 2800, 1800, and 1560 Series APs:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DH_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DH_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- Cipher suites supported by Cisco Aironet 3700, 2700, 3600, 2600 Series, and 802 APs:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA256

Restrictions on Data Encryption

- The following access points support DTLS data encryption with hardware-based encryption: 1540, 1560, 1570, 1700, 1815, 2700, 2800, 3700, 3800, and 4800.
- DTLS data encryption is not supported on Cisco Aironet 700, 800, 1530 Series APs.
- Cisco Wave 1 APs does not support TLS v1.2.
- 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.
- You can use the controller to enable or disable DTLS data encryption for a specific access point or for all APs.
- Some AP models have hardware-based DTLS support, but some do not. The APs that do not have hardware-based DTLS support will have significantly reduced throughput if Data DTLS is enabled.
- Central switching is not supported on Cisco vWLC and therefore Data DTLS is not supported on Cisco vWLC.
- For Cisco 5520 and 8540 Wireless Controllers, data DTLS is available without the need for an additional license.
- 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.

Configuring Data Encryption (GUI)

Ensure that the base license is installed on the controller. Once the license is installed, you can enable data encryption for the access points.

Procedure

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:

Procedure

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 Enable new cipher suites for DTLS connection between AP and controller by entering this command:

config ap dtls-cipher-suite {**RSA-AES256-SHA256** | **RSA-AES256-SHA** | **RSA-AES128-SHA**}

Note
If you choose to use the **RSA-AES256-SHA256** option, ensure that you set the DTLS version to **dtls_all** in the next step.

Step 7 Configure the DTLS version by entering this command:

config ap dtls-version {**dtls1.0** | **dtls1.2** | **dtls_all**}

Step 8 See the summary of DTLS cipher suite by entering this command:

show ap dtls-cipher-suite

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.

For more information about which APs support CAPWAP VLAN Tagging, see Feature Matrix for Wave 2 and 802.11ax (Wi-Fi 6) Access Points.

This section contains the following subsections:

Configuring VLAN Tagging for CAPWAP Frames from Access Points (GUI)

Procedure

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, check the **VLAN Tagging** check box.

Step 5 In the **Trunk VLAN ID** field, enter an ID.

If the AP is unable to route traffic through the specified trunk VLAN after about 10 minutes, the AP 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 AP 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 AP 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 AP. 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)

Procedure

Step 1 Configure VLAN tagging for CAPWAP frames from APs 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*}

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.

Discovering and Joining Controllers

This section contains the following subsections:

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:

- 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.
- 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.

Note You can configure up to three IP addresses in the hexadecimal string.

- 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.
- 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.

Guidelines and Restrictions on Controller Discovery Process

- 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.
- Cisco 2800 and 3800 Series APs replaces the underscore with a hypen in hostname field of DHCP Discover packet. For more information about this behavior, see **RFC1035**.

- 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.

Using DHCP Option 43 and DHCP Option 60

Cisco access points use the type-length-value (TLV) format for DHCP option 43. DHCP servers must may 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. For more information about DHCP option 43, see https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html.

If the AP is ordered with the Service Provider Option - AIR-OPT60-DHCP selected, the VCI string for that AP 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.

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)

Procedure

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 8540 Controllers is 10–15 (inclusive) and is 1–10 (inclusive) for other controllers. The default value for the heartbeat timeout for Cisco 8540 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 8540 Controllers is 10–15 (inclusive) and is 1–10 for other controllers. The default value for the heartbeat timeout for Cisco 8540 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)

Procedure

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 10 and 15 seconds for Cisco 3504, 5520, and 8540 controllers, and 1 and 10 seconds for Cisco vWLC controllers. 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.................. 192.0.2.1
Secondary Cisco Switch Name...................... 1-8540
Secondary Cisco Switch IP Address................ 198.51.100.1
Tertiary Cisco Switch Name....................... 2-8540
Tertiary Cisco Switch IP Address................. 209.165.201.1
...
```

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......................... Mak_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
```

Failover Priority for Access Points

If a controller has the maximum number of supported APs joined to it, the failover priority feature allows it to disconnect a lower priority AP, if a higher priority AP tries to join.

The default priority is 1, the lowest priority; set higher priorities on APs if you want to enable this feature.

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 slots.
- 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)

Procedure

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)

Procedure

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.

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.

Procedure

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 2 and 5 seconds. The valid range for the **count** parameter is between 3 and 8.

- 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 2 and 5 seconds. The valid range for the **count** parameter is between 3 and 8.

- 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*

Authorizing Access Points

When an AP joins a controller, that connection is mutually authenticated via X.509 certificates, that is, the controller authenticates the AP's certificate and the AP authenticates the controller's certificate.

All Cisco wireless controllers and all Cisco APs manufactured after July 18 2005, have manufacturing installed certificates (MICs).

By default, the controllers and APs authenticate each other via MICs. MICs generated before mid-2017 expire after 10 years, at which point, by default, the APs will no longer be able to join the controller. To allow the APs with expired MICs to join the controller, and/or APs to join a controller with an expired MIC, use the following command:

config ap cert-expiry-ignore mic enable

For more information, see this field notice: https://www.cisco.com/c/en/us/support/docs/field-notices/639/fn63942.html.

Authorizing Access Points against Local MAC Address

By default, the controller accepts AP authorization based on MIC and does not accept or require any other form of AP authorization. If you want to allow APs with SSCs to join, enable it, if you want APs with LSCs to join, enable it.

Mesh APs must be MAC authorized in addition to certificate authorized. For extra security, you can configure MAC authorization of other APs.

This section contains the following subsections:

Authorizing Access Points Using SSCs

Cisco APs manufactured prior to 2005 did not have MICs. Tools were provided to generate SSCs on older APs without MICs. Those tools and APs are no longer supported. All such SSCs expired on January 1, 2020. To allow the APs with the expired SSCs to join the controller, use the following command:

config ap cert-expiry-ignore ssc enable

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.

Note When a factory default AP tries to join the virtual controller, the SSC token does not get downloaded when AP joins initially. So once the AP gets registered with a controller, we need to reconfigure the SSC token to push it to the AP. The AP will then save the SSC token.

To push the SSC token to the AP, use the command

config certificate ssc auth-token *token*

Configuring SSC (GUI)

Procedure

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)

Procedure

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.

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.
  - Starting in Release 8.8, when LSC is enabled, the LSC device certifcate present can be configured. By default, the device certificate is disabled. For more information, see https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvk38802.
- 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.
- If you are using Cisco 3504 Controller and want to update device certificate, we recommend that you use Windows Server 2012 R2 as the certificate authority server. If you are using Windows Server 2008 R2 as the certificate authority server, there exists a known issue for which you must have a fix. For more information about this issue and the fix, see https://support.microsoft.com/en-us/help/2483564/renewal-request-for-an-scep-certificate-fails-in-windows-server-2008-r.

Configuring Locally Significant Certificates (GUI)

Procedure

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)

Procedure

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)

Procedure

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

Plug and Play (PnP)

PnP solution provides staging parameters to the AP before it joins a controller. Using this staging configuration, the AP gets the runtime configuration when it joins the controller. PNP is activated on AP only if the AP is fresh out-of-box or reset to the factory default. PnP is not initiated after the AP connects to the controller for the first time.

PnP IPv4 functionality is supported on Cisco Aironet 700, 1700, 2700, and 3700 series APs.

Both PnP IPv4 and IPv6 functionalities are supported on Cisco Wave 2 802.11ax Wi-Fi6 APs. For more information about specifc APs that support PnP, see https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html.

AP PnP Scenarios

- On-Premise Redirection—Customer hosting the PNP server in the customer-internal network. APs discover the PnP server using the DHCP option or DNS resolution.

Note For AP time sync with the controller, configure the controller NTP server with a reachable NTP IP address. APs do not support FQDN in a day0 scenario.

- Cloud Redirection—APs are connected to the third-party network where customers do not have control over the DHCP or DNS, or do not host the PNP server. In this scenario, AP connects to the Cisco Cloud redirect service to get either the controller or PnP address. The controller address is configured in the redirect service for customers without the PnP server.

For more information about PnP, see the documentation for *Wireless Plug and Play Deployment Guide* at http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-4/b_wireless_plug_and_play_deployment_guide.html.

AP Wired 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.

Here, the Cisco switch is the authenticator; the Cisco AP is the supplicant, and the RADIUS/ISE server the authentication server. You may enable one of the three protocols—EAP-TLS, EAP-PEAP, or EAP-FAST on the controller to authenticate the supplicant devices (APs).

The EAP-TLS protocol uses the client certificate to authenticate the device. On the other hand, the EAP-PEAP protocol uses the client key exchange to authenticate the AP. This is after the AP is provisioned with the LSC certificate to validate the server certificate.

Cisco APs use the LSC provisioning method to download the vendor device and CA certificate to the AP. These certificates help authenticate the Cisco AP to use the switch port with EAP-TLS or PEAP protocol for data traffic.

The deployment occurs in two stages.

First, the Cisco APs are configured with 802.1X credentials, EAP method, and the LSC from the controller. In the second stage, the AP 802.1X enabled switch port passes the 802.1X authentication process to join the controller and begin serving data traffic.

Note Each time the dot1x user or the EAP method is changed the AP will restart the authentication process.

Starting in Release 8.6, the AP wired 802.1X supplicant is supported in Cisco Wave 2 APs for EAP-FAST. Starting in Release 8.7, all Cisco Wave 2 APs support wired 802.1X in EAP-FAST, PEAP, and EAP-TLS. Cisco Wave 1 (IOS-based) APs support 802.1X only in EAP-FAST.

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 25: 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 Wired 802.1X Authentication for Access Points

Procedure

Step 1 If the AP is new, do the following:

a) Boot the AP with the installed lightweight AP image.

b) If you choose not to follow this suggested flow and instead enable 802.1X authentication on the switch port connected to the AP prior to the AP joining the controller, enter this command:

capwap 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 AP 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 AP to the switch port.

Note
While ISE communicates with AP (acting as supplicant), the password policy criteria needs to be applied to the ISE. As AP 802.1X supplicant follows an authenticator password policy and cannot have a password criteria of their own.

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

- 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.
- Cisco Wave 1 APs supports only EAP-FAST authentication method.
- Trunk ports, dynamic ports, or EtherChannel ports are not supported.
- Certificate revocation checks are not implemented on the AP.
- Limited to only one LSC certificate which can be downloaded or provisioned on the AP.
- Cisco APs in bridge mode or Flex+bridge mode is not supported.
- Network Edge Authentication Topology (NEAT) is not supported.
- Client Information Signaling Protocol (CISP) is not supported.

- Downgrade from Cisco Release 8.7 to earlier version changes the EAP method on the Cisco AP to EAP-FAST (default).
- The EAP method needs to be manually deleted and set to default EAP-FAST method when dot1x credentials are deleted. Enter one of the following commands to set the default method.
  - **config ap 802.1Xuser eap-method delete** {**eap-fast | eap-tls | peap**} *ap-name*—Sets the Cisco AP specific method to static EAP-FAST
  - **config ap 802.1Xuser eap-method delete** {**eap-fast | eap-tls | peap all**}—Sets the global EAP method to static EAP-FAST

Configuring 802.1X Authentication Protocols for All Access Points (GUI)

Procedure

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 From the EAP Method drop down list, choose from the following protocol options:

- EAP-FAST
- EAP-TLS
- PEAP

Step 6 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 7 Click **Save Configuration** to save your changes.

Configuring 802.1X Authentication Protocols for All Access Points (CLI)

Procedure

- Configure the global authentication username and password for all access points 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.

- Configure the 802.1x EAP method for all access points by entering this command

  config ap 802.1Xuser eap-method add {**eap-fast | eap-tls | peap** }**all**

- (Optional) Delete the EAP method explicitly after deleting dot1x credentials. Use the following delete command to set the default (EAP-FAST) method.
  - Set the global EAP method to static EAP-FAST:

    config ap 802.1Xuser eap-method delete {**eap-fast | eap-tls | peap**} **all**

- (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.

- View 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
```

- See the authentication status on the AP by entering this command:

  show authentication interface wired-port status

Configuring 802.1X Authentication Protocols for An Access Point (GUI)

Procedure

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

Step 2 Click the name of the access point for which you want to override the authentication settings.

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

Step 4 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.

Step 5 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.

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.

Step 6 From the EAP Method drop down list, choose from the following protocol options:

- EAP-FAST
- EAP-TLS
- PEAP

Step 7 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 8 Click **Save Configuration** to save your changes.

Configuring 802.1X Authentication Protocols for An Access Point (CLI)

Procedure

- Override the global authentication settings and assign a unique username and password to a specific access point by entering 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. 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.

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.

- Configure the 802.1x EAP method for a specific access point by entering this command:

  config ap 802.1Xuser eap-method add {**eap-fast | eap-tls | peap**} *ap-name*

- (Optional) Delete the EAP method explicitly after deleting dot1x credentials. Use the following delete commands to set the default (EAP-FAST) method.
  - **config ap 802.1Xuser eap-method delete** {**eap-fast | eap-tls | peap**} *ap-name*—Sets the Cisco AP specific method to static EAP-FAST
- Enter the **save config** command to save your changes.
- (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.

- 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."

- See the authentication status on the AP by entering this command:

  show authentication interface wired-port status

Configuring LSC Authentication State (GUI)

Use this procedure to configure the AP to use the LSC certificate when the controller is configured with 802.1x port authentication with a RADIUS server.

Procedure

Step 1 Choose **Security** > **Certificate** > **LSC** to open the **Local Significant Certificates (LSC)** page.

Step 2 Choose the **AP Provisioning** tab to open the **AP Provisioning** page.

Step 3 From the **LSC AP Auth State** drop down list, choose one of the options:

- 802.1x AP port authentication
- APWAP-DTLS
- 802.1x+CAPWAP-DTLS

Step 4 Click **Apply**.

Configuring LSC Authentication State (CLI)

Procedure

- Configure the LSC certificate authentication state by entering this command:
  config certificate lsc ap-auth-state {**capwap_dtls** | **dot1x_port_auth** | **both**}
- View the status of the LSC Certificate by entering this command:

  show certificate lsc summary

Adding AP to an LSC Provisioned Network

When you need to add new Cisco APs to an already active LSC-provisioned network, there are two methods to achieve this with no downtime:

Procedure

- Method One:
  1. Associate the new APs to a VLAN which is linked to the LSC provisioning controller.
  2. Download the LSC certificate and configuration on to the Cisco APs.
  3. Associate these APs to the production VLAN.
- Method Two:
  1. Connect the new APs to a dedicated switch port for provisioning LSC certificate.

2. Download the LSC certificate and configuration on to the Cisco APs.
3. Connect these APs to the production switch port.

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**

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)

Procedure

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)

Procedure

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
```

Retaining Static IP Address of an AP (CLI)

Cisco APs can fall back from static IP mode to DHCP mode when they are not able to associate with a controller. While it is useful to get the APs to fall back to DHCP mode so that they continue to serve clients by getting a new IP address, the APs retain their new IP address until they are rebooted. In a network where the APs are assigned static IP addresses, the DHCP IP addresses prevent the APs from being monitored. To address this issue, you can choose to retain the static IP addresses for APs by disabling the fallback to DHCP option.

Procedure

- Enable or disable static IP address failover for an AP or all APs by entering this command:

  config ap static-ip failover {**enable | disable**} {*ap_name* | **all**}

- View the static IP address that is configured on an AP by entering this command:

  show ap config general *ap_name*

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 controller. When the DHCP lease address is deleted in controller, the access point reloads with the following message:

AP Rebooting: Reset Reason - Admin Reload. This is a common behavior in Cisco Wave 1 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.

When the name of the access point is modified using the **config ap name** *new_name old_name* command, then the new AP name is updated. You can view the new AP name updated in both the **show ap join stats summary all** as well as the **show ap summary** commands.

Note When an AP in a Release 8.0 image tries to join controller, 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 controller 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)

Procedure

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)

Procedure

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*

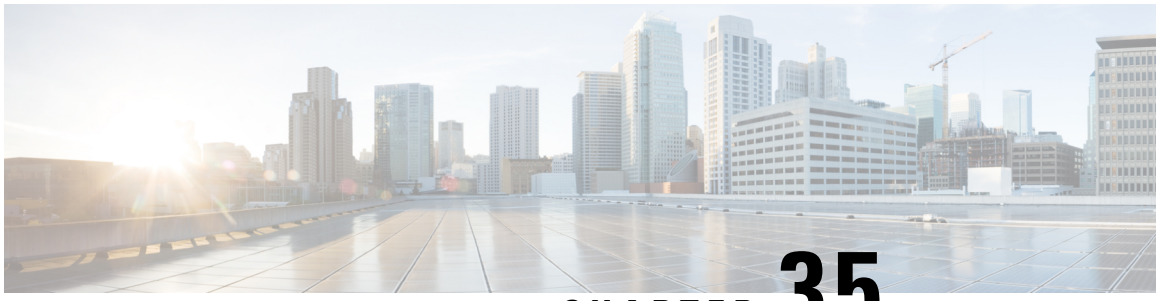
  Information similar to the following appears:

```
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*}



CHAPTER 35

Managing APs

- Access Point Modes, on page 705
- Global Credentials for Access Points, on page 706
- Configuring Telnet and SSH for Access Points, on page 709
- Spectrum Expert Connection, on page 710
- Cisco Universal Small Cell 8x18 Dual-Mode Module, on page 713
- LED States for Access Points, on page 717
- Access Points with Dual-Band Radios, on page 719

Access Point Modes

Each lightweight AP is configured to operate in one of several different AP modes. In some modes, the AP provides network service to clients; in other modes, the AP operates as a dedicated network management tool.

Not all AP models support all AP modes.

Client-Serving AP Modes

- **Local**: This is the default mode. A local mode AP tunnels all client traffic, for all WLANs, in CAPWAP, to the controller. In this mode, the AP's radios are operational only when the AP is connected to its controller. Local mode APs do not support mesh operation. All AP models support Local mode.
- **FlexConnect**: In this mode, client traffic can either be tunneled in CAPWAP to the controller, or egress at the AP's LAN port, depending on the WLAN configuration. FlexConnect mode APs do not support mesh operation. All models support FlexConnect mode.
- **Bridge and Flex+Bridge**: These modes are used in mesh deployments, where wireless rather than wired backhaul is used for CAPWAP connectivity. Not all AP models support these modes; see the relevant mesh documentation for information about support for mesh operation.

Network Management AP Modes

- **Monitor**: In this mode, the AP radios are dedicated to monitoring the Wi-Fi channel for RRM and rogue detection. All AP models support this mode.
- **Rogue Detector**: In this mode, the AP radios are disabled; the AP monitors the LAN to detect on-wire rogue activity. This mode is not supported on Cisco Wave 2 or 802.11ax APs and is deprecated.

- **Sniffer**: In this mode, the AP radio operates in promiscuous mode and captures all Wi-Fi traffic on a channel. These packets are tunneled in CAPWAP to the controller, which forwards them to a machine running OmniPeek or Wireshark for storage and analysis.
- **SE-Connect**: In this mode, the AP provides a dedicated connection to CleanAir for spectrum analysis by software such as Spectrum Expert or Chanalyzer. SE-Connect mode is supported only on SE models with CleanAir.

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 controller cannot be removed.

Configuring Global Credentials for Access Points

Configuring Global Credentials for Access Points (GUI)

Procedure

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)

Procedure

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.”

Configuring Telnet and SSH for Access Points

Configuring Telnet and SSH for APs (GUI)

Procedure

Step 1 Global configuration:

a) Choose **Wireless** > **Access Points** > **Global Configuration**.
b) In the **Global Telnet SSH** area, check or uncheck **Telnet** and **SSH** check boxes.

When you enable Telnet or SSH for all APs, the functionality is allowed on APs that are yet to join the controller regardless of their mode.

c) Click **Apply**.
d) Click **Save Configuration**.

Step 2 Configuration for a specific AP:

a) Choose **Wireless** > **Access Points** > **All APs**.
b) Click an AP name.
c) Click the **Advanced** tab.
d) From the **Telnet** drop-down list, choose **AP Specific** and check the check box to enable the functionality for the AP.
e) From the **SSH** drop-down list, choose **AP Specific** and check the check box to enable the functionality.
f) Click **Apply**.

g) Click **Save Configuration**.

Configuring Telnet and SSH for APs (CLI)

Procedure

- Configure Telnet or SSH for all APs or a specific AP by entering this command:
  config ap {**telnet** | **ssH**} {**enable** | **disable**} {*ap-name* | **all**}
- Replace the Telnet or SSH configuration for a specific AP with the global configuration by entering this command:
  config ap {**telnet** | **ssH**} **default** *ap-name*

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:

Guidelines and Limitations for Spectrum Expert Connection

You may encounter the error message **Unable to contact the remote sensor** while connecting to the Cisco Catalyst 9120 AP. This error message appears due to a difference in the AP architecture compared to the Cisco Wave 2 APs. You can view the 5G data by switching the Spectrum Expert panel to sensord using Slot #0.

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.

Note Starting in Release 8.9, NSI ports can be blocked on APs. Prior to Release 8.9, the NSI ports were always open and it was not possible to block them on APs.

Note Prior to establishing a connection between the Spectrum Expert or Chanalyzer Pro application and the AP, make sure the NSI ports are open on the AP.

Procedure

Step 1 Ensure that Cisco CleanAir functionality is enabled for the access point that will be connected to the Spectrum Expert console.

Step 2 [Optional] Configure the NSI TCP ports (37540 and 37550) on an AP to open or disable them. Or verify the status of these ports before using the Spectrum Expert or Chanalyzer application.

Using the CLI, follow these steps:

a) To globally configure the NSI ports, enter this command:

config ap nsi-ports { **enable** | **disable**} {**all** | *ap_name*}

b) To configure the NSI ports on a specific AP, enter this command:

config ap nsi-ports default *ap_name*

c) To verify the the status of the NSI ports on the AP, enter this command:

show ap config general *ap_name*

Information similar to the following appears:

```
(device) >show ap config general AP5GC.2331A

Cisco AP Identifier.............................. 3430
Cisco AP Name.................................... AP5GC.2331A
Country code..................................... Multiple Countries : IN,J4,US
Regulatory Domain allowed by Country............. 802.11bg:-AJPQU  802.11a:-ABDJ
                    NPQU
AP Country code.................................. J4 - Japan 4(Q)
AP Regulatory Domain............................. 802.11bg:-Q    802.11a:-Q
Switch Port Number .............................. 3
MAC Address...................................... 5c:a1:78:dw:8a:5a
IP Address Configuration......................... Static IP assigned
IP Address....................................... 192.78.144.23
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 192.78.144.1
Domain.......................................
Name Server.....................................
NAT External IP Address.......................... None
CAPWAP Path MTU.................................. 1485
DHCP Release Override............................ Disabled
Telnet State..................................... Globally Enabled
Ssh State........................................ Globally Enabled
```

```
NSI Ports State.............................. Globally Enabled
Virtual IP Address........................... Not Configured
```

Step 3 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 4 On the Windows PC, access the Cisco Software Center from this URL:

http://www.cisco.com/cisco/software/navigator.html

Step 5 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 6 Run the Spectrum Expert application on the PC.

Step 7 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 8 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 9 Use the Spectrum Expert application to view and analyze spectrum data from the access point.

Cisco Universal Small Cell 8x18 Dual-Mode Module

Cisco Universal Small Cell 8x18 Dual-Mode Module is an external module (4G/LTE) that can be plugged into the Cisco Aironet 3600I APs or Cisco Aironet 3700I APs. The following features are available:

- You can configure VLAN tagging for the external module's traffic for the following modes:

Mode	Native VLAN	Non-Native VLAN
FlexConnect Local Switching	Supported	Supported
Local Mode Central Switching	Supported	Supported

- The module can be powered up by the PoE+ power supply
- Co-existence detection and warning when Wi-Fi in 2.4 GHz and 3G/4G module are enabled
- The module's inventory details are available on the controller GUI at **Wireless** > **Access Points** > ***Access Point name*** > **Inventory**.
- Supported on the following Cisco Wireless Controller models:
  - Cisco 3504 Controller
  - Cisco 5520 Controller
  - Cisco 8540 Controller

- Cisco Virtual Controller

- Supported on the following Cisco Access Point models:
  - Cisco Aironet 3700I AP

Restrictions

Cisco Universal Small Cell 8x18 Dual-Mode Modules are not supported on the following Cisco Access Point models:

- Cisco Aironet 3700E AP

For more information about Cisco Universal Small Cell 8x18 Dual-Mode modules, see http://www.cisco.com/c/en/us/support/wireless/universal-small-cell-8000-series/tsd-products-support-series-home.html.

This section contains the following subsections:

Configuring Cisco Universal Small Cell 8x18 Dual-Mode Module

Configuring Cisco Universal Small Cell 8x18 Dual-Mode Module (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs**.

Step 2 Click the AP name.
The **All APs > Details** page is displayed.

Step 3 In the **Advanced** tab, check or uncheck the **External Module Status** check box.

You might be prompted with a co-existence warning when Wi-Fi in 2.4-GHz and 3G/4G module are enabled.

Configuring Cisco Universal Small Cell 8x18 Dual-Mode Module (CLI)

Procedure

- Enable or disable the Cisco USC 8x18 Dual-Mode Module by entering this command:
  config ap module3G {**enable** | **disable**} *ap-name*

  You might be prompted with a co-existence warning when Wi-Fi in 2.4-GHz and 3G/4G module are enabled.

Configuring USC8x18 Dual-Mode Module in Different Scenarios

Configuring VLAN Tagging for USC8x18 Dual-Mode Module in FlexConnect Local Switching (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs**.

Step 2 Click the AP name.
The **All APs > Details** page is displayed.

Step 3 In the **FlexConnect** tab, check 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** box.

Step 4 To enable FlexConnect Local Switching with VLAN ID that is other than 0:

a) Enable **FlexConnect Local Switching** under **External Module**.
b) Enter a value between 2 and 4096 in the **VLAN ID** box.
c) Click **Apply**.

Step 5 To enable FlexConnect local switching with VLAN ID equal to 0:

a) Enable **FlexConnect Local Switching** under **External Module**.
b) Click **Apply**.

Step 6 To remove the FlexConnect local switching per AP configuration, click **Remove AP Specific Config**.

Step 7 Save the configuration.

Configuring VLAN Tagging for USC8x18 Dual-Mode Module in FlexConnect Local Switching (CLI)

Procedure

- **config ap flexconnect module-vlan enable** *ap-name* —Enables FlexConnect local switching for external module with native VLAN
- **config ap flexconnect module-vlan remove** *ap-name*—Removes the AP specific external module VLAN configuration
- **config ap flexconnect module-vlan enable** *ap-name* **vlan** *vlan-id*—Enables FlexConnect local switching with non-native VLAN for the external module
- **show ap module summary** {*ap-name* | **all**}—Displays detailed information about the external module.
- **show ap inventory** {*ap-name* | **all**}—Displays information about the AP's inventory and the external module, if the module is present
- **show ap flexconnect module-vlan** *ap-name*—Displays status of FlexConnect local switching and VLAN ID value
- **show ap config general** *ap-name*—Displays information about the external module info, if the module is present.

Configuring VLAN Tagging for USC8x18 Dual-Mode Module in FlexConnect Group Local Switching (GUI)

Procedure

Step 1 Choose **Wireless** > **FlexConnect Groups**.

Step 2 Click **New**, enter the FlexConnect group name, and click **Apply**.

Step 3 On the **FlexConnect Groups > Edit** page, in the **FlexConnect APs** area, click **Add AP**.

Step 4 You can either select an AP from a list of APs associated with the controller or directly specify the Ethernet MAC address of the AP that is associated with the controller.

Step 5 Click **Add**.

Step 6 To enable FlexConnect Local Switching with VLAN ID:

a) Enable **FlexConnect Local Switching** under **External Module Configuration**.

b) Enter a value between 2 and 4096 in the **VLAN ID** box.

c) Click **Apply**.

Step 7 Save the configuration.

Configuring VLAN Tagging for USC8x18 Dual-Mode Module in FlexConnect Group Local Switching (CLI)

Procedure

- **config flexconnect group** *group-name* **module-vlan enable vlan** *vlan-id*—Enables FlexConnect local switching for the FlexConnect group
- **config flexconnect group** *group-name* **module-vlan disable**—Disables the FlexConnect local switching for the FlexConnect group
- **show flexconnect group detail** *group-name* **module-vlan**—Displays status of the FlexConnect local switching and VLAN ID in the group

Configuring USC8x18 Dual-Mode Module in Local Mode Central Switching (GUI)

Procedure

Step 1 Create a Remote LAN.

For instructions to create a remote LAN, see the *Configuring Remote LANs* chapter under *WLANs*.

Step 2 On the **WLANs > Edit** page, click the **Security** tab.

Step 3 In the **Layer 2** sub-tab, uncheck the **MAC Filtering** check box.

Note
Remote LAN should be configured only with open security. 802.1X security is not supported.

Step 4 To see the current state of the 3G/4G client, choose **Monitor** > **Clients** to open the **Clients** page.

Step 5 Save the configuration.

Configuring USC8x18 Dual-Mode Module in Local Mode Central Switching (CLI)

Procedure

- Create a Remote LAN.

  For instructions to create a remote LAN, see the *Configuring Remote LANs* chapter under *WLANs*.

- **config interface 3g-vlan** *interface-name* {**enable** | **disable**}—Enables or disables the 3G/4G-VLAN interface
- **show interface detailed** *interface-name*—Displays status of the 3G/4G-VLAN flag
- **show client summary ip**—Displays status of the 3G/4G clients

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)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the **Global Configuration** page.

Step 2 Check 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)

Procedure

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 Check 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)

Procedure

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.

Configuring LED Flash State on a Specific Access Point (GUI)

Procedure

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 In the **LED Flash State** section, select one of the following radio buttons:

- Click the LED flash duration for the AP option and enter the duration range from 1 to 3600 seconds.
- Click the **Indefinite** option to configure the LED to flash indefinitely.
- Click the **Disable** option to stop flashing the LED.

Step 4 Click **Apply**.

Access Points with Dual-Band Radios

This section contains the following subsections:

Configuring Access Points with Dual-Band Radios (GUI)

Procedure

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*

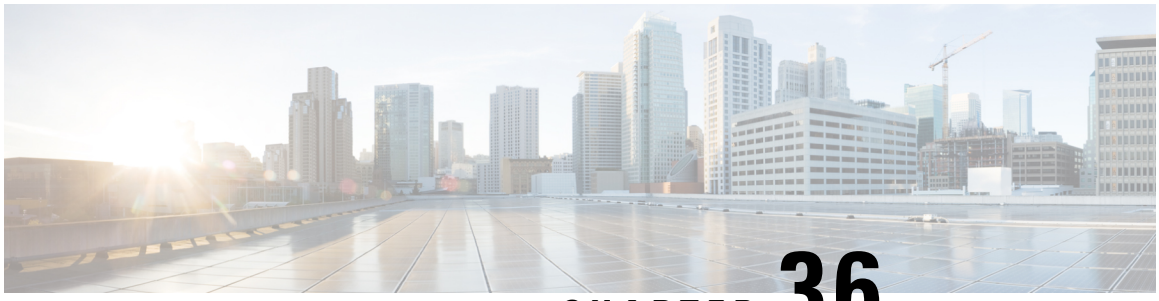
- Configure the dual band Rx-only radio features for an access point with dual-band radios by entering this command:

  config 802.11-rx-abgn {{**cleanair** {**enable** | **disable**}} | **enable** | **disable**} *ap-name*

PART VI

Mesh Access Points

- Connecting Mesh Access Points to the Network, on page 723
- Checking the Health of the Network, on page 795
- Troubleshooting Mesh Access Points, on page 809



CHAPTER 36

Connecting Mesh Access Points to the Network

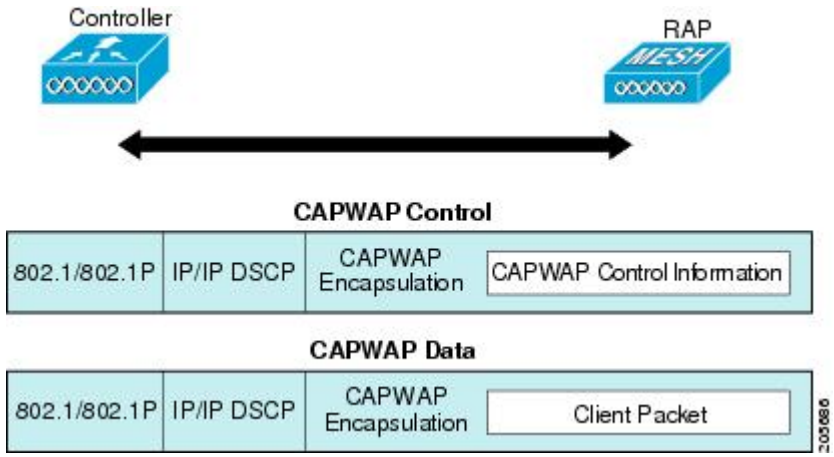
- Overview, on page 723
- Adding Mesh Access Points to the Mesh Network, on page 724
- Mesh PSK Key Provisioning , on page 729
- Configuring Global Mesh Parameters, on page 731
- Backhaul Client Access, on page 733
- Configuring Local Mesh Parameters, on page 735
- Configuring Antenna Gain, on page 739
- Configuring Mesh Leaf Node, on page 740
- Configuring Advanced Features, on page 741
- Information About DHCP on RAP, on page 789
- Information About NAT-PAT on RAP, on page 791
- Configuring Mesh Leaf Node, on page 792

Overview

This chapter describes how to connect the Cisco mesh access points to the network.

The wireless mesh terminates on two points on the wired network. The first location is where the RAP attaches to the wired network, and where all bridged traffic connects to the wired network. The second location is where the CAPWAP controller connects to the wired network; this location is where the WLAN client traffic from the mesh network connects to the wired network. The WLAN client traffic from CAPWAP is tunneled at Layer 2, and matching WLANs should terminate on the same switch VLAN where the controllers are collocated. The security and network configuration for each of the WLANs on the mesh depend on the security capabilities of the network to which the controller is connected.

Figure 24: Mesh Network Traffic Termination



Note When an HSRP configuration is in operation on a mesh network, we recommend that the In-Out multicast mode be configured. For more details on multicast configuration, see the Enabling Multicast on the Network (CLI) section.

For more information about designing and deploying mesh networks, see the relevant mesh deployment guides at

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

For more information about upgrading to a new controller software release, see the *Release Notes for Cisco Wireless Controllers and Lightweight Access Points* at https://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-release-notes-list.html.

For more information about mesh and controller software releases and the compatible access points, see the *Cisco Wireless Solutions Software Compatibility Matrix* at https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html.

Adding Mesh Access Points to the Mesh Network

This section assumes that the controller is already active in the network and is operating in Layer 3 mode.

Note Controller ports that the mesh access points connect to should be untagged.

Before adding a mesh access point to a network, do the following:

Procedure

Step 1 Add the MAC address of the mesh access point to the controller's MAC filter. See the Adding MAC Addresses of Mesh Access Points to MAC Filter section.

Step 2 Define the role (RAP or MAP) for the mesh access point. See the Defining Mesh Access Point Role section.

Step 3 Verify that Layer 3 is configured on the controller. See the Verifying Layer 3 Configuration section.

Step 4 Configure a primary, secondary, and tertiary controller for each mesh access point. See the Configuring Multiple Controllers Using DHCP 43 and DHCP 60 section.

Configure a backup controller. See the Configuring Backup Controllers section.

Step 5 Configure external authentication of MAC addresses using an external RADIUS server. See the Configuring External Authentication and Authorization Using a RADIUS Server.

Step 6 Configure global mesh parameters. See the Configuring Global Mesh Parameters section.

Step 7 Configure backhaul client access. See the Configuring Advanced Features section.

Step 8 Configure local mesh parameters. See the Configuring Local Mesh Parameters section.

Step 9 Configure antenna parameters. See the Configuring Antenna Gain section.

Step 10 Configure channels for serial backhaul. This step is applicable only to serial backhaul access points. See the Backhaul Channel Deselection on Serial Backhaul Access Point section.

Step 11 Configure the DCA channels for the mesh access points. See the Configuring Dynamic Channel Assignment section.

Step 12 Configure mobility groups (if desired) and assign controllers. See the Configuring Mobility Groups chapter in the *Cisco Wireless Controller Configuration Guide*.

Step 13 Configure Ethernet bridging (if desired). See the Configuring Ethernet Bridging section.

Step 14 Configure advanced features such as Ethernet VLAN tagging network, video, and voice. See the Configuring Advanced Features section.

Adding MAC Addresses of Mesh Access Points to MAC Filter

You must enter the radio MAC address for all mesh access points that you want to use in the mesh network into the appropriate controller. A controller only responds to discovery requests from outdoor radios that appear in its authorization list. MAC filtering is enabled by default on the controller, so only the MAC addresses need to be configured. If the access point has an SSC and has been added to the AP Authorization List, then the MAC address of the AP does not need to be added to the MAC Filtering List.

You can add the mesh access point using either the GUI or the CLI.

Note You can also download the list of mesh access point MAC addresses and push them to the controller using Cisco Prime Infrastructure.

Adding the MAC Address of the Mesh Access Point to the Controller Filter List (CLI)

To add a MAC filter entry for the mesh access point on the controller using the controller CLI, follow these steps:

Procedure

Step 1 To add the MAC address of the mesh access point to the controller filter list, enter this command:

config macfilter add *ap_mac wlan_id interface* [*description*]

A value of zero (0) for the *wlan_id* parameter specifies any WLAN, and a value of zero (0) for the *interface* parameter specifies none. You can enter up to 32 characters for the optional *description* parameter.

Step 2 To save your changes, enter this command:

save config

Defining Mesh Access Point Role

By default, AP1500s are shipped with a radio role set to MAP. You must reconfigure a mesh access point to act as a RAP.

Configuring the AP Role (CLI)

To configure the role of a mesh access point using the CLI, enter the following command:

config ap role {**rootAP** | **meshAP**} *Cisco_AP*

Configuring Multiple Controllers Using DHCP 43 and DHCP 60

To configure DHCP Option 43 and 60 for mesh access points in the embedded Cisco IOS DHCP server, follow these steps:

Procedure

Step 1 Enter configuration mode at the Cisco IOS CLI.

Step 2 Create the DHCP pool, including the necessary parameters such as the default router and name server. The commands used to create a DHCP pool are as follows:

```
ip dhcp pool pool name
network IP Network Netmask
default-router Default router
dns-server DNS Server
```

where:

```
pool name is the name of the DHCP pool, such as AP1520
IP Network is the network IP address where the controller resides, such as 10.0.15.1
Netmask is the subnet mask, such as 255.255.255.0
Default router is the IP address of the default router, such as 10.0.0.1
DNS Server is the IP address of the DNS server, such as 10.0.10.2
```

Step 3 Add the option 60 line using the following syntax:

```
option 60 ascii "VCI string"
```

For the VCI string, use one of the values below. The quotation marks must be included.

```
For Cisco 1550 series access points, enter "Cisco AP c1550"
For Cisco 1520 series access points, enter "Cisco AP c1520"
For Cisco 1240 series access points, enter "Cisco AP c1240"
For Cisco 1130 series access points, enter "Cisco AP c1130"
```

Step 4 Add the option 43 line using the following syntax:

```
option 43 hex hex string
```

The hex string is assembled by concatenating the TLV values shown below:

Type + Length + Value

Type is always f1(hex). Length is the number of controller management IP addresses times 4 in hex. Value is the IP address of the controller listed sequentially in hex.

For example, suppose that there are two controllers with management interface IP addresses 10.126.126.2 and 10.127.127.2. The type is f1(hex). The length is 2 * 4 = 8 = 08 (hex). The IP addresses translate to 0a7e7e02 and 0a7f7f02. Assembling the string then yields f1080a7e7e020a7f7f02.

The resulting Cisco IOS command added to the DHCP scope is listed below:

```
option 43 hex f1080a7e7e020a7f7f02
```

Configuring External Authentication and Authorization Using a RADIUS Server

External authorization and authentication of mesh access points using a RADIUS server such as Cisco ACS (4.1 and later) is supported in release 5.2 and later releases. The RADIUS server must support the client authentication type of EAP-FAST with certificates.

Before you employ external authentication within the mesh network, ensure that you make these changes:

- The RADIUS server to be used as an AAA server must be configured on the controller.
- The controller must also be configured on the RADIUS server.
- Add the mesh access point configured for external authorization and authentication to the user list of the RADIUS server.

- For additional details, see the Adding a Username to a RADIUS Server section.

- Configure EAP-FAST on the RADIUS server and install the certificates. EAP-FAST authentication is required if mesh access points are connected to the controller using an 802.11a interface; the external RADIUS servers need to trust Cisco Root CA 2048. For information about installing and trusting the CA certificates, see the Configuring RADIUS Servers section.

Note If mesh access points connect to a controller using a Fast Ethernet or Gigabit Ethernet interface, only MAC authorization is required.

Note This feature also supports local EAP and PSK authentication on the controller.

Configuring RADIUS Servers

To install and trust the CA certificates on the RADIUS server, follow these steps:

Procedure

Step 1 Download the CA certificates for Cisco Root CA 2048 from the following locations:

- https://www.cisco.com/security/pki/certs/crca2048.cer
- https://www.cisco.com/security/pki/certs/cmca.cer

Step 2 Install the certificates as follows:

a) From the CiscoSecure ACS main menu, click **System Configuration** > **ACS Certificate Setup** > **ACS Certification Authority Setup**.
b) In the **CA certificate file** box, type the CA certificate location (path and name). For example: C:\Certs\crca2048.cer.
c) Click **Submit**.

Step 3 Configure the external RADIUS servers to trust the CA certificate as follows:

a) From the CiscoSecure ACS main menu, choose **System Configuration** > **ACS Certificate Setup** > **Edit Certificate Trust List**. The Edit Certificate Trust List appears.
b) Select the check box next to the **Cisco Root CA 2048 (Cisco Systems)** certificate name.
c) Click **Submit**.
d) To restart ACS, choose **System Configuration** > **Service Control**, and then click **Restart**.

For additional configuration details on Cisco ACS servers, see the following:

- http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html(Windows)
- http://www.cisco.com/en/US/products/sw/secursw/ps4911/(UNIX)

Enable External Authentication of Mesh Access Points (CLI)

To enable external authentication for mesh access points using the CLI, enter the following commands:

Procedure

Step 1 **config mesh security eap**
Step 2 **config macfilter mac-delimiter colon**
Step 3 **config mesh security rad-mac-filter enable**
Step 4 **config mesh radius-server** *index* **enable**
Step 5 **config mesh security force-ext-auth enable** (Optional)

View Security Statistics (CLI)

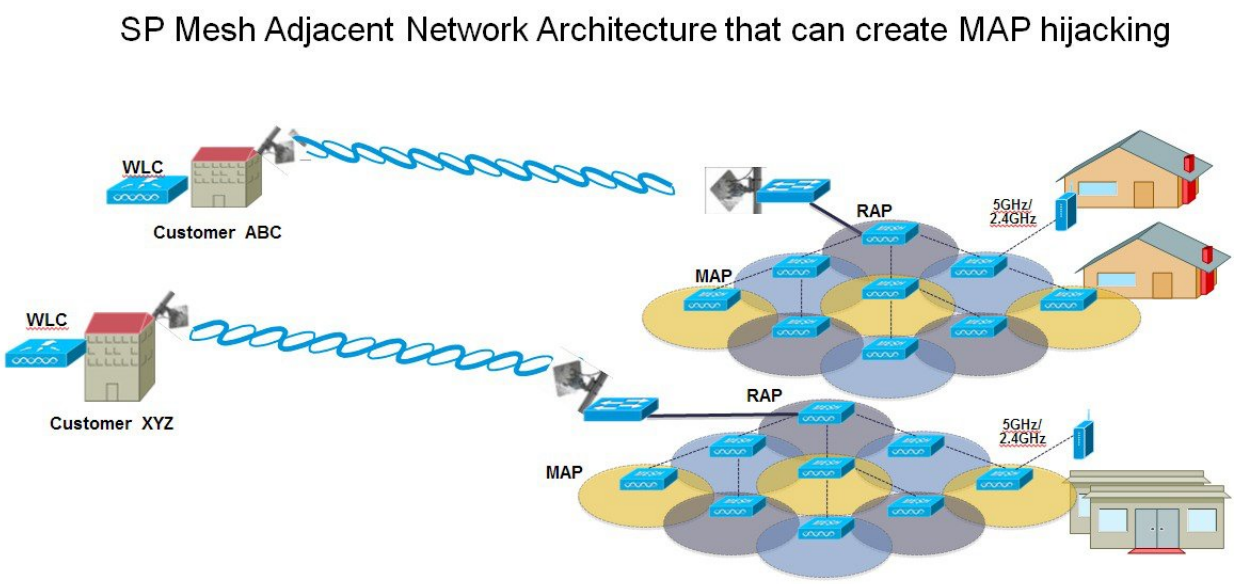
To view security statistics for mesh access points using the CLI, enter the following command:

show mesh security-stats *Cisco_AP*

Use this command to display packet error statistics and a count of failures, timeouts, and association and authentication successes as well as reassociations and reauthentications for the specified access point and its child.

Mesh PSK Key Provisioning

Customers with Cisco Mesh deployment will see their Mesh Access Points (MAP) possibly moving out of their network and joining another Mesh network when both of these Mesh Deployments use AAA with wild card MAC filtering to allow MAPs association. As Mesh APs security may use EAP-FAST this cannot be controlled since for EAP security combination of MAC address and type of AP is used and there is no controlled configuration is available. PSK option with default passphrase also presents security risk and hijack possibility. This issue will be prominently seen in overlapping deployments of two different SPs when the MAPs are used in a moving vehicle (public transportations, ferry, ship and so on.). This way, there is no restriction on MAPs to 'stick' to the SPs mesh network and MAPs can be hijacked / getting used by another SPs network / and cannot serve intended customers of SPs in a deployment.



The new feature introduced in 8.2 release will enable a provision-able PSK functionality from controller which will help make a controlled mesh deployment and enhance MAPs security beyond default **'cisco'** PSK used today. With this new feature the MAPs which are configured with a custom PSK, will use this key to do their authentication with their RAPs and controller. A special precaution should be taken when upgrading from Controller Software release 8.1 and below or downgrading from release 8.2. Admin needs to understand the implications when MAP software is moving in and out of PSK support.

If a mesh PSK mismatch occurs, we recommend that you do any one of the following three tasks to address the issue:

1. Delete the PSK key from the MAP as follows:
   a. With MAP in connected state, move the MAP to EAP.
   b. On the controller UI, navigate to the Mesh tab and delete the PSK key for the MAP.
2. Have a wired connection between MAP and the controller and then clear the configuration on the MAP.
3. Clear the configuration from the MAP console.

CLI Commands for PSK Provisioning

- **config mesh security psk provisioning** {**enable** | **disable**}
- **config mesh security psk provisioning key** *pre-shared-key*
- **config mesh security psk provision window** {**enable** | **disable**}
- **config mesh security psk provisioning delete_psk** {**ap** *ap-name* |**wlc** *psk_index*}

Configuring Global Mesh Parameters

This section provides instructions to configure the mesh access point to establish a connection with the controller including:

- Setting the maximum range between RAP and MAP (not applicable to indoor MAPs).
- Enabling a backhaul to carry client traffic.
- Defining if VLAN tags are forwarded or not.
- Defining the authentication mode (EAP or PSK) and method (local or external) for mesh access points including security settings (local and external authentication).

You can configure the necessary mesh parameters using either the GUI or the CLI. All parameters are applied globally.

Configuring Global Mesh Parameters (CLI)

To configure global mesh parameters including authentication methods using the controller CLI, follow these steps:

Note See the Configuring Global Mesh Parameters (GUI) section for descriptions, valid ranges, and default values of the parameters used in the CLI commands.

Procedure

Step 1 To specify the maximum range (in feet) of all mesh access points in the network, enter this command:

config mesh range *feet*

To see the current range, enter the **show mesh range** command.

Step 2 To enable or disable IDS reports for all traffic on the backhaul, enter this command:

config mesh ids-state {**enable** | **disable**}

Step 3 To specify the rate (in Mbps) at which data is shared between access points on the backhaul interface, enter this command:

config ap bhrate {*rate* | **auto**} *Cisco_AP*

Step 4 To enable or disable client association on the primary backhaul (802.11a) of a mesh access point, enter these commands:

config mesh client-access {**enable** | **disable**}

config ap wlan {**enable** | **disable**} **802.11a** *Cisco_AP*

config ap wlan {**add** | **delete**} **802.11a** *wlan_id Cisco_AP*

Step 5 To enable or disable VLAN transparent, enter this command:

config mesh ethernet-bridging VLAN-transparent {**enable** | **disable**}

Step 6 To define a security mode for the mesh access point, enter one of the following commands:

a) To provide local authentication of the mesh access point by the controller, enter this command:

config mesh security {**eap** | **psk**}

b) To store the MAC address filter in an external RADIUS server for authentication instead of the controller (local), enter these commands:

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server *index* **enable**

c) To provide external authentication on a RADIUS server and define a local MAC filter on the controller, enter these commands:

config mesh security eap

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server *index* **enable**

config mesh security force-ext-auth enable

d) To provide external authentication on a RADIUS server using a MAC username (such as c1520-123456) on the RADIUS server, enter these commands:

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server *index* **enable**

config mesh security force-ext-auth enable

Step 7 To save your changes, enter this command:

save config

Viewing Global Mesh Parameter Settings (CLI)

Use these commands to obtain information on global mesh settings:

- **show mesh client-access**—When Backhaul Client Access is enabled, it allows wireless client association over the backhaul radio. Generally, backhaul radio is a 5-GHz radio for most of the mesh access points. This means that a backhaul radio can carry both backhaul traffic and client traffic.

  When Backhaul Client Access is disabled, only backhaul traffic is sent over the backhaul radio and client association is only over the second radio(s).

```
(Cisco Controller)> show mesh client-access
Backhaul with client access status: enabled
```

- **show mesh ids-state**—Shows the status of the IDS reports on the backhaul as either enabled or disabled.

```
(Cisco Controller)> show mesh ids-state
Outdoor Mesh IDS(Rogue/Signature Detect): .... Disabled
```

- **show mesh config**—Displays global configuration settings.

```
(Cisco Controller)> show mesh config
Mesh Range..................................... 12000
Mesh Statistics update period.................. 3 minutes
Backhaul with client access status............. disabled
Background Scanning State...................... enabled
Backhaul Amsdu State........................... disabled

Mesh Security
Security Mode.................................. EAP
External-Auth.................................. disabled
Use MAC Filter in External AAA server......... disabled
Force External Authentication.................. disabled

Mesh Alarm Criteria
Max Hop Count.................................. 4
Recommended Max Children for MAP............... 10
Recommended Max Children for RAP............... 20
Low Link SNR................................... 12
High Link SNR.................................. 60
Max Association Number......................... 10
Association Interval........................... 60 minutes
Parent Change Numbers.......................... 3
Parent Change Interval......................... 60 minutes

Mesh Multicast Mode............................ In-Out
Mesh Full Sector DFS........................... enabled

Mesh Ethernet Bridging VLAN Transparent Mode..... enabled
```

Backhaul Client Access

When Backhaul Client Access is enabled, it allows wireless client association over the backhaul radio. The backhaul radio is a 5-GHz radio. This means that a backhaul radio can carry both backhaul traffic and client traffic.

When Backhaul Client Access is disabled, only backhaul traffic is sent over the backhaul radio and client association is only over the second radio(s).

Note Backhaul Client Access is disabled by default. After this feature is enabled, all mesh access points, except subordinate AP and its child APs in Daisy-chained deployment, reboot.

This feature is applicable to mesh access points with two radios (1552, 1532, 1540, 1560, 1572, and Indoor APs in Bridge mode).

Configuring Backhaul Client Access (GUI)

Procedure

Step 1 Choose **Wireless** > **Mesh** to navigate to the **Mesh** page.

Step 2 In the **General** section, check the **Backhaul Client Access** check box.

Step 3 Save the configuration.

What to do next

In a Flex+Bridge deployment, after you enable Backhaul Client Access globally, for the 5-GHz radios to beacon as expected, you must enable the **Install mapping on radio backhaul** option for the root APs operating in Flex+Bridge mode.

For more information about enabling the **Install mapping on radio backhaul** option, see the "Configuring Flex+Bridge Mode (GUI)" section.

Related Topics

Configuring Flex+Bridge Mode (GUI), on page 1180

Configuring Backhaul Client Access (CLI)

Use the following command to enable Backhaul Client Access:

```
(Cisco Controller)> config mesh client-access enable
```

The following message is displayed:

```
All Mesh APs will be rebooted
Are you sure you want to start? (y/N)
```

What to do next

In a Flex+Bridge deployment, after you enable Backhaul Client Access globally, for the 5-GHz radios to beacon as expected, you must enable the **Install mapping on radio backhaul** option for the root APs operating in Flex+Bridge mode.

For more information about enabling the **Install mapping on radio backhaul** option, see the "Configuring Flex+Bridge Mode (CLI)" section.

Related Topics

Configuring Flex+Bridge Mode (CLI), on page 1180

Configuring Local Mesh Parameters

After configuring global mesh parameters, you must configure the following local mesh parameters for these specific features if in use in your network:

- Backhaul Data Rate.
- Ethernet Bridging.
- Bridge Group Name.
- Workgroup Bridge.
- Power and Channel Setting.
- Antenna Gain Settings.
- Dynamic Channel Assignment.

Configuring Wireless Backhaul Data Rate

Backhaul is used to create only the wireless connection between the access points. The backhaul interface vary between 802.11a/n/ac rates depending upon the access point. The rate selection is important for effective use of the available RF spectrum. The rate can also affect the throughput of client devices, and throughput is an important metric used by industry publications to evaluate vendor devices.

Dynamic Rate Adaptation (DRA) introduces a process to estimate optimal transmission rate for packet transmissions. It is important to select rates correctly. If the rate is too high, packet transmissions fail resulting in communication failure. If the rate is too low, the available channel bandwidth is not used, resulting in inferior products, and the potential for catastrophic network congestion and collapse.

Data rates also affect the RF coverage and network performance. Lower data rates, for example 6 Mbps, can extend farther from the access point than can higher data rates, for example 1300 Mbps. As a result, the data rate affects cell coverage and consequently the number of access points required. Different data rates are achieved by sending a more redundant signal on the wireless link, allowing data to be easily recovered from noise. The number of symbols sent out for a packet at the 1-Mbps data rate is higher than the number of symbols used for the same packet at 11 Mbps. Therefore, sending data at the lower bit rates takes more time than sending the equivalent data at a higher bit rate, resulting in reduced throughput.

In the controller release 5.2, the default data rate for the mesh 5-GHz backhaul is 24 Mbps. It remains the same with 6.0 and 7.0 controller releases.

With the 6.0 controller release, mesh backhaul can be configured for ‘Auto’ data rate. Once configured, the access point picks the highest rate where the next higher rate cannot be used because of conditions not being suitable for that rate and not because of conditions that affect all rates. That is, once configured, each link is free to settle down to the best possible rate for its link quality.

We recommend that you configure the mesh backhaul to Auto.

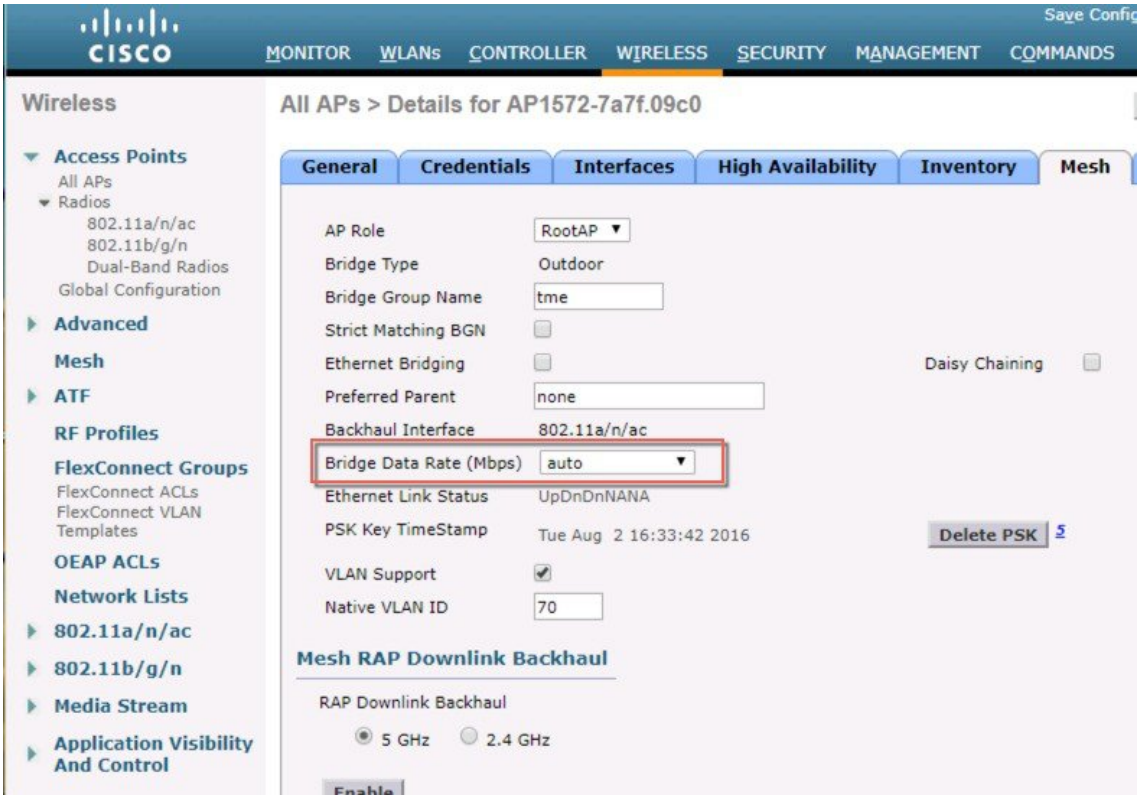
For example, if mesh backhaul chose 48 Mbps, then this decision is taken after ensuring that we cannot use 54 Mbps as there is not enough SNR for 54 and not because some just turned the microwave oven on which affects all rates.

A lower bit rate might allow a greater distance between MAPs, but there are likely to be gaps in the WLAN client coverage, and the capacity of the backhaul network is reduced. An increased bit rate for the backhaul

network either requires more MAPs or results in a reduced SNR between MAPs, limiting mesh reliability and interconnection.

This figure shows the RAP using the "auto" backhaul data rate, and it is currently using 54 Mbps with its child MAP.

Figure 25: Bridge Rate Set to Auto



Note The data rate can be set on the backhaul on a per-AP basis. It is not a global command.

Related Commands

Use these commands to obtain information about backhaul:

Command	Description
config ap bhrate—Configures the Cisco Bridge backhaul Tx rate. The syntax is as follows: `(controller) > config ap bhrate backhaul-rate ap-name`	

Command	Description

Note Preconfigured data rates for each AP (RAP=18 Mbps, MAP1=36 Mbps) are preserved after the upgrade to 6.0 or later software releases.??Before you upgrade to the 6.0 release, if you have the backhaul data rate configured to any data rate, then the configuration is preserved.

The following example shows how to configure a backhaul rate of 36000 Kbps on a RAP:

```
(controller) > config ap bhrate 36000 HPRAP1
```

show ap bhrate—Displays the Cisco Bridge backhaul rate.

The syntax is as follows:

```
(controller) > show ap bhrate ap-name
```

show mesh neigh summary—Displays the link rate summary including the current rate being used in backhaul

Example:

```
(controller) > show mesh neigh summary HPRAP1

AP Name/Radio    Channel     Rate     Link-Snr     Flags      State
---------------- --------   -------   -------     -----      -----
00:0B:85:5C:B9:20 0          auto        4       0x10e8fcb8   BEACON
00:0B:85:5F:FF:60 0          auto        4       0x10e8fcb8   BEACON DEFAULT
00:0B:85:62:1E:00 165        auto        4       0x10e8fcb8   BEACON
OO:0B:85:70:8C:A0 0          auto        1       0x10e8fcb8   BEACON
HPMAP1           165         54          40      0x36         CHILD BEACON
HJMAP2           0          auto         4       0x10e8fcb8   BEACON
```

Backhaul capacity and throughput depends upon the type of the AP, that is, if it is 802.11a/n or only 802.11a, number of backhaul radios it has, and so on.

Configuring Ethernet Bridging

For security reasons, the Ethernet port on all MAPs is disabled by default. It can be enabled only by configuring Ethernet bridging on the root and its respective MAP.

When Ethernet bridging is enabled:

- VLAN ID 0 can be configured as a native VLAN and an access VLAN, but not as non-native VLAN.
- All native VLANs can be configured as a non-native VLANs also and vice-versa.
- Deleting a native VLAN from the allowed VLAN list does not interfere with the native VLAN.
- An old native VLAN will not be automatically added to the allowed VLAN list.

Note Exceptions are allowed for a few protocols even though Ethernet bridging is disabled. For example, the following protocols are allowed:

- Spanning Tree Protocol (STP)
- Address Resolution Protocol (ARP)
- Control and Provisioning of Wireless Access Points (CAPWAP)
- Bootstrap Protocol (BOOTP) packets

Enable Spanning Tree Protocol (STP) on all connected switch ports to avoid Layer 2 looping.

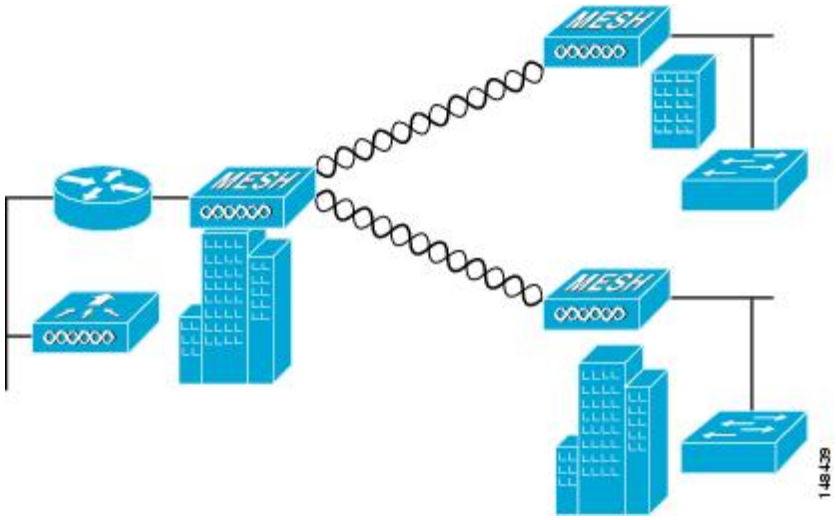
Ethernet bridging has to be enabled for two scenarios:

1. When you want to use the mesh nodes as bridges.

Note You do not need to configure VLAN tagging to use Ethernet bridging for point-to-point and point-to-multipoint bridging deployments.

2. When you want to connect any Ethernet device such as a video camera on the MAP using its Ethernet port. This is the first step to enable VLAN tagging.

Figure 26: Point-to-Multipoint Bridging



Configuring Native VLAN (CLI)

Note Prior to 8.0, the Native VLAN on the wired backhaul was set as VLAN 1. Starting with the 8.0 release, the Native VLAN can be set.

1. Set the Native VLAN on the wired backhaul port using the command **config ap vlan-trunking native *vlan-id ap-name***.

   This applies the Native VLAN configuration to the access point.

Configuring Bridge Group Names

Bridge group names (BGNs) control the association of mesh access points. BGNs can logically group radios to avoid two networks on the same channel from communicating with each other. The setting is also useful if you have more than one RAP in your network in the same sector (area). BGN is a string of 10 characters maximum.

A BGN of *NULL VALUE* is assigned by default by manufacturing. Although not visible to you, it allows a mesh access point to join the network prior to your assignment of your network-specific BGN.

If you have two RAPs in your network in the same sector (for more capacity), we recommend that you configure the two RAPs with the same BGN, but on different channels.

When Strict Match BGN is enabled on the mesh AP, it will scan ten times to find the matched BGN parent. After ten scans, if the AP does not find the parent with matched BGN, it will connect to the non-matched BGN and maintain the connection for 15 minutes. After 15 minutes the AP will again scan ten times and this cycle continues. The default BGN functionalities remain the same when Strict Match BGN is enabled.

Configuring Bridge Group Names (CLI)

Procedure

Step 1 To set a bridge group name (BGN), enter this command:

config ap bridgegroupname set *group-name ap-name*

Note
The mesh access point reboots after a BGN configuration.

Caution
Exercise caution when you configure a BGN on a live network. Always start a BGN assignment from the farthest-most node (last node, bottom of mesh tree) and move up toward the RAP to ensure that no mesh access points are dropped due to mixed BGNs (old and new BGNs) within the same network.

Step 2 To verify the BGN, enter the following command:

show ap config general *ap-name*

Configuring Antenna Gain

You must configure the antenna gain for the mesh access point to match that of the antenna installed using the controller GUI or controller CLI.

Configuring Antenna Gain (CLI)

Enter this command to configure the antenna gain for the 802.11a backhaul radio using the controller CLI:

config 802.11a antenna extAntGain *antenna_gain AP_name*

where gain is entered in 0.5-dBm units (for example, 2.5 dBm =5).

Configuring Mesh Leaf Node

Access points within a mesh network operate in one of the following two ways:

1. Root access point (RAP)
2. Mesh access point (MAP)

While the RAPs have wired connections to their controller, the MAPs have wireless connections to their controller. MAPs communicate among themselves and back to the RAP using wireless connections over the 802.11a/n/g radio backhaul. MAPs use the Cisco Adaptive Wireless Path Protocol (AWPP) to determine the best path through the other mesh access points to the controller.

Relationships among mesh access points are as a parent, child, or neighbor.

- A parent access point offers the best route back to the RAP. A parent can be either the RAP itself or another MAP.
- A child access point selects the parent access point as its best route back to the RAP.
- A neighbor access point is within RF range of another access point but is not selected as its parent or a child.

You can configure the MAP with lower performance to work only as a leaf node. When the mesh network is formed and converged, the leaf node can only work as a child MAP, and cannot be selected by other MAPs as a parent MAP, so that the wireless backhaul performance will not be downgraded.

Note The mesh leaf node feature is supported only for the IR829 AP803 and the IW3700 Series access points.

Use the following command to configure an MAP as a leaf node:

```
(Cisco Controller) >config mesh block-child <ap_name> {enable|disable}

enable         Enable blocking child for an MAP
disable        Disable blocking child for an MAP
```

Use the following commands to display the details of the leaf node configuration:

```
(Cisco Controller) >show mesh block-child {summary|<ap_name>}
```

Examples

```
(Cisco Controller) >show mesh block-child summary

AP Name       AP Model            BVI MAC Hop  Bridge Group Name  Block Child Set
```

```
----------  ------------------  -----------------  ---  -----------------  -------------
AP3         AIR-CAP3602I-C-K9    4c:00:82:07:64:6b  1    mesh               True

Number of Mesh APs Block Child Set.............................. 1

(Cisco Controller) >show mesh block-child AP3

AP Name         AP Model             BVI MAC Hop  Bridge Group Name  Block Child Set
----------  ------------------  -----------------  ---  -----------------  -------------
AP3         AIR-CAP3602I-C-K9    4c:00:82:07:64:6b  1    mesh               True
```

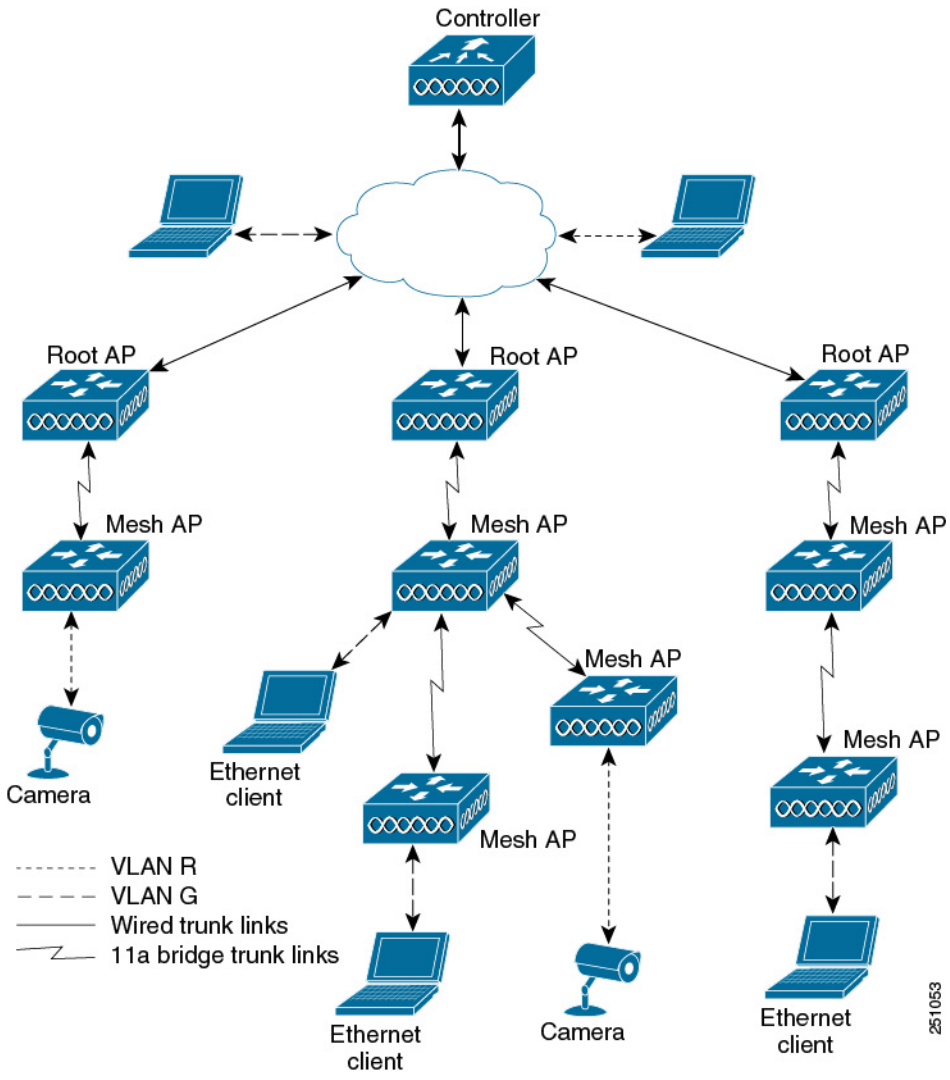
Configuring Advanced Features

Configuring Ethernet VLAN Tagging

Ethernet VLAN tagging allows specific application traffic to be segmented within a wireless mesh network and then forwarded (bridged) to a wired LAN (access mode) or bridged to another wireless mesh network (trunk mode).

A typical public safety access application that uses Ethernet VLAN tagging is the placement of video surveillance cameras at various outdoor locations within a city. Each of these video cameras has a wired connection to a MAP. The video of all these cameras is then streamed across the wireless backhaul to a central command station on a wired network.

Figure 27: Ethernet VLAN Tagging



Ethernet Port Notes

Ethernet VLAN tagging allows Ethernet ports to be configured as normal, access, or trunk in both indoor and outdoor implementations:

Note When VLAN Transparent is disabled, the default Ethernet port mode is normal. VLAN Transparent must be disabled for VLAN tagging to operate and to allow configuration of Ethernet ports. To disable VLAN Transparent, which is a global parameter, see the Configuring Global Mesh Parameters section.

- Access Mode—In this mode, only untagged packets are accepted. All incoming packets are tagged with user-configured VLANs called access-VLANs.

  Use the access mode for applications in which information is collected from devices connected to the MAP, such as cameras or PCs, and then forwarded to the RAP. The RAP then applies tags and forwards traffic to a switch on the wired network.

- Trunk mode—This mode requires the user to configure a native VLAN and an allowed VLAN list (no defaults). In this mode, both tagged and untagged packets are accepted. Untagged packets are accepted and are tagged with the user-specified native VLAN. Tagged packets are accepted if they are tagged with a VLAN in the allowed VLAN list.

- Use the trunk mode for bridging applications such as forwarding traffic between two MAPs that reside on separate buildings within a campus.

Note The Master AP blocks the ethernet port when it receives any Bridge Protocol Data Unit (BPDU) on any VLAN on it as it works globally (one BPDU is enough to block the port on all VLANs). This method avoids loops, and the MAP's port does not operate until the wired link between switches is down.

In Release 8.10 and later releases, the AP performs a loop detection and drops all VLAN packets and BPDU so that the switch does not block the port itself.

Ethernet VLAN tagging operates on Ethernet ports that are not used as backhauls.

Note In the controller releases prior to 7.2, the Root Access Point (RAP) native VLAN is forwarded out of Mesh Access Point (MAP) Ethernet ports with Mesh Ethernet Bridging and VLAN Transparent enabled.

In the 7.2 and 7.4 releases, the Root Access Point (RAP) native VLAN is not forwarded out of Mesh Access Point (MAP) Ethernet ports with Mesh Ethernet Bridging and VLAN Transparent enabled. This behavior is changed starting 7.6, where the native VLAN is forwarded by the MAP when VLAN transparent is enabled.

This change in behavior increases reliability and minimizes the possibility of forwarding loops on Mesh Backhauls.

VLAN Registration

To support a VLAN on a mesh access point, all the uplink mesh access points must also support the same VLAN to allow segregation of traffic that belongs to different VLANs. The activity by which an mesh access point communicates its requirements for a VLAN and gets response from a parent is known as VLAN registration.

Note VLAN registration occurs automatically. No user intervention is required.

VLAN registration is summarized below:

1. Whenever an Ethernet port on a mesh access point is configured with a VLAN, the port requests its parent to support that VLAN.
2. If the parent is able to support the request, it creates a bridge group for the VLAN and propagates the request to its parent. This propagation continues until the RAP is reached.
3. When the request reaches the RAP, it checks whether it is able to support the VLAN request. If yes, the RAP creates a bridge group and a subinterface on its uplink Ethernet interface to support the VLAN request.
4. If the mesh access point is not able to support the VLAN request by its child, at any point, the mesh access point replies with a negative response. This response is propagated to downstream mesh access points until the mesh access point that requested the VLAN is reached.
5. Upon receiving negative response from its parent, the requesting mesh access point defers the configuration of the VLAN. However, the configuration is stored for future attempts. Given the dynamic nature of mesh, another parent and its uplink mesh access points might be able to support it in the case of roaming or a CAPWAP reconnect.

Ethernet VLAN Tagging Guidelines

Follow these guidelines for Ethernet tagging:

- For security reasons, the Ethernet port on a mesh access point (RAP and MAP) is disabled by default. It is enabled by configuring Ethernet bridging on the mesh access point port.
- Ethernet bridging must be enabled on all the mesh access points in the mesh network to allow Ethernet VLAN tagging to operate.
- VLAN mode must be set as non-VLAN transparent (global mesh parameter). See the Configuring Global Mesh Parameters (CLI) section. VLAN transparent is enabled by default. To set as non-VLAN transparent, you must unselect the VLAN transparent option on the Wireless > Mesh page.
- VLAN tagging can only be configured on Ethernet interfaces as follows:
  - On AP1500s, three of the four ports can be used as secondary Ethernet interfaces: port 0-PoE in, port 1-PoE out, and port 3- fiber. Port 2 - cable cannot be configured as a secondary Ethernet interface.
  - In Ethernet VLAN tagging, port 0-PoE in on the RAP is used to connect to the trunk port of the switch of the wired network. Port 1-PoE out on the MAP is used to connect to external devices such as video cameras.
- Backhaul interfaces (802.11a radios) act as primary Ethernet interfaces. Backhauls function as trunks in the network and carry all VLAN traffic between the wireless and wired network. No configuration of primary Ethernet interfaces is required.
- For indoor mesh networks, the VLAN tagging feature functions as it does for outdoor mesh networks. Any access port that is not acting as a backhaul is *secondary* and can be used for VLAN tagging.

- VLAN tagging cannot be implemented on RAPs because the RAPs do not have a secondary Ethernet port, and the primary port is used as a backhaul. However, VLAN tagging can be enabled on MAPs with a single Ethernet port because the Ethernet port on a MAP does not function as a backhaul and is therefore a secondary port.
- No configuration changes are applied to any Ethernet interface acting as a backhaul. A warning displays if you attempt to modify the backhaul's configuration. The configuration is only applied after the interface is no longer acting as a backhaul.
- No configuration is required to support VLAN tagging on any 802.11a backhaul Ethernet interface within the mesh network as follows:
  - This includes the RAP uplink Ethernet port. The required configuration occurs automatically using a registration mechanism.
  - Any configuration changes to an 802.11a Ethernet link acting as a backhaul are ignored and a warning results. When the Ethernet link no longer functions as a backhaul, the modified configuration is applied.
- VLAN configuration is not allowed on port-02-cable modem port of AP1500s (wherever applicable). VLANs can be configured on ports 0 (PoE-in), 1 (PoE-out), and 3 (fiber).
- Up to 16 VLANs are supported on each sector. The cumulative number of VLANs supported by a RAP's children (MAP) cannot exceed 16.
- The switch port connected to the RAP must be a trunk:
  - The trunk port on the switch and the RAP trunk port must match.
  - The RAP must always connect to the native VLAN ID 1 on a switch. The RAP's primary Ethernet interface is by default the native VLAN of 1.
  - The switch port in the wired network that is attached to the RAP (port 0–PoE in) must be configured to accept tagged packets on its trunk port. The RAP forwards all tagged packets received from the mesh network to the wired network.
  - No VLANs, other than those destined for the mesh sector, should be configured on the switch trunk port.
- A configured VLAN on a MAP Ethernet port cannot function as a Management VLAN.
- Configuration is effective only when a mesh access point is in the CAPWAP RUN state and VLAN-Transparent mode is disabled.
- Whenever there roaming or a CAPWAP restart, an attempt is made to apply configuration again.

Configuring Ethernet VLAN Tagging (CLI)

To configure a MAP *access* port, enter this command:

config ap ethernet 1 mode access enable *AP1500-MAP 50*

where *AP1500-MAP* is the variable *AP_name* and *50* is the variable *access_vlan ID*

To configure a RAP or MAP *trunk* port, enter this command:

config ap ethernet 0 mode trunk enable *AP1500-MAP 60*

where *AP1500-MAP* is the variable *AP_name* and *60* is the variable *native_vlan ID*

To add a VLAN to the VLAN allowed list of the native VLAN, enter this command:

config ap ethernet 0 mode trunk add *AP1500-MAP3 65*

where *AP1500-MAP 3* is the variable *AP_name* and *65* is the variable *VLAN ID*

Viewing Ethernet VLAN Tagging Configuration Details (CLI)

Procedure

- To view VLAN configuration details for Ethernet interfaces on a specific mesh access point (*AP Name*) or all mesh access points (*summary*), enter this command:

  show ap config ethernet *ap-name*

- To see if VLAN transparent mode is enabled or disabled, enter this command:

  show mesh config

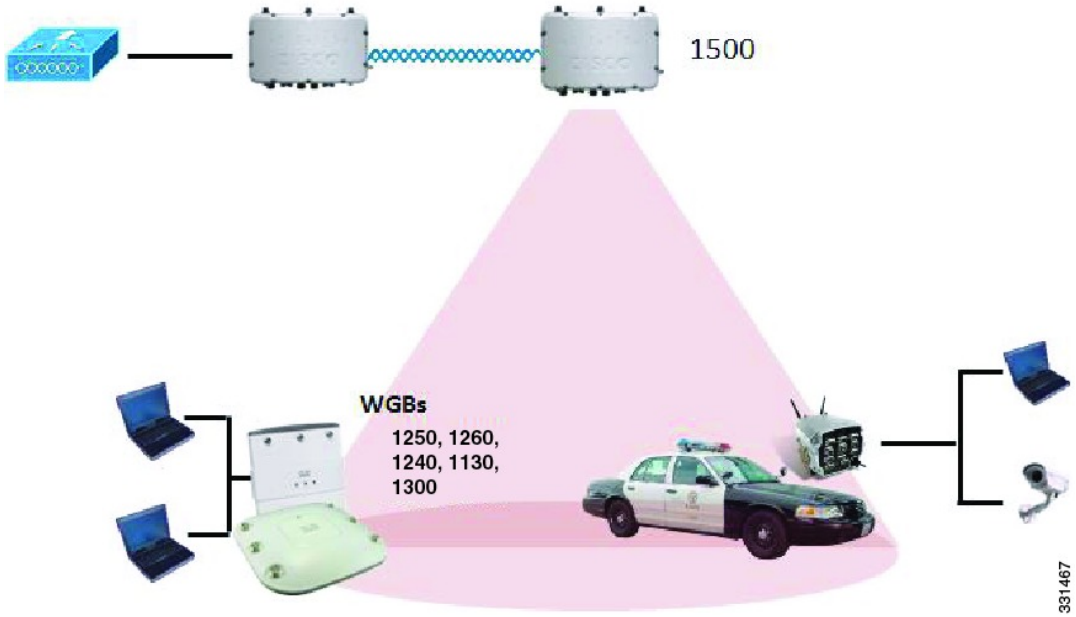
Workgroup Bridge Interoperability with Mesh Infrastructure

A workgroup bridge (WGB) is a small standalone unit that can provide a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter to connect to the wireless network can be connected to the WGB through the Ethernet port. The WGB is associated with the root AP through the wireless interface, which means that wired clients get access to the wireless network.

A WGB is used to connect wired networks over a single wireless segment by informing the mesh access point of all the clients that the WGB has on its wired segment via IAPP messages. The data packets for WGB clients contain an additional MAC address in the 802.11 header (4 MAC headers, versus the normal 3 MAC data headers). The additional MAC in the header is the address of the WGB itself. This additional MAC address is used to route the packet to and from the clients.

WGB association is supported on all radios of every mesh access point.

Figure 28: WGB Example



In the current architecture, while an autonomous AP functions as a workgroup bridge, only one radio interface is used for controller connectivity, Ethernet interface for wired client connectivity, and other radio interface for wireless client connectivity. dot11radio 1 (5 GHz) can be used to connect to a controller (using the mesh infrastructure) and Ethernet interface for wired clients. dot11radio 0 (2.4 GHz) can be used for wireless client connectivity. Depending on the requirement, dot11radio 1 or dot11radio 0 can be used for client association or controller connectivity.

With the 7.0 release, a wireless client on the second radio of the WGB is not dissociated by the WGB upon losing its uplink to a wireless infrastructure or in a roaming scenario.

With two radios, one radio can be used for client access and the other radio can be used for accessing the access points. Having two independent radios performing two independent functions provides you better control and lowers the latency. Also, wireless clients on the second radio for the WGB do not get disassociated by the WGB when an uplink is lost or in a roaming scenario. One radio has to be configured as a Root AP (radio role) and the second radio has to be configured as a WGB (radio role).

Note If one radio is configured as a WGB, then the second radio cannot be a WGB or a repeater.

The following features are not supported for use with a WGB:

- Idle timeout
- Web authentication—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 (web-authentication WLAN is another name for a guest WLAN).
- For wired clients behind the WGB, MAC filtering, link tests, and idle timeout

Configuring Workgroup Bridges

A workgroup bridge (WGB) is used to connect wired networks over a single wireless segment by informing the mesh access point of all the clients that the WGB has on its wired segment via IAPP messages. In addition to the IAPP control messages, the data packets for WGB clients contain an extra MAC address in the 802.11 header (4 MAC headers, versus the normal 3 MAC data headers). The extra MAC in the header is the address of the workgroup bridge itself. This extra MAC address is used to route the packet to and from the clients.

WGB association is supported on both the 2.4-GHz (802.11b/g) and 5-GHz (802.11a) radios on all Cisco APs.

Supported platforms are autonomous 1600, 1700, 2600, 2700, 3600, 3700, 1530, 1550, and 1570, which are configured as WGBs can associate with a mesh access point. See the "Cisco Workgroup Bridges" section in *Cisco Wireless LAN Controller Configuration Guide* for configuration steps at https://www.cisco.com/c/en/us/support/wireless/8500-series-wireless-controllers/products-installation-and-configuration-guides-list.html

The supported WGB modes and capacities are as follows:

- The autonomous access points configured as WGBs must be running Cisco IOS release 12.4.25d-JA or later.

Note If your mesh access point has two radios, you can only configure workgroup bridge mode on one of the radios. We recommend that you disable the second radio. Workgroup bridge mode is not supported on access points with three radios.

- Client mode WGB (BSS) is supported; however, infrastructure WGB is not supported. The client mode WGB is not able to trunk VLAN as in an infrastructure WGB.
- Multicast traffic is not reliably transmitted to WGB because no ACKs are returned by the client. Multicast traffic is unicast to infrastructure WGB, and ACKs are received back.
- If one radio is configured as a WGB in a Cisco IOS access point, then the second radio cannot be a WGB or a repeater.
- Mesh access points can support up to 200 clients including wireless clients, WGB, and wired clients behind the associated WGB.
- A WGB cannot associate with mesh access points if the WLAN is configured with WPA1 (TKIP) +WPA2 (AES), and the corresponding WGB interface is configured with only one of these encryptions (either WPA1 or WPA2):

Figure 29: WPA Security Settings for a WGB

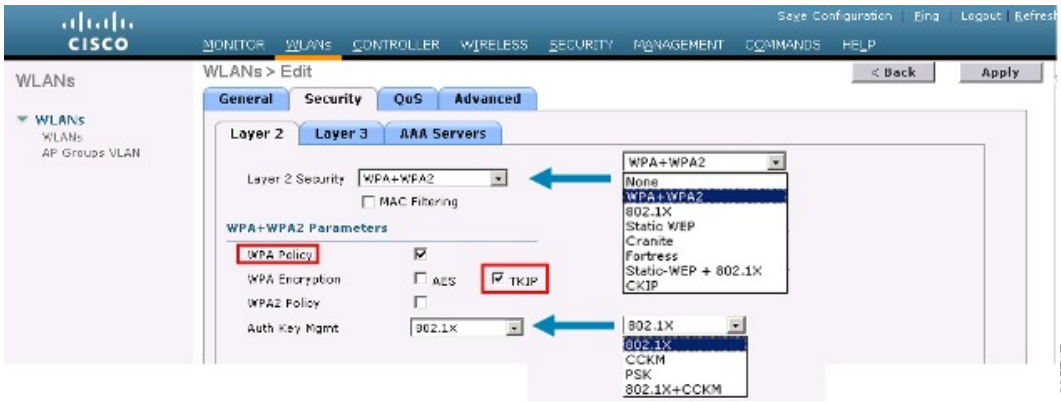
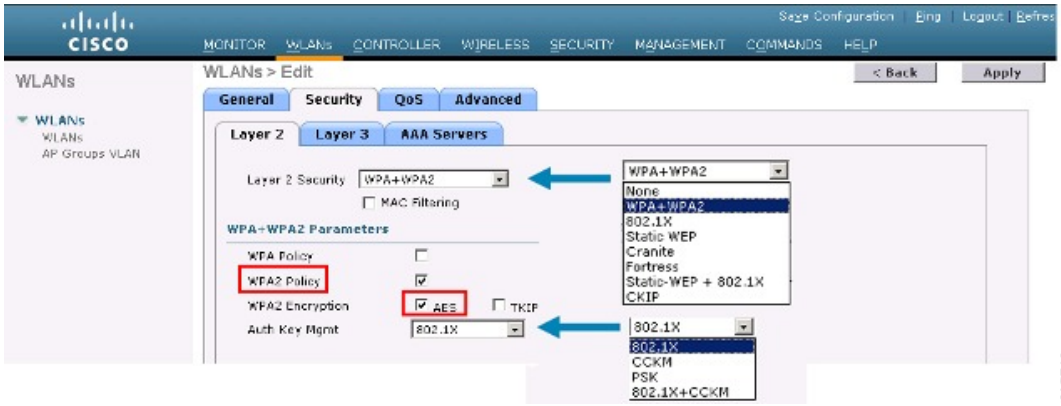


Figure 30: WPA-2 Security Settings for a WGB



To view the status of a WGB client, follow these steps:

Procedure

Step 1 Choose **Monitor** > **Clients**.

Step 2 On the client summary page, click on the MAC address of the client or search for the client using its MAC address.

Step 3 In the page that appears, note that the client type is identified as a *WGB* (far right).

Figure 31: Clients are Identified as a WGB

Step 4 Click on the MAC address of the client to view configuration details:

- For a wireless client, the page seen in **Monitor** > **Clients** > **Detail Page (Wireless WGB Client)** is displayed.
- For a wired client, the page seen in **Monitor** > **Clients** > **Detail Page (Wireless WGB Client)** is displayed.

Figure 32: Monitor > Clients > Detail Page (Wireless WGB Client)

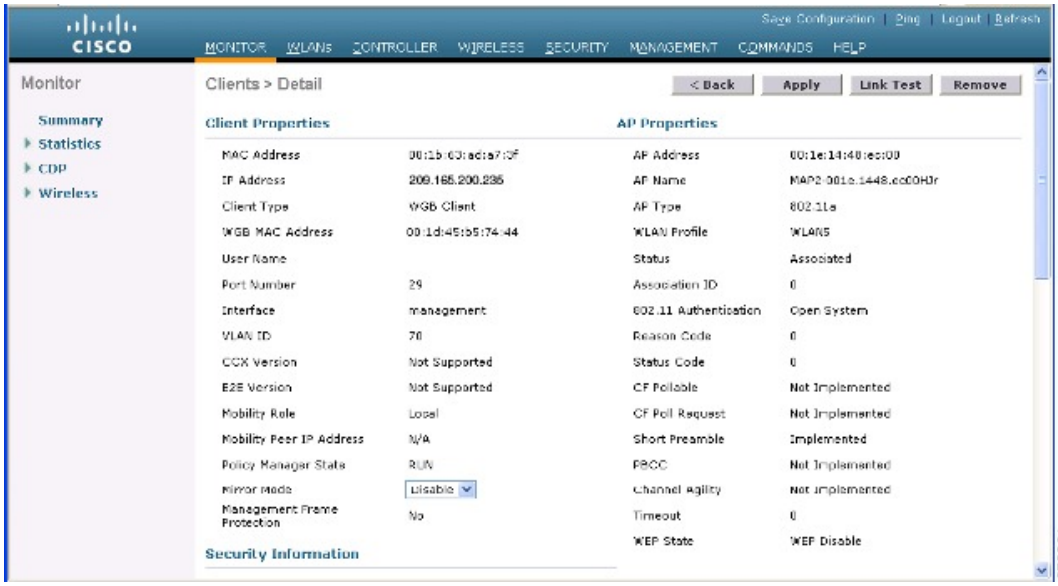
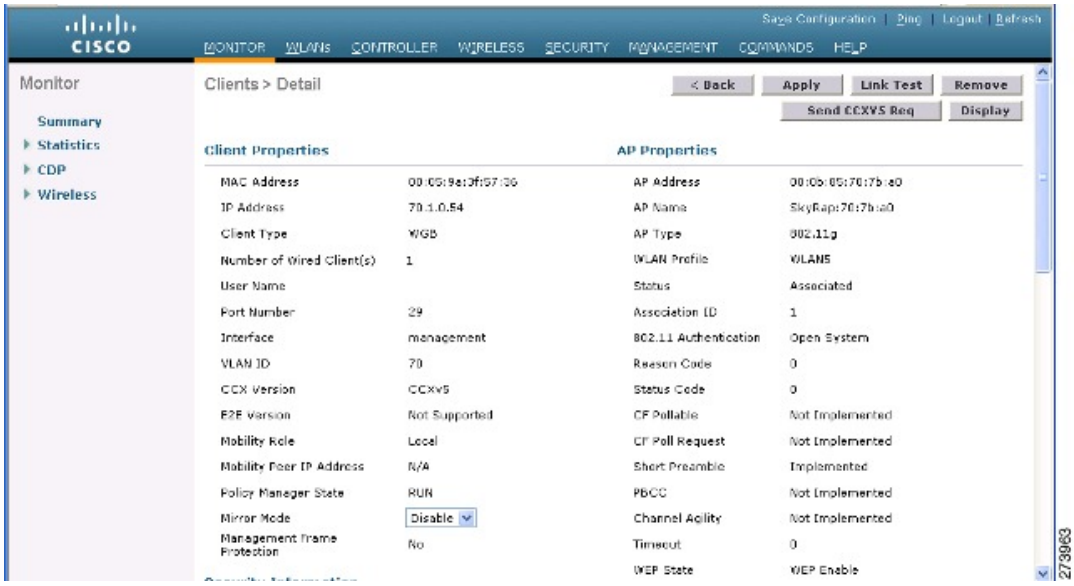


Figure 33: Monitor > Clients > Detail Page (Wired WGB Client)



Guidelines for Configuration

Follow these guidelines when you configure:

- We recommend using a 5-GHz radio for the uplink to Mesh AP infrastructure so you can take advantage of a strong client access on two 5-GHz radios available on mesh access points. A 5-GHz band allows more Effective Isotropic Radiated Power (EIRP) and is less polluted. In a two-radio WGB, configure 5-GHz radio (radio 1) mode as WGB. This radio will be used to access the mesh infrastructure. Configure the second radio 2.4-GHz (radio 0) mode as Root for client access.
- On the Autonomous access points, only one SSID can be assigned to the native VLAN. You cannot have multiple VLANs in one SSID on the autonomous side. SSID to VLAN mapping should be unique because this is the way to segregate traffic on different VLANs. In a unified architecture, multiple VLANs can be assigned to one WLAN (SSID).
- Only one WLAN (SSID) for wireless association of the WGB to the access point infrastructure is supported. This SSID should be configured as an infrastructure SSID and should be mapped to the native VLAN.
- A dynamic interface should be created in the controller for each VLAN configured in the WGB.
- A second radio (2.4-GHz) on the access point should be configured for client access. You have to use the same SSID on both radios and map to the native VLAN. If you create a separate SSID, then it is not possible to map it to a native VLAN, due to the unique VLAN/SSID mapping requirements. If you try to map the SSID to another VLAN, then you do not have multiple VLAN support for wireless clients.
- All Layer 2 security types are supported for the WLANs (SSIDs) for wireless client association in WGB.
- This feature does not depend on the AP platform. On the controller side, both mesh and nonmesh APs are supported.
- There is a limitation of 20 clients in the WGB. The 20-client limitation includes both wired and wireless clients. If the WGB is talking to autonomous access points, then the client limit is very high.

- The controller treats the wireless and wired clients behind a WGB in the same manner. Features such as MAC filtering and link test are not supported for wireless WGB clients from the controller.
- If required, you can run link tests for a WGB wireless client from an autonomous AP.
- Multiple VLANs for wireless clients associated to a WGB are not supported.
- Up to 16 multiple VLANs are supported for wired clients behind a WGB from the 7.0 release and later releases.
- Roaming is supported for wireless and wired clients behind a WGB. The wireless clients on the other radio will not be dissociated by the WGB when an uplink is lost or in a roaming scenario.

We recommend that you configure radio 0 (2.4 GHz) as a Root (one of the mode of operations for Autonomous AP) and radio 1 (5 GHz) as a WGB.

Configuration Example

When you configure from the CLI, the following are mandatory:

- dot11 SSID (security for a WLAN can be decided based on the requirement).
- Map the subinterfaces in both the radios to a single bridge group.

Note A native VLAN is always mapped to bridge group 1 by default. For other VLANs, the bridge group number matches the VLAN number; for example, for VLAN 46, the bridge group is 46.

- Map the SSID to the radio interfaces and define the role of the radio interfaces.

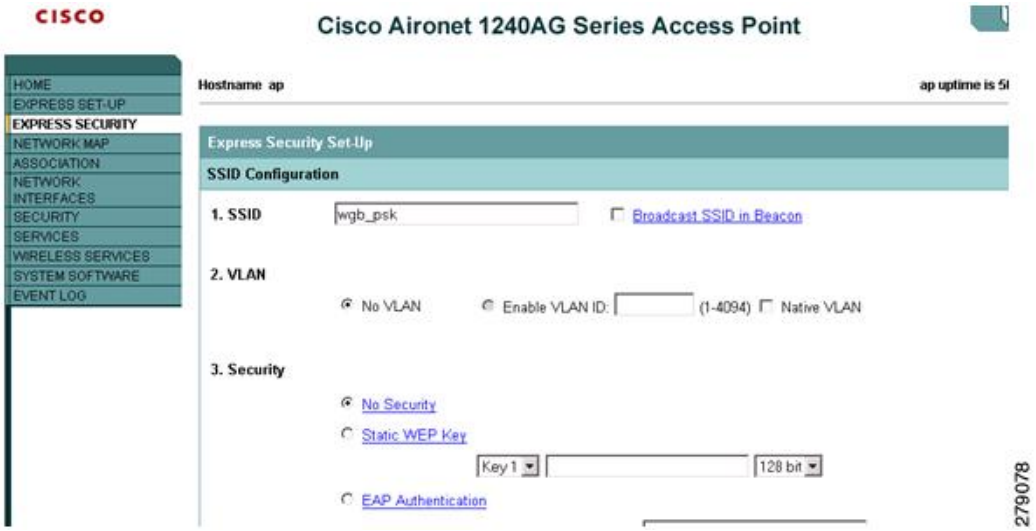
In the following example, one SSID (WGBTEST) is used in both radios, and the SSID is the infrastructure SSID mapped to NATIVE VLAN 51. All radio interfaces are mapped to bridge group -1.

```
WGB1#config t
WGB1(config)#interface Dot11Radio1.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#interface Dot11Radio0.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#dot11 ssid WGBTEST
WGB1(config-ssid)#VLAN 51
WGB1(config-ssid)#authentication open
WGB1(config-ssid)#infrastructiure-ssid
WGB1(config-ssid)#exit
WGB1(config)#interface Dot11Radio1
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role workgroup-bridge
WGB1(config-if)#exit
WGB1(config)#interface Dot11Radio0
```

```
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role root
WGB1(config-if)#exit
```

You can also use the GUI of an autonomous AP for configuration. From the GUI, subinterfaces are automatically created after the VLAN is defined.

Figure 34: SSID Configuration Page



WGB Association Check

Both the WGB association to the controller and the wireless client association to WGB can be verified by entering the **show dot11 associations client** command in autonomous AP.

```
WGB#show dot11 associations client

802.11 Client Stations on Dot11Radio1:

SSID [WGBTEST] :
```

MAC Address	IP Address	Device	Name	Parent	State
0024.130f.920e	209.165.200.225	LWAPP-Parent	RAPSB	-	Assoc

From the controller, choose **Monitor > Clients**. The WGB and the wireless/wired client behind the WGB are updated and the wireless/wired client are shown as the WGB client.

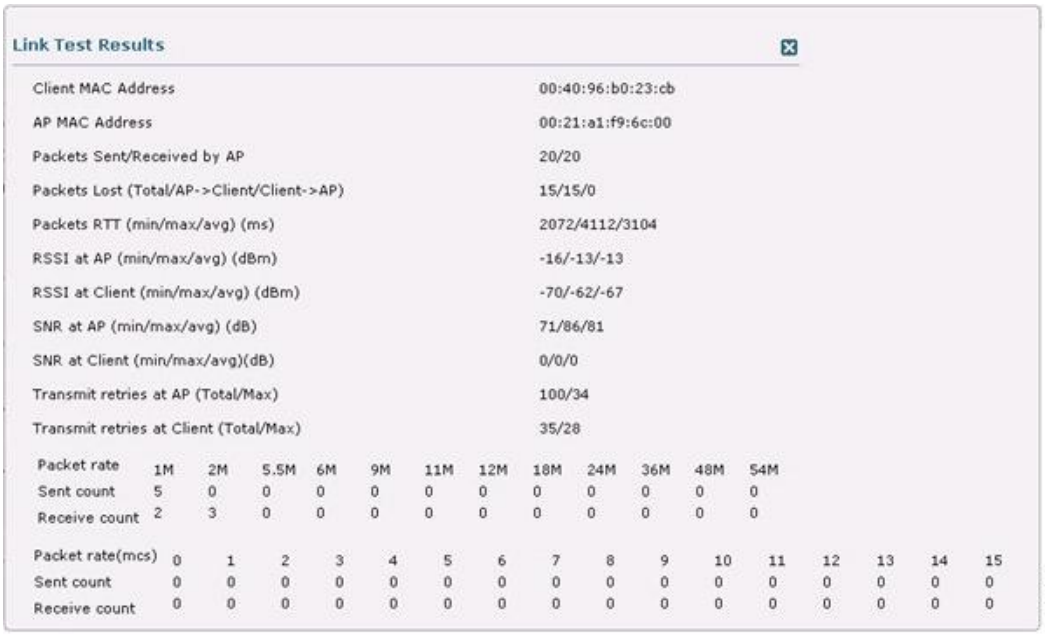
Figure 35: Updated WGB Clients

Figure 36: Updated WGB Clients

Figure 37: Updated WGB Clients

Link Test Result

Figure 38: Link Test Results



A link test can also be run from the controller CLI using the following command:

```
(Cisco Controller) > linktest client mac-address
```

Link tests from the controller are only limited to the WGB, and they cannot be run beyond the WGB from the controller to a wired or wireless client connected to the WGB. You can run link tests for the wireless client connected to the WGB from the WGB itself using the following command:

```
ap#dot11 dot11Radio 0 linktest target client-mac-address
Start linktest to 0040.96b8.d462, 100 512 byte packets
ap#
```

POOR (4% lost)	Time (msec)	Strength (dBm)		SNR Quality		Retries	
		In	Out	In	Out	In	Out
Sent: 100	Avg. 22	-37	-83	48	3	Tot. 34	35
Lost to Tgt: 4	Max. 112	-34	-78	61	10	Max. 10	5
Lost to Src: 4	Min. 0	-40	-87	15	3		

```
Rates (Src/Tgt)     24Mb 0/5  36Mb 25/0  48Mb 73/0  54Mb 2/91
Linktest Done in 24.464 msec
```

WGB Wired/Wireless Client

You can also use the following commands to know the summary of WGBs and clients associated with a Cisco lightweight access point:

```
(Cisco Controller) > show wgb summary
Number of WGBs..................................... 2
```

MAC Address	IP Address	AP Name	Status	WLAN	Auth	Protocol	Clients
00:1d:70:97:bd:e8	209.165.200.225	c1240	Assoc	2	Yes	802.11a	2
00:1e:be:27:5f:e2	209.165.200.226	c1240	Assoc	2	Yes	802.11a	5

```
(Cisco Controller) > show client summary

Number of Clients.................................. 7
```

MAC Address	AP Name	Status	WLAN/Guest-Lan	Auth	Protocol	Port	Wired
00:00:24:ca:a9:b4	R14	Associated	1	Yes	N/A	29	No
00:24:c4:a0:61:3a	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:61:f4	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:61:f8	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:62:0a	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:62:42	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:71:d2	R14	Associated	1	Yes	802.11a	29	No

```
(Cisco Controller) > show wgb detail 00:1e:be:27:5f:e2

Number of wired client(s): 5
```

MAC Address	IP Address	AP Name	Mobility	WLAN	Auth
00:16:c7:5d:b4:8f	Unknown	c1240	Local	2	No
00:21:91:f8:e9:ae	209.165.200.232	c1240	Local	2	Yes

00:21:55:04:07:b5	209.165.200.234	c1240	Local	2	Yes
00:1e:58:31:c7:4a	209.165.200.236	c1240	Local	2	Yes
00:23:04:9a:0b:12	Unknown	c1240	Local	2	No

Client Roaming

High-speed roaming of Cisco Compatible Extension (CX), version 4 (v4) clients is supported at speeds up to 70 miles per hour in outdoor mesh deployments. An example application might be maintaining communication with a terminal in an emergency vehicle as it moves within a mesh public network.

Three Cisco CX v4 Layer 2 client roaming enhancements are supported:

- Access point assisted roaming—Helps clients save scanning time. When a Cisco CX v4 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—Focuses on improving a Cisco CX v4 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.
- Roam reason report—Enables Cisco CX v4 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.

Note Client roaming is enabled by default. For more information, see the Enterprise Mobility Design Guide at http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/eMob4.1.pdf

WGB Roaming Guidelines

Follow these guidelines for WGB roaming:

- Configuring a WGB for roaming—If a WGB is mobile, you can configure it to scan for a better radio connection to a parent access point or bridge. Use the ap(config-if)#**mobile station period 3 threshold 50** command to configure the workgroup bridge as a mobile station.

  When you enable this setting, the WGB scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. Using these criteria, a WGB configured as a mobile station searches for a new parent association and roams to a new parent before it loses its current association. When the mobile station setting is disabled (the default setting), a WGB does not search for a new association until it loses its current association.
- Configuring a WGB for Limited Channel Scanning—In mobile environments such as railroads, a WGB instead of scanning all the channels is restricted to scan only a set of limited channels to reduce the

hand-off delay when the WGB roams from one access point to another. By limiting the number of channels, the WGB scans only those required channels; the mobile WGB achieves and maintains a continuous wireless LAN connection with fast and smooth roaming. This limited channel set is configured using the ap(config-if)#**mobile station scan** *set of channels*.

This command invokes scanning to all or specified channels. There is no limitation on the maximum number of channels that can be configured. The maximum number of channels that can be configured is restricted only by the number of channels that a radio can support. When executed, the WGB scans only this limited channel set. This limited channel feature also affects the known channel list that the WGB receives from the access point to which it is currently associated. Channels are added to the known channel list only if they are also part of the limited channel set.

Configuration Example

The following example shows how to configure a roaming configuration:

```
ap(config)#interface dot11radio 1
ap(config-if)#ssid outside
ap(config-if)#packet retries 16
ap(config-if)#station role workgroup-bridge
ap(config-if)#mobile station
ap(config-if)#mobile station period 3 threshold 50
ap(config-if)#mobile station scan 5745 5765
```

Use the **no mobile station scan** command to restore scanning to all the channels.

Troubleshooting Tips

If a wireless client is not associated with a WGB, use the following steps to troubleshoot the problem:

1. Verify the client configuration and ensure that the client configuration is correct.
2. Check the **show bridge** command output in autonomous AP, and confirm that the AP is reading the client MAC address from the right interface.
3. Confirm that the subinterfaces corresponding to specific VLANs in different interfaces are mapped to the same bridge group.
4. If required, clear the bridge entry using the **clear bridge** command (remember that this command will remove all wired and wireless clients associated in a WGB and make them associate again).
5. Check the **show dot11 association** command output and confirm that the WGB is associated with the controller.
6. Ensure that the WGB has not exceeded its 20-client limitation.

In a normal scenario, if the **show bridge** and **show dot11 association** command outputs are as expected, wireless client association should be successful.

Configuring Voice Parameters in Indoor Mesh Networks

You can configure call admission control (CAC) and QoS on the controller to manage voice and video quality on the mesh network.

The indoor mesh access points are 802.11e capable, and QoS is supported on the local 2.4 and 5-Ghz access radio and the 2.4 and 5 Ghz access radio and the 2.4 and 5 Ghz backhaul radio. CAC is supported on the backhaul and the CCXv4 clients (which provides CAC between the mesh access point and the client)

Note Voice is supported only on indoor mesh networks. Voice is supported on a best-effort basis in the outdoors in a mesh network.

Call Admission Control

Call Admission Control (CAC) enables a mesh access point 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, to maintain QoS under differing network loads, CAC in CCXv4 or later is required.

Note CAC is supported in Cisco Compatible Extensions (CCX) v4 or later. See Chapter 6 of the *Cisco Wireless LAN Controller Configuration Guide* at http://www.cisco.com/en/US/docs/wireless/controller/7.0/configuration/guide/c70sol.html

Two types of CAC are available for access points: static CAC and load-based CAC. All calls on a mesh network are bandwidth-based, so mesh access points use only static CAC.

Static CAC enables the client to specify how much bandwidth or shared medium time is required to accept a new call. Each access point determines whether it is capable of accommodating a particular call by looking at the bandwidth available and compares it against the bandwidth required for the call. If there is not enough bandwidth available to maintain the maximum allowed number of calls with acceptable quality, the mesh access point rejects the call.

Quality of Service and Differentiated Services Code Point Marking

Cisco supports 802.11e on the local access and on the backhaul. Mesh access points prioritize user traffic based on classification, and therefore all user traffic is treated on a best-effort basis.

Resources available to users of the mesh vary, according to the location within the mesh, and a configuration that provides a bandwidth limitation in one point of the network can result in an oversubscription in other parts of the network.

Similarly, limiting clients on their percentage of RF is not suitable for mesh clients. The limiting resource is not the client WLAN, but the resources available on the mesh backhaul.

Similar to wired Ethernet networks, 802.11 WLANs employ Carrier Sense Multiple Access (CSMA), but instead of using collision detection (CD), WLANs use collision avoidance (CA), which means that instead of each station trying to transmit as soon as the medium is free, WLAN devices will use a collision avoidance mechanism to prevent multiple stations from transmitting at the same time.

The collision avoidance mechanism uses two values called CWmin and CWmax. CW stands for contention window. The CW determines what additional amount of time an endpoint should wait, after the interframe space (IFS), to attend to transmit a packet. Enhanced distributed coordination function (EDCF) is a model that allows end devices that have delay-sensitive multimedia traffic to modify their CWmin and CWmax values to allow for statically greater (and more frequent) access to the medium.

Cisco access points support EDCF-like QoS. This provides up to eight queues for QoS.

These queues can be allocated in several different ways, as follows:

- Based on TOS / DiffServ settings of packets
- Based on Layer 2 or Layer 3 access lists
- Based on VLAN
- Based on dynamic registration of devices (IP phones)

AP1500s, with Cisco controllers, provide a minimal integrated services capability at the controller, in which client streams have maximum bandwidth limits, and a more robust differentiated services (diffServ) capability based on the IP DSCP values and QoS WLAN overrides.

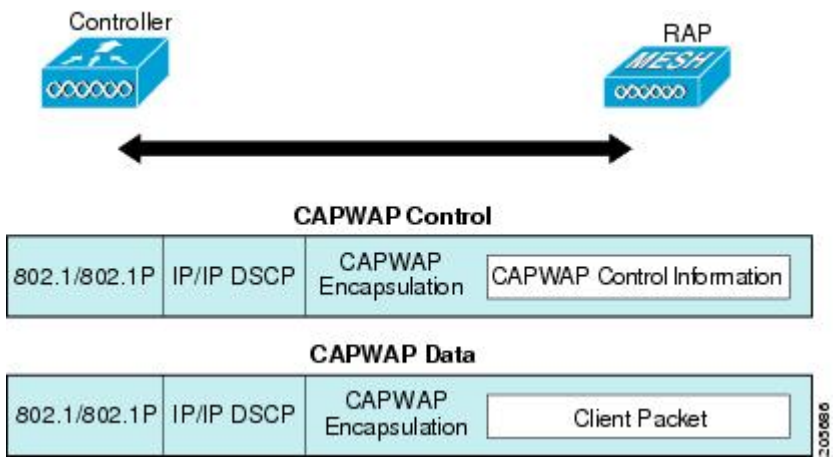
When the queue capacity has been reached, additional frames are dropped (tail drop).

Encapsulations

Several encapsulations are used by the mesh system. These encapsulations include CAPWAP control and data between the controller and RAP, over the mesh backhaul, and between the mesh access point and its client(s). The encapsulation of bridging traffic (noncontroller traffic from a LAN) over the backhaul is the same as the encapsulation of CAPWAP data.

There are two encapsulations between the controller and the RAP. The first is for CAPWAP control, and the second is for CAPWAP data. In the control instance, CAPWAP is used as a container for control information and directives. In the instance of CAPWAP data, the entire packet, including the Ethernet and IP headers, is sent in the CAPWAP container.

Figure 39: Encapsulations

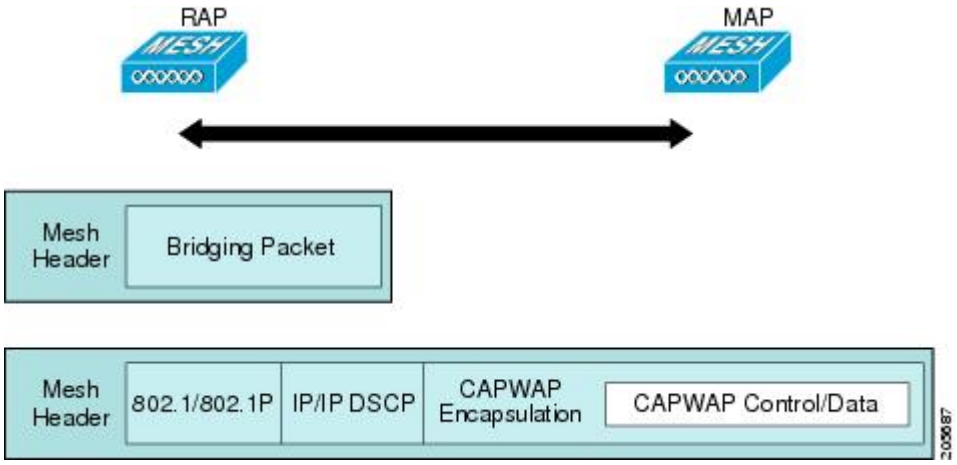


For the backhaul, there is only one type of encapsulation, encapsulating mesh traffic. However, two types of traffic are encapsulated: bridging traffic and CAPWAP control and data traffic. Both types of traffic are encapsulated in a proprietary mesh header.

In the case of bridging traffic, the entire packet Ethernet frame is encapsulated in the mesh header.

All backhaul frames are treated identically, regardless of whether they are MAP to MAP, RAP to MAP, or MAP to RAP.

Figure 40: Encapsulating Mesh Traffic



Note Mesh Data DTLS encryption is only supported on the wave 2 Mesh AP such as 1540 and 1560 models only.

Queuing on the Mesh Access Point

The mesh access point uses a high speed CPU to process ingress frames, Ethernet, and wireless on a first-come, first-serve basis. These frames are queued for transmission to the appropriate output device, either Ethernet or wireless. Egress frames can be destined for either the 802.11 client network, the 802.11 backhaul network, or Ethernet.

AP1500s support four FIFOs for wireless client transmissions. These FIFOs correspond to the 802.11e platinum, gold, silver, and bronze queues, and obey the 802.11e transmission rules for those queues. The FIFOs have a user configurable queue depth.

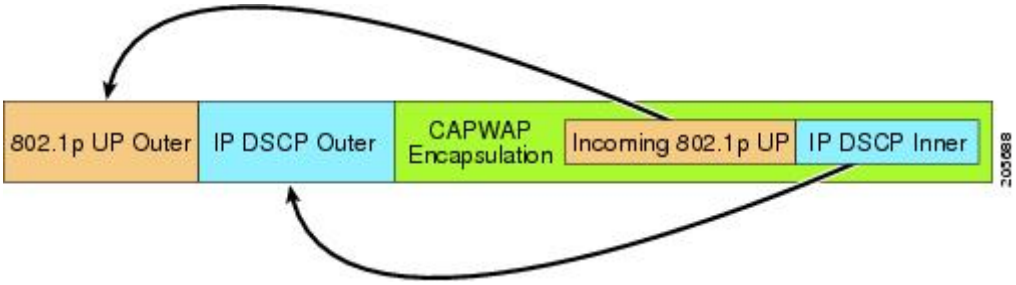
The backhaul (frames destined for another outdoor mesh access point) uses four FIFOs, although user traffic is limited to gold, silver, and bronze. The platinum queue is used exclusively for CAPWAP control traffic and voice, and has been reworked from the standard 802.11e parameters for CWmin, CWmax, and so on, to provide more robust transmission but higher latencies.

The 802.11e parameters for CWmin, CWmax, and so on, for the gold queue have been reworked to provide lower latency at the expense of slightly higher error rate and aggressiveness. The purpose of these changes is to provide a channel that is more conducive to video applications.

Frames that are destined for Ethernet are queued as FIFO, up to the maximum available transmit buffer pool (256 frames). There is support for a Layer 3 IP Differentiated Services Code Point (DSCP), so marking of the packets is there as well.

In the controller to RAP path for the data traffic, the outer DSCP value is set to the DSCP value of the incoming IP frame. If the interface is in tagged mode, the controller sets the 802.1Q VLAN ID and derives the 802.1p UP (outer) from 802.1p UP incoming and the WLAN default priority ceiling. Frames with VLAN ID 0 are not tagged.

Figure 41: Controller to RAP Path



For CAPWAP control traffic the IP DSCP value is set to 46, and the 802.1p user priority is set to 7. Prior to transmission of a wireless frame over the backhaul, regardless of node pairing (RAP/MAP) or direction, the DSCP value in the outer header is used to determine a backhaul priority. The following sections describe the mapping between the four backhaul queues the mesh access point uses and the DSCP values shown in Backhaul Path QoS.

Table 26: Backhaul Path QoS

DSCP Value	Backhaul Queue
2, 4, 6, 8 to 23	Bronze
26, 32 to 63	Gold
46 to 56	Platinum
All others including 0	Silver

Note The platinum backhaul queue is reserved for CAPWAP control traffic, IP control traffic, and voice packets. DHCP, DNS, and ARP requests are also transmitted at the platinum QoS level. The mesh software inspects each frame to determine whether it is a CAPWAP control or IP control frame in order to protect the platinum queue from use by non-CAPWAP applications.

For a MAP to the client path, there are two different procedures, depending on whether the client is a WMM client or a normal client. If the client is a WMM client, the DSCP value in the outer frame is examined, and the 802.11e priority queue is used.

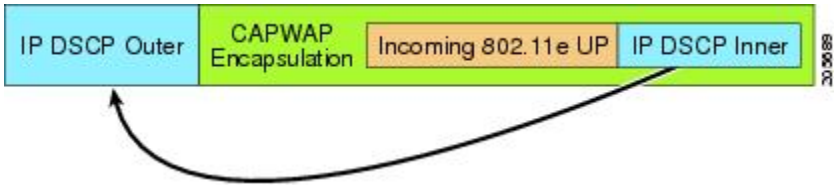
Table 27: MAP to Client Path QoS

DSCP Value	Backhaul Queue
2, 4, 6, 8 to 23	Bronze
26, 32 to 45, 47	Gold
46, 48 to 63	Platinum
All others including 0	Silver

If the client is not a WMM client, the WLAN override (as configured at the controller) determines the 802.11e queue (bronze, gold, platinum, or silver), on which the packet is transmitted.

For a client of a mesh access point, there are modifications made to incoming client frames in preparation for transmission on the mesh backhaul or Ethernet. For WMM clients, a MAP illustrates the way in which the outer DSCP value is set from an incoming WMM client frame.

Figure 42: MAP to RAP Path



The minimum value of the incoming 802.11e user priority and the WLAN override priority is translated using the information listed in Table 28: DSCP to Backhaul Queue Mapping, on page 763 to determine the DSCP value of the IP frame. For example, if the incoming frame has as its value a priority indicating the gold priority, but the WLAN is configured for the silver priority, the minimum priority of silver is used to determine the DSCP value.

Table 28: DSCP to Backhaul Queue Mapping

DSCP Value	802.11e UP	Backhaul Queue	Packet Types
2, 4, 6, 8 to 23	1, 2	Bronze	Lowest priority packets, if any
26, 32 to 34	4, 5	Gold	Video packets
46 to 56	6, 7	Platinum	CAPWAP control, AWPP, DHCP/DNS, ARP packets, voice packets
All others including 0	0, 3	Silver	Best effort, CAPWAP data packets

If there is no incoming WMM priority, the default WLAN priority is used to generate the DSCP value in the outer header. If the frame is an originated CAPWAP control frame, the DSCP value of 46 is placed in the outer header.

With the 5.2 code enhancements, DSCP information is preserved in an AWPP header.

All wired client traffic is restricted to a maximum 802.1p UP value of 5, except DHCP/DNS and ARP packets, which go through the platinum queue.

The non-WMM wireless client traffic gets the default QoS priority of its WLAN. The WMM wireless client traffic may have a maximum 802.11e value of 6, but it must be below the QoS profile configured for its WLAN. If admission control is configured, WMM clients must use TSPEC signaling and get admitted by CAC.

The CAPWAPP data traffic carries wireless client traffic and has the same priority and treatment as wireless client traffic.

Now that the DSCP value is determined, the rules described earlier for the backhaul path from the RAP to the MAP are used to further determine the backhaul queue on which the frame is transmitted. Frames transmitted from the RAP to the controller are not tagged. The outer DSCP values are left intact, as they were first constructed.

Bridging Backhaul Packets

Bridging services are treated a little differently from regular controller-based services. There is no outer DSCP value in bridging packets because they are not CAPWAP encapsulated. Therefore, the DSCP value in the IP header as it was received by the mesh access point is used to index into the table as described in the path from the mesh access point to the mesh access point (backhaul).

Bridging Packets from and to a LAN

Packets received from a station on a LAN are not modified in any way. There is no override value for the LAN priority. Therefore, the LAN must be properly secured in bridging mode. The only protection offered to the mesh backhaul is that non-CAPWAP control frames that map to the platinum queue are demoted to the gold queue.

Packets are transmitted to the LAN precisely as they are received on the Ethernet ingress at entry to the mesh.

The only way to integrate QoS between Ethernet ports on AP1500 and 802.11a is by tagging Ethernet packets with DSCP. AP1500s take the Ethernet packet with DSCP and places it in the appropriate 802.11e queue.

AP1500s do not tag DSCP itself:

- On the ingress port, the AP1500 sees a DSCP tag, encapsulates the Ethernet frame, and applies the corresponding 802.11e priority.
- On the egress port, the AP1500 decapsulates the Ethernet frame, and places it on the wire with an untouched DSCP field.

Ethernet devices, such as video cameras, should have the capability to mark the bits with DSCP value to take advantage of QoS.

Note QoS only is relevant when there is congestion on the network.

Guidelines For Using Voice on the Mesh Network

Follow these guidelines when you use voice on the mesh network:

- Voice is supported only on indoor mesh networks. For outdoors, voice is supported on a best-effort basis on a mesh infrastructure.
- When voice is operating on a mesh network, calls must not traverse more than two hops. Each sector must be configured to require no more than two hops for voice.
- RF considerations for voice networks are as follows:
  - Coverage hole of 2 to 10 percent
  - Cell coverage overlap of 15 to 20 percent
  - Voice needs RSSI and SNR values that are at least 15 dB higher than data requirements
  - RSSI of -67 dBm for all data rates should be the goal for 11b/g/n and 11a/n
  - SNR should be 25 dB for the data rate used by client to connect to the AP
  - Packet error rate (PER) should be configured for a value of one percent or less

- Channel with the lowest utilization (CU) must be used

- On the **802.11a/n/ac** or **802.11b/g/n** > *Global* parameters page, do the following:
  - Enable dynamic target power control (DTPC).
  - Disable all data rates less than 11 Mbps.

- On the **802.11a/n/ac** or **802.11b/g/n** > *Voice* parameters page, do the following:
  - Load-based CAC must be disabled.
  - Enable admission control (ACM) for CCXv4 or v5 clients that have WMM enabled. Otherwise, static CAC does not operate properly.
  - Set the maximum RF bandwidth to 50 percent.
  - Set the reserved roaming bandwidth to 6 percent.
  - Enable traffic stream metrics.

- On the **802.11a/n/ac** or **802.11b/g/n** > *EDCA* parameters page, you should do the following:
  - Set the EDCA profile for the interface as voice optimized.
  - Disable low latency MAC.

- On the **QoS** > *Profile* page, you should do the following:
  - Create a voice profile and select 802.1Q as the wired QoS protocol type.

- On the **WLANs** > *Edit* > *QoS* page, you should do the following:
  - Select a QoS of platinum for voice and gold for video on the backhaul.
  - Select allowed as the WMM policy.

- On the **WLANs** > *Edit* > *QoS* page, you should do the following:
  - Select CCKM for authorization (*auth*) key management (*mgmt*) if you want to support fast roaming.

- On the **x** > *y* page, you should do the following:
  - Disable voice active detection (VAD).

Voice Call Support in a Mesh Network

Table 29: Calls Possible with 1550 Series in 802.11a/n 802.11b/g/n Radios, on page 766 shows the actual calls in a clean, ideal environment.

Table 29: Calls Possible with 1550 Series in 802.11a/n 802.11b/g/n Radios

No. of Calls [4]	802.11a/n Radio 20 MHz	802.11a/n Radio 40 MHz	802.11b/g/n Backhaul Radio 20 MHz	802.11b/g/n Backhaul Radio 40 MHz
RAP	20	35	20	20
MAP1 (First Hop)	10	20	15	20
MAP2 (Second Hop)	8	15	10	15

[4] Traffic was bidirectional 64K voice flows. VoCoder type: G.711, PER <= 1%. Network setup was daisy-chained with no calls traversing more than 2 hops. No external interference.

While making a call, observe the MOS score of the call on the 7921 phone. A MOS score between 3.5 and 4 is acceptable.

Table 30: MOS Ratings

MOS rating	User satisfaction
> 4.3	Very satisfied
4.0	Satisfied
3.6	Some users dissatisfied
3.1	Many users dissatisfied
< 2.58	—

Enabling Mesh Multicast Containment for Video

You can use the controller CLI to configure three mesh multicast modes to manage video camera broadcasts on all mesh access points. When enabled, these modes reduce unnecessary multicast transmissions within the mesh network and conserve backhaul bandwidth.

Mesh multicast modes determine how bridging-enabled access points MAP and RAP send multicasts among Ethernet LANs within a mesh network. Mesh multicast modes manage non-CAPWAP multicast traffic only. CAPWAP multicast traffic is governed by a different mechanism.

The three mesh multicast modes are as follows:

- **Regular mode**—Data is multicast across the entire mesh network and all its segments by bridging-enabled RAP and MAP.
- **In-only mode**—Multicast packets received from the Ethernet by a MAP are forwarded to the RAP's Ethernet network. No additional forwarding occurs, which ensures that non-CAPWAP multicasts received by the RAP are not sent back to the MAP Ethernet networks within the mesh network (their point of origin), and MAP to MAP multicasts do not occur because they are filtered out.

Note When an HSRP configuration is in operation on a mesh network, we recommend the In-Out multicast mode be configured.

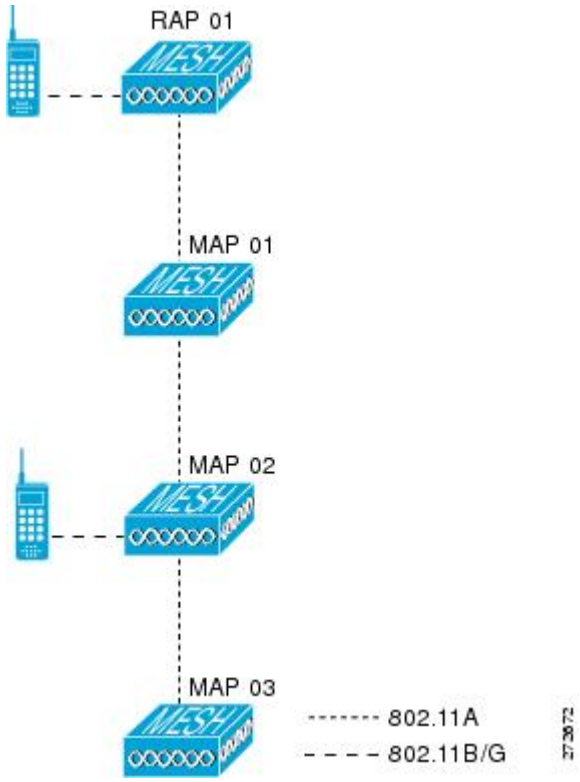
- **In-out mode**—The RAP and MAP both multicast but in a different manner:
  - In-out mode is the default mode.
  - If multicast packets are received at a MAP over Ethernet, they are sent to the RAP; however, they are not sent to other MAP over Ethernet, and the MAP to MAP packets are filtered out of the multicast.
  - If multicast packets are received at a RAP over Ethernet, they are sent to all the MAPs and their respective Ethernet networks. When the in-out mode is in operation, it is important to properly partition your network to ensure that a multicast sent by one RAP is not received by another RAP on the same Ethernet segment and then sent back into the network.

Note If 802.11b clients need to receive CAPWAP multicasts, then multicast must be enabled globally on the controller as well as on the mesh network (using the **config network multicast global enable** CLI command). If multicast does not need to extend to 802.11b clients beyond the mesh network, the global multicast parameter should be disabled (using the **config network multicast global disable** CLI command).

Viewing the Voice Details for Mesh Networks (CLI)

Use the commands in this section to view details on voice and video calls on the mesh network:

Figure 43: Mesh Network Example



- To view the total number of voice calls and the bandwidth used for voice calls on each RAP, enter this command:

  show mesh cac summary

  Information similar to the following appears:

```
AP Name           Slot#   Radio  BW Used/Max  Calls
------------     -------  -----  -----------  -----
SB_RAP1               0   11b/g     0/23437    0
                      1   11a       0/23437    2
SB_MAP1               0   11b/g     0/23437    0
                      1   11a       0/23437    0
SB_MAP2               0   11b/g     0/23437    0
                      1   11a       0/23437    0
SB_MAP3               0   11b/g     0/23437    0
                      1   11a      0/23437    0?
```

- To view the mesh tree topology for the network and the bandwidth utilization (used/maximum available) of voice calls and video links for each mesh access point and radio, enter this command:

  show mesh cac bwused {**voice** | **video**} *AP_name*

  Information similar to the following appears:

```
AP Name        Slot#    Radio      BW Used/Max
-------------- -------  -----      -----------
SB_RAP1          0      11b/g       1016/23437
```

```
                1       11a         3048/23437
|SB_MAP1        0       11b/g       0/23437
                1       11a         3048/23437
||  SB_MAP2     0       11b/g       2032/23437
                1       11a         3048/23437
||| SB_MAP3     0       11b/g       0/23437
                1       11a         0/23437
```

Note The bars (|) to the left of the AP Name field indicate the number of hops that the MAP is from its RAP.

Note When the radio type is the same, the backhaul bandwidth utilization (bw used/max) at each hop is identical. For example, mesh access points *map1*, *map2*, *map3*, and *rap1* are all on the same radio backhaul (802.11a) and are using the same bandwidth (3048). All of the calls are in the same interference domain. A call placed anywhere in that domain affects the others.

- To view the mesh tree topology for the network and display the number of voice calls that are in progress by mesh access point radio, enter this command:

  show mesh cac access *AP_name*

  Information similar to the following appears:

```
AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        0
|   SB_MAP1          0      11b/g      0
                     1      11a        0
||  SB_MAP2          0      11b/g      1
                     1      11a        0
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

Note Each call received by a mesh access point radio causes the appropriate calls summary column to increment by one. For example, if a call is received on the 802.11b/g radio on map2, then a value of one is added to the existing value in that radio's *calls* column. In this case, the new call is the only active call on the 802.11b/g radio of map2. If one call is active when a new call is received, the resulting value is two.

- To view the mesh tree topology for the network and display the voice calls that are in progress, enter this command:

  show mesh cac callpath *AP_name*

  Information similar to the following appears:

```
AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        1
|   SB_MAP1          0      11b/g      0
                     1      11a        1
||  SB_MAP2          0      11b/g      1
                     1      11a        1
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

Note The *calls* column for each mesh access point radio in a call path increments by one. For example, for a call that initiates at map2 (**show mesh cac call path** *SB_MAP2*) and terminates at rap1 by way of map1, one call is added to the map2 802.11b/g and 802.11a radio *calls* column, one call to the map1 802.11a backhaul radio *calls* column, and one call to the rap1 802.11a backhaul radio *calls* column.

- To view the mesh tree topology of the network, the voice calls that are rejected at the mesh access point radio due to insufficient bandwidth, and the corresponding mesh access point radio where the rejection occurred, enter this command:

  show mesh cac rejected *AP_name*

  Information similar to the following appears:

```
AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        0
|   SB_MAP1          0      11b/g      0
                     1      11a        0
||  SB_MAP2          0      11b/g      1
                     1      11a        0
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

Note If a call is rejected at the map2 802.11b/g radio, its *calls* column increments by one.

- To view the number of bronze, silver, gold, platinum, and management queues active on the specified access point, enter this command. The peak and average length of each queue are shown as well as the overflow count.

  show mesh queue-stats *AP_name*

  Information similar to the following appears:

```
Queue Type  Overflows  Peak length  Average length
 ----------  ---------  -----------  --------------
 Silver      0          1            0.000
 Gold        0          4            0.004
```

```
Platinum    0          4            0.001
Bronze      0          0            0.000
Management  0          0            0.000
```

Overflows—The total number of packets dropped due to queue overflow.

Peak Length—The peak number of packets waiting in the queue during the defined statistics time interval.

Average Length—The average number of packets waiting in the queue during the defined statistics time interval.

Enabling Multicast on the Mesh Network (CLI)

Note

- Cisco Aironet 1540 and 1560 Series Outdoor Access Points support in-out mode only.
- Cisco Aironet 1530, 1550, and 1570 Series Outdoor Access Points support all the modes.

Procedure

- To enable multicast mode on the mesh network to receive multicasts from beyond the mesh networks, enter these commands:

  config network multicast global enable

  config mesh multicast {**regular** | **in-only** | **in-out**}

- To enable multicast mode only the mesh network (multicasts do not need to extend to 802.11b clients beyond the mesh network), enter these commands:

  config network multicast global disable

  config mesh multicast {**regular** | **in-only** | **in-out**}

Note Multicast for mesh networks cannot be enabled using the controller GUI.

IGMP Snooping

IGMP snooping delivers improved RF usage through selective multicast forwarding and optimizes packet forwarding in voice and video applications.

A mesh access point transmits multicast packets only if a client is associated with the mesh access point that is subscribed to the multicast group. So, when IGMP snooping is enabled, only that multicast traffic relevant to given hosts is forwarded.

To enable IGMP snooping on the controller, enter the following command:

configure network multicast igmp snooping enable

A client sends an IGMP *join* that travels through the mesh access point to the controller. The controller intercepts the *join* and creates a table entry for the client in the multicast group. The controller then proxies the IGMP *join* through the upstream switch or router.

You can query the status of the IGMP groups on a router by entering the following command:

```
router# show ip gmp groups
IGMP Connected Group Membership

Group Address    Interface   Uptime  Expires    Last Reporter
233.0.0.1        Vlan119     3w1d    00:01:52   10.1.1.130
```

For Layer 3 roaming, an IGMP query is sent to the client's WLAN. The controller modifies the client's response before forwarding and changes the source IP address to the controller's dynamic interface IP address.

The network hears the controller's request for the multicast group and forwards the multicast to the new controller.

For more information about video, see the following:

- *Video Surveillance over Mesh Deployment Guide*: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a0080b02511.shtml
- *Cisco Unified Wireless Network Solution: VideoStream Deployment Guide*: http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080b6e11e.shtml

Locally Significant Certificates for Mesh APs

Until the 7.0 release, mesh APs supported only the Manufactured Installed Certificate (MIC) to authenticate and get authenticated by controllers to join the controller. You might have had to have your own public key infrastructure (PKI) to control CAs, to define policies, to define validity periods, to define restrictions and usages on the certificates that are generated, and get these certificates installed on the APs and controllers. After these customer-generated or locally significant certificates (LSCs) are present on the APs and controllers, the devices start using these LSCs, to join, authenticate, and derive a session key. Cisco supported normal APs from the 5.2 release and later releases and extended the support for mesh APs as well from the 7.0 release.

- Graceful fallback to MIC if APs are unable to join the controller with LSC certificates—Local APs try to join a controller with an LSC for the number of times that are configured on the controller (the default value is 3). After these trials, the AP deletes the LSC and tries to join a controller with an MIC.

  Mesh APs try to join a controller with an LSC until its lonely timer expires and the AP reboots. The lonely timer is set for 40 minutes. After the reboot, the AP tries to join a controller with an MIC. If the AP is again not able to join a controller with an MIC in 40 minutes, the AP reboots and then tries to join a controller with an LSC.

Note An LSC in mesh APs is not deleted. An LSC is deleted in mesh APs only when the LSC is disabled on the controller, which causes the APs to reboot.

- Over the air provisioning of MAPs.

Guidelines for Configuration

Follow these guidelines when using LSCs for mesh APs:

- This feature does not remove any preexisting certificates from an AP. It is possible for an AP to have both LSC and MIC certificates.
- After an AP is provisioned with an LSC, it does not read in its MIC certificate on boot-up. A change from an LSC to an MIC will require the AP to reboot. APs do it for a fallback if they cannot be joined with an LSC.
- Provisioning an LSC on an AP does not require an AP to turn off its radios, which is vital for mesh APs, which may get provisioned over-the-air.
- Because mesh APs need a dot1x authentication, a CA and ID certificate is required to be installed on the server in the controller.
- LSC provisioning can happen over Ethernet and over-the-air in case of MAPs.You have to connect the mesh AP to the controller through Ethernet and get the LSC certificate provisioned. After the LSC becomes the default, an AP can be connected over-the-air to the controller using the LSC certificate.

Differences Between LSCs for Mesh APs and Normal APs

CAPWAP APs use LSC for DTLS setup during a JOIN irrespective of the AP mode. Mesh APs also use the certificate for mesh security, which involves a dot1x authentication with the controller through the parent AP. After the mesh APs are provisioned with an LSC, they need to use the LSC for this purpose because MIC will not be read in.

Mesh APs use a statically configured dot1x profile to authenticate.

This profile is hardcoded to use "cisco" as the certificate issuer. This profile needs to be made configurable so that vendor certificates can be used for mesh authentication (enter the **config local-auth eap-profile cert-issuer vendor "prfMaP1500LlEAuth93"** command).

You must enter the **config mesh lsc enable/disable** command to enable or disable an LSC for mesh APs. This command will cause all the mesh APs to reboot.

Note An LSC on mesh is open for very specific Oil and Gas customers with the 7.0 release. Initially, it is a hidden feature. The **config mesh lsc enable/disable** is a hidden command. Also, the **config local-auth eap-profile cert-issuer vendor "prfMaP1500LlEAuth93"** command is a normal command, but the "prfMaP1500LlEAuth93" profile is a hidden profile, and is not stored on the controller and is lost after the controller reboot.

Certificate Verification Process in LSC AP

LSC-provisioned APs have both LSC and MIC certificates, but the LSC certificate will be the default one. The verification process consists of the following two steps:

1. The controller sends the AP the MIC device certificate, which the AP verifies with the MIC CA.
2. The AP sends the LSC device certificate to the controller, which the controller verifies with the LSC CA.

Getting Certificates for LSC Feature

To configure LSC, you must first gather and install the appropriate certificates on the controller. The following steps show how to accomplish this using Microsoft 2003 Server as the CA server.

To get the certificates for LSC, follow these steps:

Procedure

Step 1 Go to the CA server (http://<ip address of caserver/crtsrv) and login.

Step 2 Get the CA certificate as follows:

a) Click the Download a CA certificate link, certificate chain, or CRF.
b) Choose the encoding method as DER.
c) Click the Download CA certificate link and use the save option to download the CA certificate on to your local machine.

Step 3 To use the certificate on the controller, convert the downloaded certificate to PEM format. You can convert this in a Linux machine using the following command:

openssl x509 -in <input.cer> -inform DER -out <output.cer> -outform PEM

Step 4 Configure the CA certificate on the controller as follows:

a) Choose **COMMANDS > Download File**.
b) Choose the file type as Vendor CA Certificate from the File Type drop-down list.
c) Update the rest of the fields with the information of the TFTP server where the certificate is located.
d) Click **Download**.

Step 5 To install the Device certificate on the controller, login to the CA server as mentioned in Step 1 and do the following:

a) Click the Request a certificate link.
b) Click the advanced certificate request link.
c) Click Create and submit a request to this CA link.
d) Go to the next screen and choose the Server Authentication Certificate from the Certificate Template drop-down list.
e) Enter a valid name, email, company, department, city, state, and country/region. (Remember it in case you want the cap method to check the username against its database of user credentials).

Note
The e-mail is not used.

f) Enable Mark keys as exportable.
g) Click **Submit**.
h) Install the certificate on your laptop.

Step 6 Convert the device certificate obtained in the Step 5. To get the certificate, go to your internet browser options and choose exporting to a file. Follow the options from your browser to do this. You need to remember the password that you set here.

To convert the certificate, use the following command in a Linux machine:

openssl pkcs12 -in <input.pfx> -out <output.cer>

Step 7 On the controller GUI, choose **Command > Download File**. Choose Vendor Device Certificate from the File Type drop-down list. Update the rest of the fields with the information of the TFTP server where the certificate is located and the password you set in the previous step and click **Download**.

Step 8 Reboot the controller so that the certificates can then be used.

Step 9 You can check that the certificates were successfully installed on the controller using this command:

show local-auth certificates

Configuring a Locally Significant Certificate (CLI)

To configure a locally significant certificate (LSC), follow these steps:

Procedure

Step 1 Enable LSC and provision the LSC CA certificate in the controller.

Step 2 Enter the following command:

config local-auth eap-profile cert-issuer vendor *prfMaP1500LlEAuth93*

Step 3 Turn on the feature by entering the following command:

config mesh lsc {**enable** | **disable**}

Step 4 Connect the mesh AP through Ethernet and provision for an LSC certificate.

Step 5 Let the mesh AP get a certificate and join the controller using the LSC certificate.

Figure 44: Local Significant Certificate Page

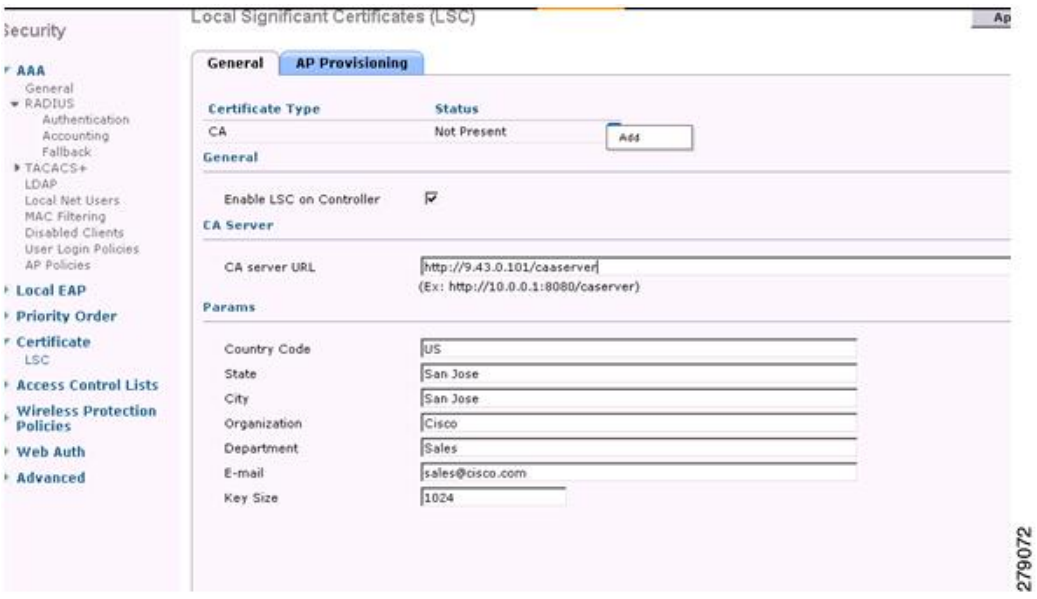


Figure 45: AP Policy Configuration

LSC only MAP Authentication using wild card MAC

Information about LSC-Only MAP Authentication Using Wild Card MAC

The 8.0 release supports LSC only authentication using a wild card MAC address thus disabling the MAC filter. To ensure only authorized access points authenticate, the controller must be able to force the EAP with LSC authentication.

The table shows the different forms of LSC authentication.

Table 31: MAP Authentication Methods

Operation	MAC Filter	LSC Only Authentication
LSC-Only MAP Authentication enabled	disabled	enabled
LSC-Only MAP Authentication disabled	enabled	disabled
Security mode: EAP & PSK	EAP or PSK can be used	Only EAP with LSC should be used
Certificates: MIC & LSC	MIC or LSC can be used	Only EAP with LSC should be used

Controller includes MAC authorization is disabled automatically. EAP security mode provides valid security with LSC. During EAP-FAST, the AP gets authenticated using LSC and gets the MSK key from controller. Any rogue APs are filtered out. Using these keys message handshake happens and the PTK key is generated. The Mesh AP joins the controller using LSC only.

The PSK security mode leads to security threat. As the MSK key is hardcoded inside the code of the mesh AP, any AP even a rogue AP can join the controller. Using these keys, message handshake happens and the

PTK key is generated. The Mesh AP joins the controller using LSC only. Wildcard with PSK must be used only for the debugging purposes.

Configuring LSC-Only Authentication for Mesh Access Points (GUI)

Mesh access points must authenticate before associating with the controller. It is not feasible to enter every AP MAC address into every controller filter list. Service providers have locally significant certificates (LSC), which you can use to bypass MAC authentication and use only LSC.

Procedure

Step 1 Choose **Security** > **Certificate** > **LSC** .

The **Locally Significant Certificates** page is displayed.

Step 2 Select the **AP Provisioning** tab.

Step 3 Select the **Enable LSC on Controller** check box.

Step 4 Select the **General** tab.

Step 5 Select the **Enable** check box in the **AP Provisioning** group.

Step 6 Choose **Wireless** > **Mesh**.

The **Mesh** page is displayed.

Step 7 Select or unselect the **LSC Only MAP Authentication** check box.

Step 8 Click **Apply**.

Step 9 Click **Save Configuration**.

Configuring LSC-Only Authentication for Mesh Access Points (CLI)

Mesh access points must authenticate before associating with the controller. It is not feasible to enter every AP MAC address into every controller filter list. Service providers have locally significant certificates (LSC), which you can use to bypass MAC authentication and use only LSC.

Procedure

- Configure LSC-only authentication for mesh access points by entering this command:
  config mesh security lsc-only-auth {**enable** | **disable**}

LSC-Related Commands

The following commands are related to LSCs:

- **config certificate lsc** {**enable** | **disable**}
  - **enable**—To enable an LSC on the system.
  - **disable**—To disable an LSC on the system. Use this keyword to remove the LSC device certificate and send a message to an AP, to do the same and disable an LSC, so that subsequent joins could be made using the MIC/SSC. The removal of the LSC CA cert on the controller should be done explicitly by using the CLI to accommodate any AP that has not transitioned back to the MIC/SSC.

- **config certificate lsc ca-server url-path** *ip-address*

  Following is the example of the URL when using Microsoft 2003 server:

  http:<ip address of CA>/sertsrv/mscep/mscep.dll

  This command configures the URL to the CA server for getting the certificates. The URL contains either the domain name or the IP address, port number (typically=80), and the CGI-PATH.

  http://ipaddr:port/cgi-path

  Only one CA server is allowed to be configured. The CA server has to be configured to provision an LSC.

- **config certificate lsc ca-server delete**

  This command deletes the CA server configured on the controller.

- **config certificate lsc ca-cert** {**add** | **delete**}

  This command adds or deletes the LSC CA certificate into/from the controller's CA certificate database as follows:

  - **add**—Queries the configured CA server for a CA certificate using the SSCEP getca operation, and gets into the controller and installs it permanently into the controller database. If installed, this CA certificate is used to validate the incoming LSC device certificate from the AP.
  - **delete**—Deletes the LSC CA certificate from the controller database.

- **config certificate lsc subject-params** *Country State City Orgn Dept Email*

  This command configures the parameters for the device certificate that will be created and installed on the controller and the AP.

  All of these strings have 64 bytes, except for the Country that has a maximum of 3 bytes. The Common Name is automatically generated using its Ethernet MAC address. This should be given prior to the creation of the controller device certificate request.

  The above parameters are sent as an LWAPP payload to the AP, so that the AP can use these parameters to generate the certReq. The CN is automatically generated on the AP using the current MIC/SSC "Cxxxx-MacAddr" format, where xxxx is the product number.

- **config certificate lsc other-params** *keysize*

  The default keysize value is 2048 bits.

- **config certificate lsc ap-provision** {**enable** | **disable**}

  This command enables or disables the provisioning of the LSCs on the APs if the APs just joined using the SSC/MIC. If enabled, all APs that join and do not have the LSC will get provisioned.

  If disabled, no more automatic provisioning will be done. This command does not affect the APs, which already have LSCs in them.

- **config certificate lsc ra-cert** {**add** | **delete**}

  We recommend this command when the CA server is a Cisco IOS CA server. The controller can use the RA to encrypt the certificate requests and make communication more secure. RA certificates are not currently supported by other external CA servers, such as MSFT.

- **add**—Queries the configured CA server for an RA certificate using the SCEP operation and installs it into the controller database. This keyword is used to get the certReq signed by the CA.
- **delete**—Deletes the LSC RA certificate from the controller database.

- **config auth-list ap-policy lsc** {**enable** | **disable**}

  After getting the LSC, an AP tries to join the controller. Before the AP tries to join the controller, you must mandatorily enter this command on the controller console. By default, the **config auth-list ap-policy lsc** command is in the disabled state, and the APs are not allowed to join the controller using the LSC.

- **config auth-list ap-policy mic** {**enable** | **disable**}

  After getting the MIC, an AP tries to join the controller. Before the AP tries to join the controller, you must mandatorily enter this command on the controller console. By default, the **config auth-list ap-policy mic** command is in the enabled state. If an AP cannot join because of the enabled state, this log message on the controller side is displayed: LSC/MIC AP is not allowed to join.

- **show certificate lsc summary**

  This command displays the LSC certificates installed on the controller. It would be the CA certificate, device certificate, and optionally, an RA certificate if the RA certificate has also been installed. It also indicates if an LSC is enabled or not.

- **show certificate lsc ap-provision**

  This command displays the status of the provisioning of the AP, whether it is enabled or disabled, and whether a provision list is present or not.

- **show certificate lsc ap-provision details**

  This command displays the list of MAC addresses present in the AP provisioning lists.

Controller GUI Security Settings

Although the settings are not directly related to the feature, it might help you in achieving the desired behavior with respect to APs provisioned with an LSC.

- Case 1—Local MAC Authorization and Local EAP Authentication

  Add the MAC address of RAP/MAP to the controller MAC filter list.

  Example:

```
(Cisco Controller) > config macfilter mac-delimiter colon
(Cisco Controller) > config macfilter add 00:0b:85:60:92:30 0 management
```

- Case 2—External MAC Authorization and Local EAP authentication

  Enter the following command on the controller:

```
(Cisco Controller) > config mesh security rad-mac-filter enable
```

  or

  Check only the external MAC filter authorization on the GUI page and follow these guidelines:

- Do not add the MAC address of the RAP/MAP to the controller MAC filter list.
- Configure the external radius server details on the controller.
- Enter the **config macfilter mac-delimiter colon** command configuration on the controller.
- Add the MAC address of the RAP/MAP in the external radius server in the following format:

  User name: 11:22:33:44:55:66 Password : 11:22:33:44:55:66

- Case 3—LSC Only MAP Authentication

  Enter the following command on the controller:

```
(Cisco Controller) > config mesh security lsc-only-auth enable
```

  or

  Check LSC Only MAP Authentication on the GUI page. This message will be displayed:

```
Warning: Enabling LSC Only MAP Authentication will provision LSC Certificate
 into MAP
(if MAP are being provisioned for first time). Please make sure MAP is connected
 to WLC using Ethernet
cable to avoid security risk.
Are you sure you want to continue? (Y/N)
```

Deployment Guidelines

- When using local authorization, the controller should be installed with the vendor's CA and device certificate.
- When using an external AAA server, the controller should be installed with the vendor’s CA and device certificate.
- Mesh security should be configured to use ‘vendor’ as the cert-issuer.
- MAPs cannot move from an LSC to an MIC when they fall back to a backup controller.

The **config mesh lsc** {**enable** | **disable**} command is required to enable or disable an LSC for mesh APs. This command causes all the mesh APs to reboot.

Configuring Antenna Band Mode

Information About Configuring Antenna Band Modes

You can configure the antenna band modes for mesh access points as either of the following:

- Dual Antenna Band Mode—The bottom two ports, port 1 and port 2, are used for dual band 2.4-GHz and 5-GHz dual radiating element (DRE) antennas.
- Single Antenna Band Mode—The top two ports, port 3 and port 4, are used for 5-GHz single radiating element (SRE) antennas and the bottom two ports, port 1 and port 2, are used for 2.4-GHz SRE antennas.

Restrictions for Configuring Antenna Band Modes

The antenna band mode configuration is available on the Cisco Aironet 1532E and 1572EC/EAC access point models.

Note The Cisco Aironet 1532I access point model has internal antenna and does not require additional antennas.

Configuring Antenna Band Mode (CLI)

Before you begin

Ensure that the physical antennas are correctly configured before changing the antenna band mode. If the antenna band mode is incorrectly configured, the mesh AP could be stranded.

Procedure

- Configure antenna band mode for a mesh AP by entering this command on the controller CLI:
  config ap antenna-band-mode {**single** | **dual**} *mesh-ap-name*
- View the status of the antenna band mode by entering this command:
  show ap config general *mesh-ap-name*

Configuring Antenna Band Mode (AP CLI)

Procedure

- Configure antenna band mode on the mesh AP CLI by entering this command on the AP console:
  capwap ap ant-band-mode {**dual** | **single**}

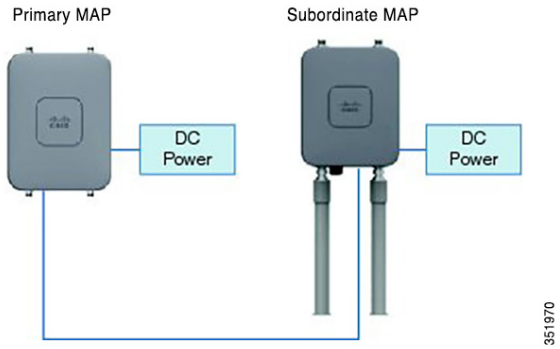
Configuring Daisy Chaining on Cisco Aironet 1530 Series Access Points

Information About Daisy Chaining the Cisco Aironet 1530 Series Access Points

The Cisco Aironet 1530 Series Access Points have the capability to "daisy chain" access points when they function as mesh APs (MAPs). The "daisy chained" MAPs can either operate the access points as a serial backhaul, allowing different channels for uplink and downlink access thus improving backhaul bandwidth, or extend universal access. Extending universal access allows you to connect a local mode or FlexConnect mode Cisco AP1530 to the Ethernet port of a MAP, thus extending the network to provide better client access.

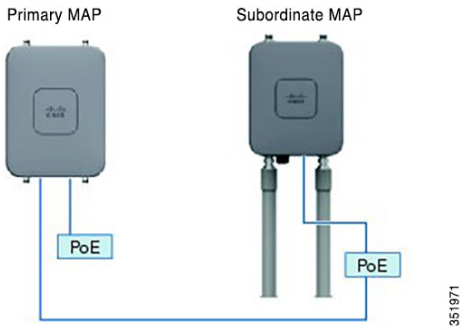
Daisy chained access points must be cabled differently depending on how the APs are powered. If the access point is powered using DC power, an Ethernet cable must be connected directly from the LAN port of the primary AP to the PoE in port of the subordinate AP.

Figure 46: Daisy Chained APs using DC Power



If the access point is powered using PoE, an Ethernet cable must be connected from the LAN port of the primary AP into the PoE Injector, which powers the subordinate AP.

Figure 47: Daisy Chained APs using PoE Injector



Daisy Chaining with the 1572

One of the key features of the 1572 access point (AP) is the ability to “daisy chain” APs while they are operating as Mesh APs (MAPs). By “daisy chaining” MAPs, customers can either operate the APs as a serial backhaul, allowing different channels for uplink and downlink access thus improving backhaul bandwidth, or to extend universal access. Extending universal access allows a customer to connect a local mode or flexconnect mode 1572 AP to the Ethernet port of a MAP, thus extending the network to provide better client access. These features are explained in detail in the following sections.

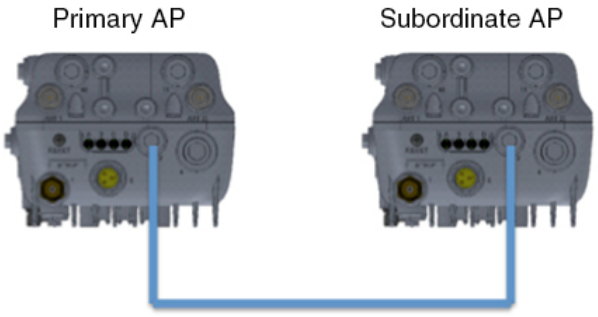
In the 8.0MR release, when the 1572 is configured as a primary AP, the following APs are supported as subordinate APs:

- 1572EAC
- 1572EC
- 1572IC
- 1552
- 1532E/I
- 3700P

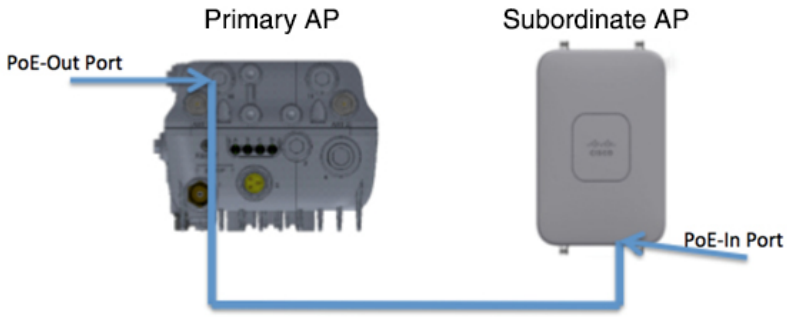
Daisy-chained access points need to be cabled differently depending on the AP type of their terminating subordinate AP.

If both the primary AP and subordinate APs are 1572s, there should be an Ethernet cable from the primary AP's Ethernet port to the subordinate AP's Ethernet port. Daisy chaining should be enabled on both APs.

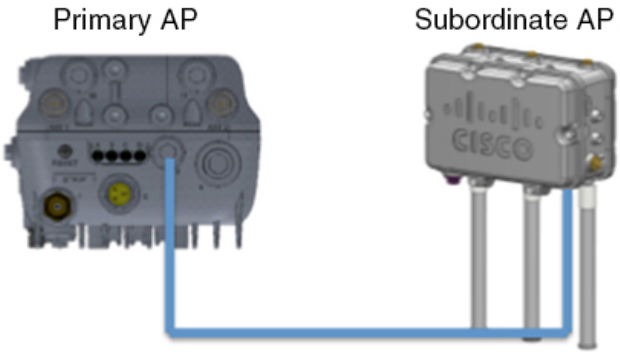
Caution We recommend that you connect Ethernet Bridged wired clients or Daisy-chained APs to either the Ethernet port or PoE-Out port only. Ethernet Bridged wired clients should never be connected to PoE-in port.



If the primary AP is a 1570 and the subordinate AP is a 1532 or 3700P, the Ethernet cable connects the PoE-Out port of the primary AP to the PoE-In port of the subordinate AP.



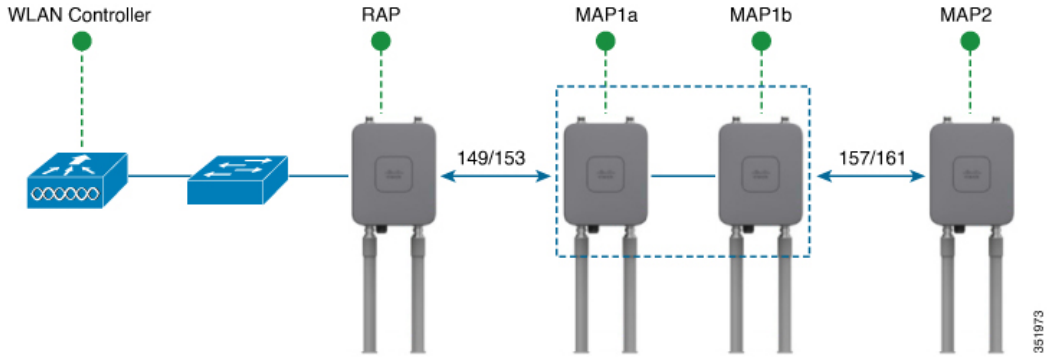
If the primary AP is a 1570 and the subordinate AP is a 1520 or 1550, the Ethernet cable connects the 1572's Ethernet port to any Ethernet port on the 1552.



Serial Backhaul on the Cisco Aironet 1530/1572 Series Access Points

Daisy chaining on the Cisco Aironet Access Points can be used to provide a serial-backhaul mesh. MAP1a is the primary MAP and has a preferred parent selected as the RAP. MAP1b is the subordinate MAP and has no preferred parent selected. MAP1b is configured in “Bridge” AP mode with “RootAP” role. Daisy chaining is enabled for MAP1b. MAP2 has preferred parent selected as MAP1b.

Figure 48: Daisy Chaining with Serial-Backhaul Mesh



High gain directional antenna must be used in typical serial-backhaul deployments. Additionally, preferred parent configurations must be used to create serial-backhaul mesh networks.

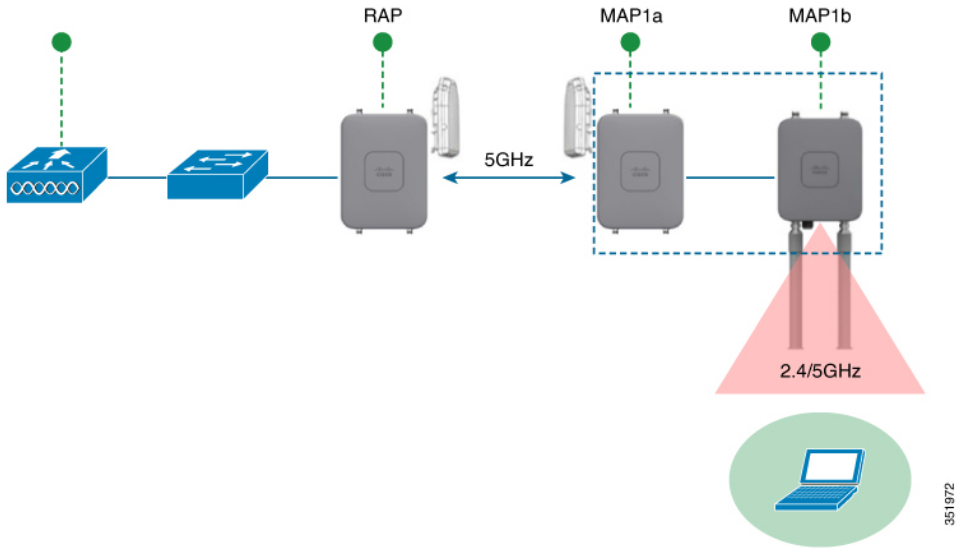
The child AP selects the preferred parent based on the following conditions:

- Preferred parent is the best parent.
- Preferred parent has a link SNR of at least 20 dB.
- Preferred parent has a link SNR in the range 12 dB and 20 dB, but no other parent is significantly better (SNR of more than 20 percent is better). For SNR that is lower than 12 dB, the configuration is ignored.
- Preferred parent is not in a blocked list.
- Preferred parent is not in silent mode because of dynamic frequency selection (DFS).
- Preferred parent is in the same bridge group name (BGN). If the configured preferred parent is not in the same BGN and no other parent is available, the child will associate with the parent AP using the default BGN.

Extended Universal Access

Daisy chaining on the Cisco Aironet 1530 Series Access Points can be used to extend Universal Access across a mesh network. In this example MAP1a is the primary MAP, it is backhauled wirelessly with the RAP. MAP1b, the subordinate MAP is operating in local/Flex-connect mode and is providing client access on both the 2.4GHz and 5GHz radio.

Figure 49: Daisy Chaining to Extend Universal Access



Important Points to Note When Configuring Daisy Chaining the Cisco Aironet 1530/1570 Series Access Points

- Only Mesh Access Points (MAPs) can operate as a daisy chained APs.
- The uplink daisy-chained AP is considered the primary AP; the connected AP is considered as the subordinate AP.
- The connecting Ethernet cable must go from the LAN port of the primary AP to the PoE in port of the subordinate AP.
- There must be a preferred parent set for each daisy-chained mesh hop; the primary MAP should have a preferred parent.
- Daisy chaining must be enabled on the subordinate AP in the Bridge mode through controller GUI or CLI or on the AP console.
- Directional antennas must be used when you create a daisy chain; the antennas must be used to guide the mesh tree formation to suit your needs.
- Directional antenna must have a physical separation of 3 meters.
- Ethernet bridging must be enabled on all the APs in the Bridge mode.

Configuring Daisy Chaining (CLI)

Procedure

- Configure daisy chaining by entering this command:
  config ap daisy-chaining {**enable** | **disable**} *cisco-mesh-ap*
- Configure the preferred parent for each serial-backhaul AP by entering this command:
  config mesh parent preferred *cisco-ap parent-mac-address*
- View the status of daisy chaining and the preferred parent that is configured by entering this command:

show ap config general *cisco-ap*

Configuring Daisy Chaining (AP CLI)

Procedure

- Configure daisy chaining on the AP by entering this command on the AP console:
  capwap ap daisy-chaining {**enable** | **disable**}

Configuring a Daisy-Chain

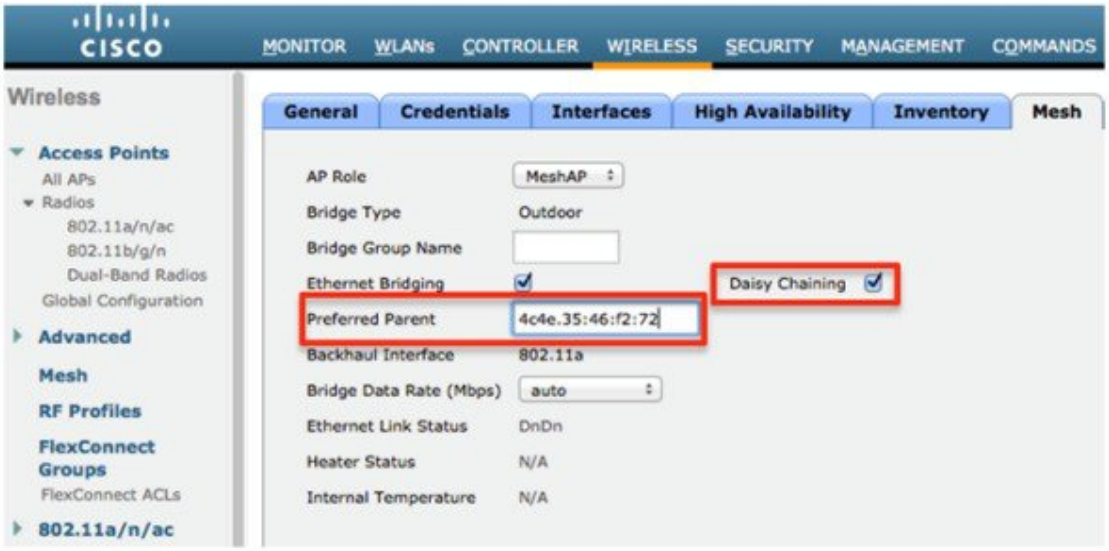
There are a few key components to address when configuring a daisy-chaining deployment:

- Only Mesh Access Points (MAPs) can operate as a daisy-chained AP.
- The uplink daisy-chained AP is considered the primary AP, and the connected AP is considered the subordinate AP.
- There must be a preferred parent set for each daisy-chained mesh hop. The primary MAP should have a preferred parent.
- Daisy-chaining must be enabled on the AP, either via controller GUI, controller CLI, or AP CLI.
- Directional antennas should be used when creating a daisy-chain, which guides the mesh tree formation to the customer needs.

Enabling Daisy-Chaining on Controller (GUI)

To enable Daisy-Chaining from the controller GUI, go to **Wireless > Access Point > (AP_NAME) > Mesh**, and then check the **Daisy-Chaining** check box. If the AP is used in a serial-backhaul solution, a **Preferred Parent** must be selected.

Note Daisy-chaining should only be enabled on the subordinate RAP. The primary MAP should have daisy-chaining as disabled.



Enabling Daisy-Chaining on the Controller (CLI)

To enable Daisy-Chaining from the controller CLI, issue the command:

```
(Cisco Controller) >config ap daisy-chaining [enable/disable] <ap_name>
```

The daisy chaining feature must be enabled on a per access point basis:

```
(Cisco Controller) >show ap config general <ap_name>
```

Then scroll down the Daisy Chaining entry

```
Daisy Chaining ................................. Disabled
```

Enabling Daisy-Chaining using the AP CLI

To enable Daisy-Chaining from the AP CLI, issue the command:

```
AP#capwap ap daisy-chaining <enable/disable>
```

Setting a Preferred Parent for each Serial-Backhaul AP

To set up a preferred parent for each serial-backhaul AP, issue the command:

```
(Cisco Controller) >config mesh parent preferred <ap_name> <PARENT_MAC_ADDRESS>
```

An access point's preferred parent can be seen by issuing:

```
Cisco Controller) >show ap config general <ap_name>
```

Then scroll down the Mesh preferred parent entry

```
Mesh preferred parent ........................... 00:24:13:0f:92:00
```

Note For more details, see this page.

Configuring Mesh Convergence

Information About Mesh Convergence

Using the controller, you can configure mesh convergence methods per mesh AP (MAP) or for all mesh APs. This enables you to choose the convergence methods based on deployment without affecting the existing convergence mechanism. The default setting is the existing convergence mechanism.

Mesh Convergence	Parent Loss Detection / Keep Alive Timers	Channel Scan / Seek	DHCP / CAPWAP Information
Standard	21 / 3 seconds	Scan/Seek all 5-GHz channels	Renew/Restart CAPWAP
Fast	7 / 3 seconds	Scan/Seek only preset channels	Maintain DHCP and CAPWAP
Very Fast	4 / 1.5 seconds	Scan/Seek only preset channels	Maintain DHCP and CAPWAP

Restrictions on Mesh Convergence

In Cisco Wave 2 APs, the convergence settings are as follows:

Table 32: Frequency to Seek Parent

Convergence Setting	Frequency to Seek Parent
Very Fast	Every 500 milliseconds
Fast	Every 750 milliseconds
Standard	Every 1 second

The frequency to seek neighbors for all convergence settings is 15 seconds.

If the AP fails to respond 8 times, the parent or the neighbor is assumed lost.

Table 33: Totaly Time Taken to Calculate Parent Loss

Convergence Setting	Total Time Taken
Very Fast	4 seconds
Fast	6 seconds
Standard	8 seconds

The neighbor (non-parent), loss time is 2 minutes.

In fast and very fast convergence, a subset channel seek is performed. The AP maintains a list of channels supported by neighboring parents and directly seeks those channels than going for a channel scan. For standard convergence, a channel scan is performed when the parent is lost.

Configuring Mesh Convergence (CLI)

Procedure

- Configure mesh convergence on the controller CLI by entering this command:
  config mesh convergence {**fast** | **standard** | **very-fast**} **all**

Note The **all** keyword denotes all MAP nodes.

- Mesh convergence commands on the AP console:
  a) To see the current subset list of channels:
  show mesh convergence
  b) To debug mesh convergence:
  debug mesh convergence
  c) To set convergence method at the AP:
  test mesh convergence {**fast** | **standard** | **very_fast**}

Switching Between LWAPP and Autonomous Images (AP CLI)

By default, the Cisco AP1532 and AP1572 are set to unified mode.

Procedure

- Switch the access point from LWAPP mode to autonomous mode (aIOS) by entering this command on the AP console:
  capwap ap autonomous

Note This command should be used only once, during initial priming of the access point. For information about switching back from autonomous mode to LWAPP mode, see https://supportforums.cisco.com/docs/DOC-14960.

Information About DHCP on RAP

This feature enables internal DHCP IPv4 server in the Root AP (RAP). This server provides the IPv4 address to the Mesh AP (MAP) and its associated clients (wired and wireless). The range available for this DHCP server is limited to a single scope of IP address. The available range is from 10.1.1.1 to 10.1.200.200.

A single controller can support multiple RAPs only if the RAPs are physically different mesh networks. Roaming of Mesh APs on a different mesh network is not supported.

This feature is supported in Cisco Outdoor APs—1540 and 1560 APs in Flex + Bridge mode only.

Restrictions on DHCP on RAP

- Only one Root AP is allowed to run the DHCP server in one subnet.
- Supports only one native VLAN in the mesh network.
- No GUI configuration available.

Configuring DHCP on RAP on a Controller (CLI)

Use these commands to configure DHCP on RAP with the controller's CLI:

Procedure

- Configure the internal AP mesh DHCP server by entering this command:

  config ap mesh-internal-dhcp {**enable | disable**}*ap-name*
- View the Mesh DHCP status by entering this command:

  show mesh dhcp status

Configuring DHCP on RAP on a Mesh AP (CLI)

Use these commands to configure DHCP on RAP with the AP CLI:

Procedure

- Configure the mesh DHCP management by entering this command:

  config mesh dhcp mgmt start-ip *start-addr end-addr mask*

  The start-IP is assigned to the RAP and is the gateway IP address.
- Configure the mesh DHCP DNS server by entering this command:

  config mesh dhcp mgmt dns-server *IP-addr*

  Limited to one IP address only.
- Configure the mesh DHCP Option43 by entering this command:

  config mesh dhcp mgmt option-43 *IP-addr*

  Limited to one IP address only.
- Configure the mesh DHCP domain by entering this command:

  config mesh dhcp mgmt domain *domain-name*
- Configure the lease time for the mesh DHCP by entering this command:

  config mesh dhcp mgmt lease *lease-time in seconds*

  The valid range is between 600 and 86,400 seconds.
- Configure mesh DHCP server state by entering this command:

  config mesh dhcp {**start-server** | **stop-server**}

- Clear the mesh DHCP IP address lease by entering this command:

  config mesh dhcp clear-lease {**all** | *IP-addr*}

- View the current DHCP configuration by entering this command:

  show mesh dhcp config

- View all the active lease IP addresses by entering this command:

  show mesh dhcp lease

- View the DHCP on RAP activity log by entering this command:

  show mesh dhcp log

Debugging DHCP on RAP on a Mesh AP (CLI)

Procedure

- Debug the Mesh DHCP by entering this command:

  debug mesh dhcp

Information About NAT-PAT on RAP

The Network Address Translation(NAT) and Port Address Translation (PAT) on Flex Mesh Root AP (RAP) depends on the internal DHCP server. This function is enabled and disabled when the internal DHCP server is enabled or disabled.

When the RAP's local DHCP server is enabled, the first IP address from the defined IP address scope is assigned as the default gateway IP address.

When there is traffic from the Mesh AP or the associated clients, the RAP NAT's the private IPv4 addresses. However, these IP addresses are sent to the controller which displays these IPv4 addresses on its GUI.

Note Only the RAP has a public IP address in the mesh network.

Restrictions on NAT-PAT on RAP

- When AP LAG is enabled in the controller, creating a daisy chain using Cisco Mesh APs fails as it is not supported for APs behind NAT-PAT.

Viewing NAT-PAT on RAP on a Mesh AP (CLI)

Use these commands to view NAT-PAT on RAP with the AP CLI:

Procedure

- View the client IP MAC mapping by entering this command:

show mesh nat client

- View the client downlink IP MAC mapping by entering this command:

  show mesh nat dl-map

- View the ICMP Mapping by entering this command:

  show mesh nat icmp

- View the TCP Mapping by entering this command:

  show mesh nat tcp

- View the UDP Mapping by entering this command:

  show mesh nat udp

Debugging NAT-PAT on RAP on a Mesh AP (CLI)

Procedure

- Debug NAT on Mesh by entering this command:

  debug mesh nat

Configuring Mesh Leaf Node

Access points within a mesh network operate in one of the following two ways:

1. Root access point (RAP)
2. Mesh access point (MAP)

While the RAPs have wired connections to their controller, the MAPs have wireless connections to their controller. MAPs communicate among themselves and back to the RAP using wireless connections over the 802.11a/n/g radio backhaul. MAPs use the Cisco Adaptive Wireless Path Protocol (AWPP) to determine the best path through the other mesh access points to the controller.

Relationships among mesh access points are as a parent, child, or neighbor.

- A parent access point offers the best route back to the RAP. A parent can be either the RAP itself or another MAP.
- A child access point selects the parent access point as its best route back to the RAP.
- A neighbor access point is within RF range of another access point but is not selected as its parent or a child.

You can configure the MAP with lower performance to work only as a leaf node. When the mesh network is formed and converged, the leaf node can only work as a child MAP, and cannot be selected by other MAPs as a parent MAP, so that the wireless backhaul performance will not be downgraded.

Note The mesh leaf node feature is supported only for the IR829 AP803 and the IW3700 Series access points.

Use the following command to configure an MAP as a leaf node:

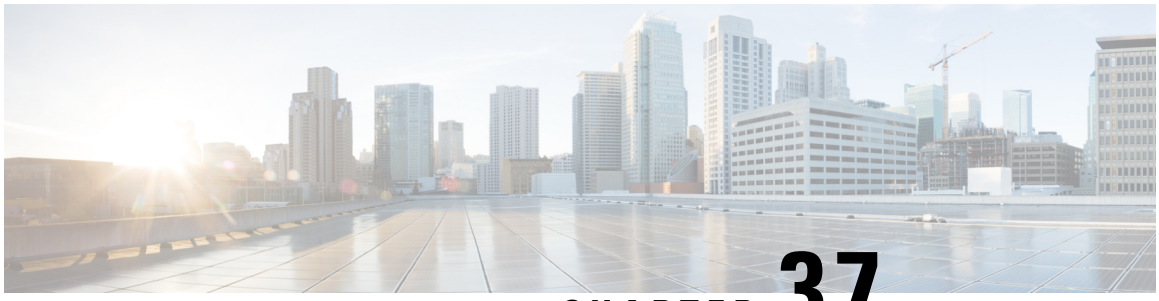
```
(Cisco Controller) >config mesh block-child <ap_name> {enable|disable}

enable          Enable blocking child for an MAP
disable         Disable blocking child for an MAP
```

Use the following commands to display the details of the leaf node configuration:

```
(Cisco Controller) >show mesh block-child {summary|<ap_name>}
```

Examples

```
(Cisco Controller) >show mesh block-child summary

AP Name       AP Model             BVI MAC Hop  Bridge Group Name  Block Child Set
----------  -------------------  -----------------  ---  -----------------  -------------
AP3        AIR-CAP3602I-C-K9    4c:00:82:07:64:6b  1    mesh               True

Number of Mesh APs Block Child Set.............................. 1

(Cisco Controller) >show mesh block-child AP3

AP Name        AP Model             BVI MAC Hop  Bridge Group Name  Block Child Set
----------  -------------------  -----------------  ---  -----------------  -------------
AP3        AIR-CAP3602I-C-K9    4c:00:82:07:64:6b  1    mesh               True
```



CHAPTER 37

Checking the Health of the Network

- Show Mesh Commands, on page 795
- Viewing Mesh Statistics for a Mesh Access Point, on page 801
- Viewing Neighbor Statistics for a Mesh Access Point, on page 805

Show Mesh Commands

The **show mesh** commands are grouped under the following sections:

Viewing General Mesh Network Details

To view general mesh network details, enter these commands:

- **show mesh env** {**summary** | *AP_name*}—Shows the temperature, heater status, and Ethernet status for either all access points (summary) or a specific access point (AP_name). The access point name, role (RootAP or MeshAP), and model are also shown.
  - The temperature is shown in both Fahrenheit and Celsius.
  - The heater status is ON or OFF.
  - The Ethernet status is UP or DOWN.

Note The battery status appears as N/A (not applicable) in the **show mesh env** *AP_name* status display because it is not provided for access points.

```
(Cisco Controller) > show mesh env summary

AP Name             Temperature(C/F)  Heater  Ethernet  Battery
------------------  ----------------  ------  --------  -------
SB_RAP1              39/102           OFF     UpDnNANA  N/A
SB_MAP1              37/98            OFF     DnDnNANA  N/A
SB_MAP2              42/107           OFF     DnDnNANA  N/A
SB_MAP3              36/96            OFF     DnDnNANA  N/A

(Cisco Controller > show mesh env SB_RAP1
AP Name..................................... SB_RAP1
AP Model.................................... AIR-LAP1522AG-A-K9
AP Role..................................... RootAP

Temperature................................. 39 C, 102 F
Heater...................................... OFF
Backhaul.................................... GigabitEthernet0
GigabitEthernet0 Status..................... UP
    Duplex.................................. FULL
    Speed................................... 100
    Rx Unicast Packets...................... 988175
    Rx Non-Unicast Packets.................. 8563
    Tx Unicast Packets...................... 106420
    Tx Non-Unicast Packets.................. 17122
GigabitEthernet1 Status..................... DOWN
POE Out..................................... OFF
Battery..................................... N/A
```

- **show mesh ap summary**—Revised to show the CERT MAC field that shows a MAC address within an AP certificate that can be used to assign a username for external authentication.

```
(Cisco Controller) > show mesh ap summary
AP Name AP Model           BVI MAC            CERT MAC          Hop Bridge Group Name
------- ---------------    -----------------  ----------------- ---- ------------------
R1      LAP1520            00:0b:85:63:8a:10  00:0b:85:63:8a:10 0    y1
R2      LAP1520            00:0b:85:7b:c1:e0  00:0b:85:7b:c1:e0 1    y1
H2      AIR-LAP1522AG-A-K9 00:1a:a2:ff:f9:00  00:1b:d4:a6:f4:60 1
Number of Mesh APs.............................. 3
Number of RAP................................... 2
Number of MAP................................... 1
```

- **show mesh path**—Displays MAC addresses, access point roles, SNR ratios (dBs) for uplink and downlink (SNRUp, SNRDown) and link SNR for a particular path.

```
(Cisco Controller) > show mesh path mesh-45-rap1
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
----------------- ------- ------ -------- -------- ------ -------
mesh-45-rap1      165     15     18       16       0x86b UPDATED NEIGH PARENT BEACON
mesh-45-rap1 is a Root AP.
```

- **show mesh neighbor summary**—Displays summary information about mesh neighbors. Neighbor information includes MAC addresses, parent-child relationships, and uplink and downlink (SNRUp, SNRDown).

```
(Cisco Controller) > show mesh neighbor summary ap1500:62:39:70
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags  State
mesh-45-rap1      165     15     18       16       0x86b  UPDATED NEIGH PARENT BEACON
00:0B:85:80:ED:D0 149     5      6        5        0x1a60 NEED UPDATE BEACON DEFAULT
00:17:94:FE:C3:5F 149     7      0        0        0x860  BEACON
```

Note After review of the **show mesh** commands above, you should be able to see the relationships between the nodes of your network and verify the RF connectivity by seeing the SNR values for every link.

- **show mesh ap tree**—Displays mesh access points within a tree structure (hierarchy).

```
(Cisco Controller) > show mesh ap tree
R1(0,y1)
|-R2(1,y1)
|-R6(2,y1)
|-H2(1,default)
Number of Mesh APs.............................. 4
Number of RAP................................... 1
Number of MAP................................... 3
```

Viewing Mesh Access Point Details

To view a mesh access point's configuration, enter these commands:

- **show ap config general** *Cisco_AP*—Displays system specifications for a mesh access point.

```
(Cisco Controller) > show ap config general aps
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........................ 1-4404
Primary Cisco Switch IP Address.................. 2.2.2.2
Secondary Cisco Switch Name...................... 1-4404
Secondary Cisco Switch IP Address................ 2.2.2.2
Tertiary Cisco Switch Name....................... 2-4404
Tertiary Cisco Switch IP Address................. 1.1.1.4
```

- **show mesh astools stats** [*Cisco_AP*]—Displays anti-stranding statistics for all outdoor mesh access points or a specific mesh access point.

```
(Cisco Controller) > show mesh astools stats

Total No of Aps stranded : 0
> (Cisco Controller) > show mesh astools stats sb_map1

Total No of Aps stranded : 0
```

- **show advanced backup-controller**—Displays configured primary and secondary backup controllers.

```
(Cisco Controller) > show advanced backup-controller
AP primary Backup Controller ..................... controller1 10.10.10.10
AP secondary Backup Controller ..............  0.0.0.0
```

- **show advanced timer**—Displays settings for system timers.

```
(Cisco Controller) > show advanced timer
Authentication Response Timeout (seconds)........ 10
Rogue Entry Timeout (seconds)..................... 1300
AP Heart Beat Timeout (seconds).................. 30
AP Discovery Timeout (seconds)................... 10
AP Primary Discovery Timeout (seconds)........... 120
```

- **show ap slots**—Displays slot information for mesh access points.

```
(Cisco Controller) > show ap slots
Number of APs.................................... 3
AP Name Slots AP Model            Slot0    Slot1   Slot2    Slot3
------------------------------  ------  -------  ------   ------
R1       2    LAP1520            802.11A  802.11BG
H1       3    AIR-LAP1521AG-A-K9 802.11BG 802.11A  802.11A
H2       4    AIR-LAP1521AG-A-K9 802.11BG 802.11A  802.11A 802.11BG
```

Viewing Global Mesh Parameter Settings

Use this command to obtain information on global mesh settings:

- **show mesh config**—Displays global mesh configuration settings.

```
(Cisco Controller) > show mesh config
Mesh Range....................................... 12000
Backhaul with client access status............... disabled
Background Scanning State........................ enabled
Mesh Security
Security Mode.................................. EAP
External-Auth.................................. disabled
Use MAC Filter in External AAA server......... disabled
Force External Authentication.................. disabled
Mesh Alarm Criteria
Max Hop Count.................................. 4
Recommended Max Children for MAP.............. 10
Recommended Max Children for RAP.............. 20
Low Link SNR................................... 12
High Link SNR.................................. 60
Max Association Number......................... 10
```

```
Association Interval.......................... 60 minutes
Parent Change Numbers......................... 3
Parent Change Interval........................ 60 minutes
Mesh Multicast Mode........................... In-Out
Mesh Full Sector DFS.......................... enabled
Mesh Ethernet Bridging VLAN Transparent Mode..... enabled
```

Viewing Bridge Group Settings

Use these commands to view bridge group settings:

- **show mesh forwarding table**—Shows all configured bridges and their MAC table entries.
- **show mesh forwarding interfaces**—Displays bridge groups and the interfaces within each bridge group. This command is useful for troubleshooting bridge group membership.

Viewing VLAN Tagging Settings

Use these commands to view VLAN tagging settings:

- **show mesh forwarding VLAN mode**—Shows the configured VLAN Transparent mode (enabled or disabled).
- **show mesh forwarding VLAN statistics**—Displays statistics for the VLAN and the path.
- **show mesh forwarding vlans**—Displays supported VLANs.
- **show mesh ethernet VLAN statistics**—Displays statistics for the Ethernet interface.

Viewing DFS Details

Use this command to view DFS details:

- **show mesh dfs history**—Displays a history of radar detections by channels and resulting outages.

```
(Cisco Controller) > show mesh dfs history
ap1520#show mesh dfs history
Channel 100 detects radar and is unusable (Time Elapsed: 18 day(s), 22 hour(s), 10
minute(s), 24 second(s)).
Channel is set to 136 (Time Elapsed: 18 day(s), 22 hour(s), 10 minute(s), 24 second(s)).
Channel 136 detects radar and is unusable (Time Elapsed: 18 day(s), 22 hour(s), 9
minute(s), 14 second(s)).
Channel is set to 161 (Time Elapsed: 18 day(s), 22 hour(s), 9 minute(s), 14 second(s)).
Channel 100 becomes usable (Time Elapsed: 18 day(s), 21 hour(s), 40 minute(s), 24
second(s)).
Channel 136 becomes usable (Time Elapsed: 18 day(s), 21 hour(s), 39 minute(s), 14
second(s)).
Channel 64 detects radar and is unusable (Time Elapsed: 0 day(s), 1 hour(s), 20 minute(s),
 52 second(s)).
Channel 104 detects radar and is unusable (Time Elapsed: 0 day(s), 0 hour(s), 47
minute(s), 6 second(s)).
Channel is set to 120 (Time Elapsed: 0 day(s), 0 hour(s), 47 minute(s), 6 second(s)).
```

- **show mesh dfs channel** *channel number*—Displays a history of radar detections and outages for a specified channel.

```
(Cisco Controller) > show mesh dfs channel 104
ap1520#show mesh dfs channel 104
Channel 104 is available
Time elapsed since radar last detected: 0 day(s), 0 hour(s), 48 minute(s), 11 second(s).
```

Viewing Security Settings and Statistics

Use this command to view security settings and statistics:

- **show mesh security-stats** *AP_name*—Shows packet error statistics and a count of failures, timeouts, and successes with respect to associations and authentications as well as reassociations and reauthentications for the specified access point and its child.

```
(Cisco Controller) > show mesh security-stats ap417

AP MAC : 00:0B:85:5F:FA:F0
Packet/Error Statistics:
----------------------------
Tx Packets 14, Rx Packets 19, Rx Error Packets 0
Parent-Side Statistics:
-------------------------
Unknown Association Requests 0
Invalid Association Requests 0
Unknown Re-Authentication Requests 0
Invalid Re-Authentication Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Child-Side Statistics:
-------------------------
Association Failures 0
Association Timeouts 0
Association Successes 0
Authentication Failures 0
Authentication Timeouts 0
Authentication Successes 0
Re-Association Failures 0
Re-Association Timeouts 0
Re-Association Successes 0
Re-Authentication Failures 0
Re-Authentication Timeouts 0
Re-Authentication Successes 0
```

Viewing GPS Status

Procedure

- See location summary of all APs by entering this command:

  show ap gps location summary

```
(Site5_AMC_02) >show ap gps location summary

AP Name             GPS Present   Latitude       Longitude       Altitude        GPS
location Age
------------------  -----------   ------------   -------------   -------------
------------------------
SJC24-RAP-EAST      NO            N/A            N/A             N/A             N/A
SJC21-RAP-NORTH     NO            N/A            N/A             N/A             N/A
SJC21-RAP-SOUTH     NO            N/A            N/A             N/A             N/A
Site5_21-17         NO            N/A            N/A             N/A             N/A
SJC22-ROOF-MAP      NO            N/A            N/A             N/A             N/A
Site5_21-28         NO            N/A            N/A             N/A             N/A
SJC-24-RAP-WEST     YES           37.42034194    -121.91973098   25.10  meters   000
days, 00 h 00 m 19 s
Site5_24-02         YES           37.41970399    -121.92051996   10.00  meters   000
days, 00 h 00 m 12 s
Site5_22-30         NO            N/A            N/A             N/A             N/A
Site5_23-200        NO            N/A            N/A             N/A             N/A
Site5_25-18         NO            N/A            N/A             N/A             N/A
Site5_22-15         NO            N/A            N/A             N/A             N/A
Site5_25-05         NO            N/A            N/A             N/A             N/A
```

- See a location summary of all mesh APs by entering this command:

  show mesh gps location summary

- See the location information for a particular mesh AP by entering this command:

  show mesh gps location *ap-name*

Viewing Mesh Statistics for a Mesh Access Point

This section describes how to use the controller GUI or CLI to view mesh statistics for specific mesh access points.

Note You can modify the Statistics Timer interval setting on the **All APs > Details** page of the controller GUI.

Viewing Mesh Statistics for a Mesh Access Point (GUI)

Procedure

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

Step 2 To view statistics for a specific mesh access point, hover the mouse over the blue drop-down arrow for the desired mesh access point and choose **Statistics**. The **All APs** > *AP Name* > **Statistics** page for the selected mesh access point appears.

This page shows the role of the mesh access point in the mesh network, the name of the bridge group to which the mesh access point belongs, the backhaul interface on which the access point operates, and the number of the physical switch port. It also displays a variety of mesh statistics for this mesh access point.

Table 34: Mesh Access Point Statistics

Statistics	Parameter	Description
Mesh Node Stats	Malformed Neighbor Packets	The number of malformed packets received from the neighbor. Examples of malformed packets include malicious floods of traffic such as malformed or short DNS packets and malformed DNS replies.
	Poor Neighbor SNR Reporting	The number of times the signal-to-noise ratio falls below 12 dB on the backhaul link.
	Excluded Packets	The number of packets received from excluded neighbor mesh access points.
	Insufficient Memory Reporting	The number of insufficient memory conditions.
	Rx Neighbor Requests	The number of broadcast and unicast requests received from the neighbor mesh access points.
	Rx Neighbor Responses	The number of responses received from the neighbor mesh access points.
	Tx Neighbor Requests	The number of unicast and broadcast requests sent to the neighbor mesh access points.
	Tx Neighbor Responses	The number of responses sent to the neighbor mesh access points.
	Parent Changes Count	The number of times a mesh access point (child) moves to another parent.
	Neighbor Timeouts Count	The number of neighbor timeouts.
Queue Stats	Gold Queue	The average and peak number of packets waiting in the gold (video) queue during the defined statistics time interval.
	Silver Queue	The average and peak number of packets waiting in the silver (best effort) queue during the defined statistics time interval.
	Platinum Queue	The average and peak number of packets waiting in the platinum (voice) queue during the defined statistics time interval.
	Bronze Queue	The average and peak number of packets waiting in the bronze (background) queue during the defined statistics time interval.
	Management Queue	The average and peak number of packets waiting in the management queue during the defined statistics time interval.

Statistics	Parameter	Description
Mesh Node Security Stats	Transmitted Packets	The number of packets transmitted during security negotiations by the selected mesh access point.
	Received Packets	The number of packets received during security negotiations by the selected mesh access point.
	Association Request Failures	The number of association request failures that occur between the selected mesh access point and its parent.
	Association Request Timeouts	The number of association request timeouts that occur between the selected mesh access point and its parent.
	Association Requests Successful	The number of successful association requests that occur between the selected mesh access point and its parent.
	Authentication Request Failures	The number of failed authentication requests that occur between the selected mesh access point and its parent.
	Authentication Request Timeouts	The number of authentication request timeouts that occur between the selected mesh access point and its parent.
	Authentication Requests Successful	The number of successful authentication requests between the selected mesh access point and its parent.
	Reassociation Request Failures	The number of failed reassociation requests between the selected mesh access point and its parent.
	Reassociation Request Timeouts	The number of reassociation request timeouts between the selected mesh access point and its parent.
	Reassociation Requests Successful	The number of successful reassociation requests between the selected mesh access point and its parent.
	Reauthentication Request Failures	The number of failed reauthentication requests between the selected mesh access point and its parent.
	Reauthentication Request Timeouts	The number of reauthentication request timeouts that occur between the selected mesh access point and its parent.
	Reauthentication Requests Successful	The number of successful reauthentication requests that occur between the selected mesh access point and its parent.
	Unknown Association Requests	The number of unknown association requests received by the parent mesh access point from its child. The unknown association requests often occur when a child is an unknown neighbor mesh access point.
	Invalid Association Requests	The number of invalid association requests received by the parent mesh access point from the selected child mesh access point. This state may occur when the selected child is a valid neighbor but is not in a state that allows association.

Statistics	Parameter	Description
Mesh Node Security Stats (continued)	Unknown Reauthentication Requests	The number of unknown reauthentication requests received by the parent mesh access point node from its child. This state may occur when a child mesh access point is an unknown neighbor.
	Invalid Reauthentication Requests	The number of invalid reauthentication requests received by the parent mesh access point from a child. This state may occur when a child is a valid neighbor but is not in a proper state for reauthentication.
	Unknown Reassociation Requests	The number of unknown reassociation requests received by the parent mesh access point from a child. This state may occur when a child mesh access point is an unknown neighbor.
	Invalid Reassociation Requests	The number of invalid reassociation requests received by the parent mesh access point from a child. This state may occur when a child is a valid neighbor but is not in a proper state for reassociation.

Viewing Mesh Statistics for a Mesh Access Point (CLI)

Use these commands to view mesh statistics for a specific mesh access point using the controller CLI:

- To view packet error statistics, a count of failures, timeouts, and successes with respect to associations and authentications, and reassociations and reauthentications for a specific mesh access point, enter this command:

  show mesh security-stats *AP_name*

  Information similar to the following appears:

```
AP MAC : 00:0B:85:5F:FA:F0
Packet/Error Statistics:
----------------------------
x Packets 14, Rx Packets 19, Rx Error Packets 0

Parent-Side Statistics:
-------------------------
Unknown Association Requests 0
Invalid Association Requests 0
Unknown Re-Authentication Requests 0
Invalid Re-Authentication Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0

Child-Side Statistics:
-------------------------
Association Failures 0
Association Timeouts 0
```

```
Association Successes 0
Authentication Failures 0
Authentication Timeouts 0
Authentication Successes 0
Re-Association Failures 0
Re-Association Timeouts 0
Re-Association Successes 0
Re-Authentication Failures 0
Re-Authentication Timeouts 0
Re-Authentication Successes 0
```

- To view the number of packets in the queue by type, enter this command:

  show mesh queue-stats *AP_name*

  Information similar to the following appears:

```
Queue Type  Overflows  Peak length  Average length
 ----------  ---------  -----------  --------------
 Silver      0          1            0.000
 Gold        0          4            0.004
 Platinum    0          4            0.001
 Bronze      0          0            0.000
 Management  0          0            0.000
```

  Overflows—The total number of packets dropped due to queue overflow.

  Peak Length—The peak number of packets waiting in the queue during the defined statistics time interval.

  Average Length—The average number of packets waiting in the queue during the defined statistics time interval.

Viewing Neighbor Statistics for a Mesh Access Point

This section describes how to use the controller GUI or CLI to view neighbor statistics for a selected mesh access point. It also describes how to run a link test between the selected mesh access point and its parent.

Viewing Neighbor Statistics for a Mesh Access Point (GUI)

Procedure

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

Step 2 To view neighbor statistics for a specific mesh access point, hover the mouse over the blue drop-down arrow for the desired mesh access point and choose **Neighbor Information**. The All APs > *Access Point Name* > Neighbor Info page for the selected mesh access point appears.

This page lists the parent, children, and neighbors of the mesh access point. It provides each mesh access point's name and radio MAC address.

Step 3 To perform a link test between the mesh access point and its parent or children, follow these steps:

a) Hover the mouse over the blue drop-down arrow of the parent or desired child and choose **LinkTest**. A pop-up window appears.
b) Click **Submit** to start the link test. The link test results appear on the Mesh > LinkTest Results page.
c) Click **Back** to return to the **All APs** > *Access Point Name* > **Neighbor Info** page.

Step 4 To view the details for any of the mesh access points on this page, follow these steps:

a) Hover the mouse over the blue drop-down arrow for the desired mesh access point and choose **Details**. The **All APs** > *Access Point Name* > **Link Details** > *Neighbor Name* page appears.
b) Click **Back** to return to the **All APs** > *Access Point Name* > **Neighbor Info** page.

Step 5 To view statistics for any of the mesh access points on this page, follow these steps:

a) Hover the mouse over the blue drop-down arrow for the desired mesh access point and choose **Stats**. The **All APs** > *Access Point Name* > **Mesh Neighbor Stats** page appears.
b) Click **Back** to return to the **All APs** > *Access Point Name* > **Neighbor Info** page.

Viewing the Neighbor Statistics for a Mesh Access Point (CLI)

Use these commands to view neighbor statistics for a specific mesh access point using the controller CLI.

- To view the mesh neighbors for a specific mesh access point, enter this command:

  show mesh neigh {**detail** | **summary**} *AP_Name*

  Information similar to the following appears when you request a summary display:

```
AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags  State
-----------------  ------- ------ -------- -------- ------  -------
mesh-45-rap1       165     15     18       16       0x86b  UPDATED NEIGH PARENT BEACON
00:0B:85:80:ED:D0  149      5      6        5       0x1a60  NEED UPDATE BEACON DEFAULT
00:17:94:FE:C3:5F  149    7      0        0      0x860      BEACON
```

- To view the channel and signal-to-noise ratio (SNR) details for a link between a mesh access point and its neighbor, enter this command:

  show mesh path *AP_Name*

  Information similar to the following appears:

```
AP Name/Radio Mac  Channel Snr-Up Snr-Down Link-Snr Flags  State
-----------------  ------- ------ -------- -------- ------  -------
mesh-45-rap1       165     15     18       16       0x86b  UPDATED NEIGH PARENT BEACON
mesh-45-rap1 is a Root AP.
```

- To view the percentage of packet errors for packets transmitted by the neighbor mesh access point, enter this command:

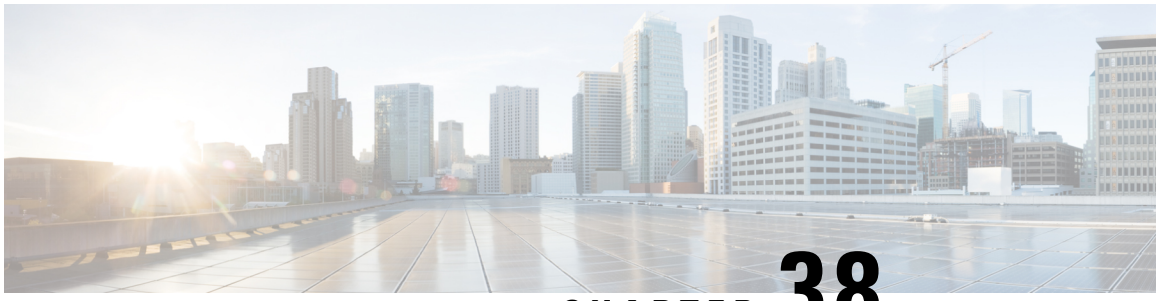
  show mesh per-stats *AP_Name*

  Information similar to the following appears:

```
Neighbor MAC Address 00:0B:85:5F:FA:F0
Total Packets transmitted: 104833
Total Packets transmitted successfully: 104833
```

```
Total Packets retried for transmission: 33028

Neighbor MAC Address 00:0B:85:80:ED:D0
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0

Neighbor MAC Address 00:17:94:FE:C3:5F
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0
```

Note Packet error rate percentage = 1 – (number of successfully transmitted packets/number of total packets transmitted).



CHAPTER 38

Troubleshooting Mesh Access Points

- Installation and Connections, on page 809

Installation and Connections

Procedure

Step 1 Connect the mesh access point that you want to be the RAP to the controller.

Step 2 Deploy the radios (MAP) at the desired locations.

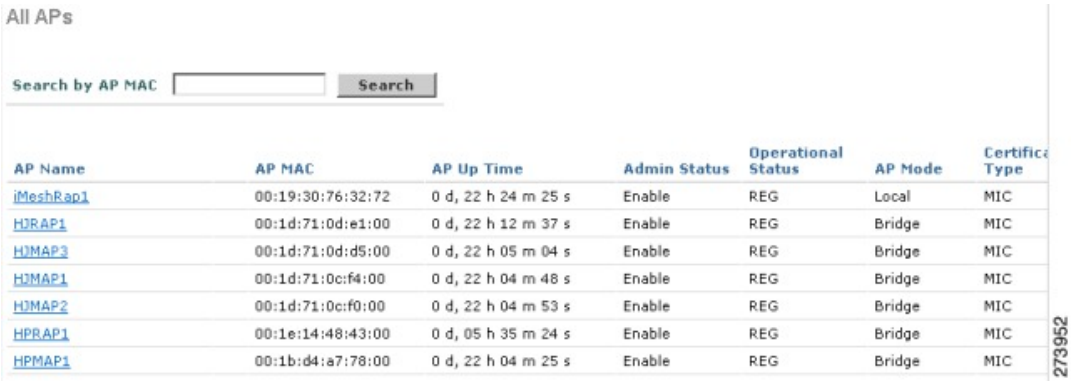
Step 3 On the controller CLI, enter the **show mesh ap summary** command to see all MAPs and RAPs on the controller.

Figure 50: Show Mesh AP Summary Page

```
(Cisco Controller) >show mesh ap summary

AP Name                AP Model             BVI MAC            CERT MAC          Hop  Bridge Group Name  Enhanced Feature Se
-----------------  -------------------  -----------------  -----------------  ---  -----------------  -------------------
1532MAP2-DaisyChained  AIR-CAP1532E-A-K9    4c:4e:35:46:f2:72  4c:4e:35:46:f2:72  0    default            N/A
1532RAP1             AIR-CAP1532E-A-K9    4c:4e:35:46:f2:64  4c:4e:35:46:f2:64  0    default            N/A
1532MAP1             AIR-CAP1532E-A-K9    4c:4e:35:46:f1:4e  4c:4e:35:46:f1:4e  1    default            N/A
1524PSRAP1           AIR-LAP1524PS-A-K9   00:22:be:41:23:00  00:22:be:41:23:00  0    MESHDEMO1          N/A
1522MAP2             AIR-LAP1522AG-A-K9   00:22:be:42:fe:00  00:22:be:42:fe:00  1    MESHDEMO1          N/A

Number of Mesh APs.............................. 3
Number of RAPs.................................. 2
Number of MAPs.................................. 1
Number of Flex+Bridge APs....................... 2
Number of Flex+Bridge RAPs...................... 1
Number of Flex+Bridge MAPs...................... 1
```

Step 4 On the controller GUI, click **Wireless** to see the mesh access point (RAP and MAP) summary.

Figure 51: All APs Summary Page



Step 5 Click **AP Name** to see the details page and then select the **Interfaces** tab to see the active radio interfaces.

The radio slot in use, radio type, subband in use, and operational status (UP or DOWN) are summarized.

- All APs supports 2 radio slots: slot 0—2.4 GHz and slot 1—5 GHz.

  If you have more than one controller connected to the same mesh network, then you must specify the name of the primary controller using global configuration for every mesh access point or specify the primary controller on every node, otherwise the least loaded controller is the preferred controller. If the mesh access points were previously connected to a controller, they already have learned a controller's name.

  After configuring the controller name, the mesh access point reboots.

Step 6 Click **Wireless > AP Name** to check the mesh access point's primary controller on the AP details page.

Debug Commands

The following two commands are very helpful to see the messages being exchanged between mesh access points and the controller.

```
(Cisco Controller) > debug capwap events enable
(Cisco Controller) > debug disable-all
```

You can use the **debug** command to see the flow of packet exchanges that occur between the mesh access point and the controller. The mesh access point initiates the discovery process. An exchange of credentials takes place during the join phase to authenticate that the mesh access point is allowed to join the mesh network.

Upon a successful join completion, the mesh access point sends a CAPWAP configuration request. The controller responds with a configuration response. When a Configure Response is received from the controller, the mesh access point evaluates each configuration element and then implements them.

Remote Debug Commands

You can log on to the mesh access point console for debugging either through a direct connection to the AP console port or through the remote debug feature on the controller.

To invoke remote debug on the controller, enter the following commands:

```
(Cisco Controller) > debug ap enable ap-name
(Cisco Controller) > debug ap command command ap-name
```

AP Console Access

AP1500s have a console port. A console cable is not shipped with the mesh access point. For the 1550 series access points, console ports are easily accessible and you need not open the access point box.

The AP1500s have console access security embedded in the code to prevent unauthorized access on the console port and provide enhanced security.

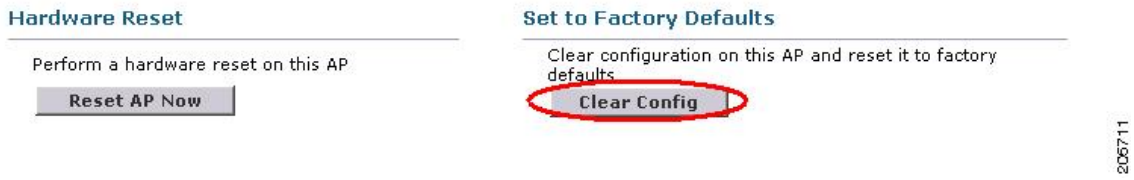
The **login ID** and **password** for console access are configured from the controller. You can use the following commands to push the username/password combination to the specified mesh access point or all access points:

```
<Cisco Controller> config ap username cisco password cisco ?

all           Configures the Username/Password for all connected APs.
<Cisco AP>    Enter the name of the Cisco AP.


<Cisco Controller> config ap username cisco password cisco all
```

You must verify whether the username/password pushed from the controller is used as *user-id* and *password* on the mesh access point. It is a nonvolatile setting. Once set, a *login ID* and *password* are saved in the private configuration of the mesh access point.

Once you have a successful login, the trap is sent to the Cisco Prime Infrastructure. If a user fails to log on three times consecutively, login failure traps are sent to the controller and Cisco Prime Infrastructure.

Caution A mesh access point must be reset to the factory default settings before moving from one location to another.



Cable Modem Serial Port Access from an AP

Commands can be sent to the cable modem from the privileged mode of the CLI. Use the command to take a text string and send it to the cable modem UART interface. The cable modem interprets the text string as one of its own commands. The cable modem response is captured and displayed on the Cisco IOS console. Up to 9600 characters are displayed from the cable modem. Any text that is greater than 4800 characters is truncated.

The modem commands are only operational on mesh APs that have devices connected to the UART port originally intended for the cable modem. If the commands are used on a mesh AP that does not have a cable modem (or any other device connected to the UART), the commands are accepted, however, but they do not produce any returned output. No errors are explicitly flagged.

Configuration

Enter the following command from the privileged mode of the MAP:

```
AP#send cmodem timeout-value modem-command
```

The modem command is any command or text to send to the cable modem. The range of timeout value is 1 to 300 seconds. However, if the captured data equals 9600 characters, any text beyond that is truncated and the response, irrespective of the timeout value and is immediately displayed on the AP console.

Figure 52: Cable Modem Console Access Command

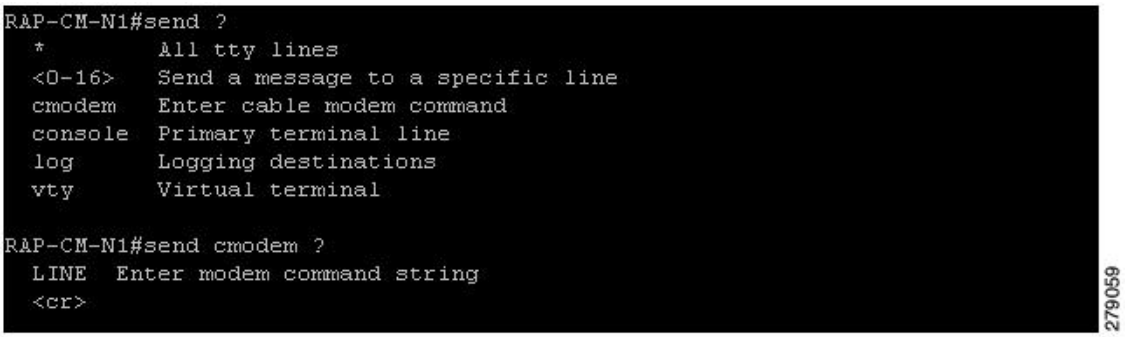
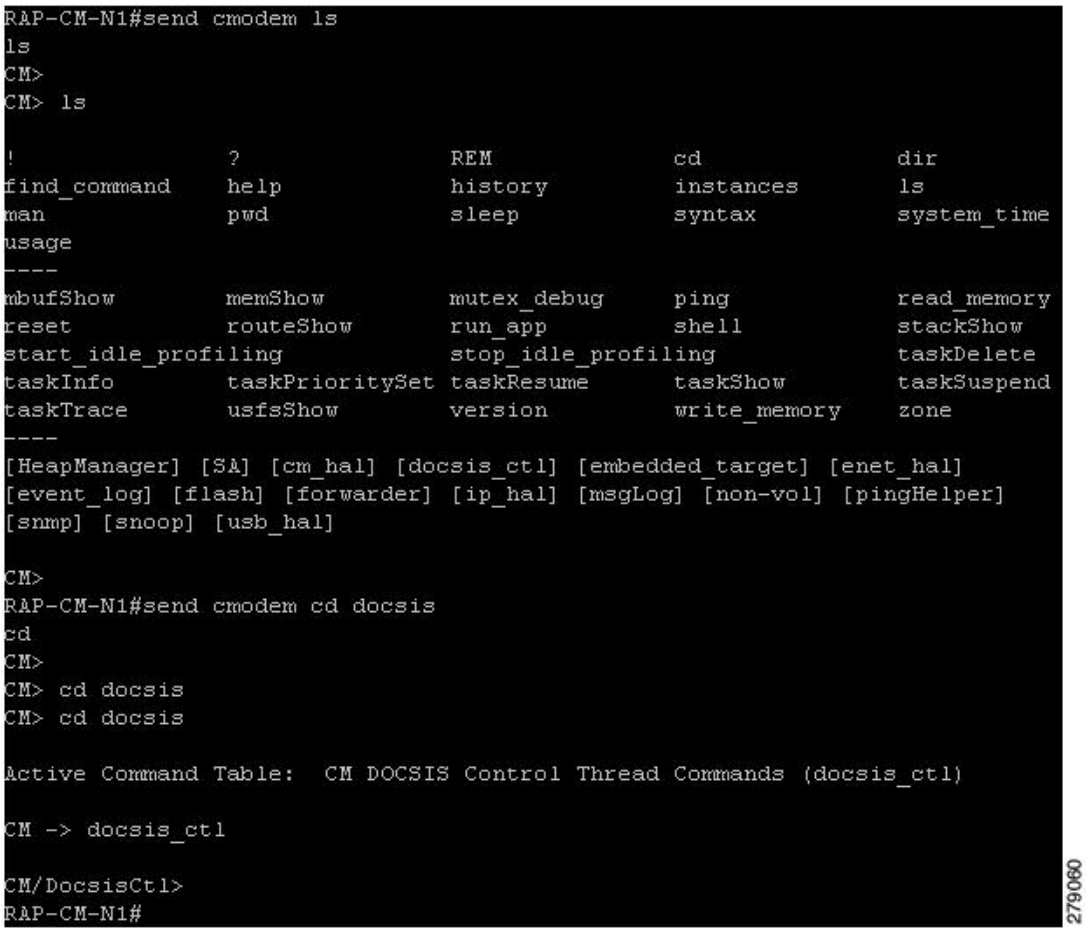


Figure 53: Cable Modem Console Access Command



Caution The question mark (?) and the exclamation point (!) should not be used in the **send cmodem** command. These characters have immediate interpreted use in the Cisco IOS CLI. Therefore, they cannot be sent to the modem.

Enabling the Cable Modem Console Port

By default, the Cable Modem console port is disabled. This is to prevent users from accessing the console through their residential cable modem. In the AP1572IC, AP1572EC, and AP1552C model, the cable modem console is connected directly to the access point. The console port is required for signaling between the AP and the cable modem. There are two methods to enable the cable modem console port, either through SNMP or by adding the command to the configuration .cm file on the CMTS.

Note For the AP1572EC, AP1572IC, AP1552C, and AP1552CU, the cable modem must be enabled.

- Enable the cable modem console port through SNMP by entering this command to the IP address of the cable modem:

```
snmpset –c private IP_ADDRESS cmConsoleMode.0 i N
```

Using the OID, enter this command:

```
snmpset –c private IP_ADDRESS
1.3.6.1.4.1.1429.77.1.4.7.0 i N
```

Where IP_ADDRESS is any IPv4 address and N is an integer, 2 to enable read-write, 1 for read-only, or 0 to disable.

Example:

```
snmpset -c private 209.165.200.224 cmConsoleMode.0 i 2
```

- Enable the cable modem console port through the configuration file. The configuration file (with a .cm extension) is loaded into the cable modem head end. It is pushed to the cable modem as part of the join process. Enter the following line to the cable modem configuration file:

  ```
  SA-CM-MIB::cmConsoleMode.0 = INTEGER: readWrite(2)
  ```

  Using the OID, enter this line:

  ```
  SA-CM-MIB::cmConsoleMode.0 = INTEGER: readWrite(2)
  ```

Resetting the AP1572xC/AP1552C Through the Cable Modem

An AP can be reset by entering an SNMP command to the Cable Modem, which resides inside the access point. For this feature to work, you must enable the cable modem console port.

Reset the AP by entering this snmpset command:

```
Snmpset -v2c -c public IP ADDRESS 1.3.6.1.4.1.1429.77.1.3.17.0 i 1
```

Where the IP ADDRESS is the IPv4 address of the cable modem.

Mesh Access Point CLI Commands

You can enter these commands directly on the mesh access point using the AP console port or you can use the remote debug feature from the controller:

```
Hl •shou lllBSh ?
  adjacency   l'ESH Adjacency
  astools     l'ESH Anti-strand tools
  backhaul    l'ESH backhaul
  channel     l'ESH channel
  canfig      l'ESH config paranenter
  dfs         l'ESH dfs lnfornatIon
  ethernet    sllou nesh Erthernet bridging
  foruarding  l'ESH Foruarding
  irwenlory   platforn inventory
  linktest    l'ESH linktest stats
  nmule       l'ESH nodule detail
  np!rf       l'ESH BN tool
  security    l'ESH  Security  shou        !2
  simulation  flESH sinul ated configLration ih
  status      l'ESH status
                                           Ul
```

```
HJRAPlllleliou nesh config
rtsfhresliold l la 0, eHs 0, a.11in 0, c:o.11ex 0
rtsfhresholdl llbg 0, aifs 0, a.1Hin 0, a.11ax 0
huRetrles O. llri<Rate O qOepth O
8O2.11MAt ient Statistics Push Int.......al: 3
range paraneter: 12000
nesh security node: 0
Universal Client Access: disabled
publ ic safety global state: enabled
Battery backup state: enabled
nul ticast node: in-out
Ful l Sector DFS: enabled
```

```
HJRAPlllehou caplolBp client mb
Adnin5tate                          ADHIN ENABLED
SuVer                               S.2.98.0
NunFll ledSlots                     2
Nane                                HJRAPl
Location                            default location
Huarllame                           SEYf-CllffROLLER
Huarrlp                             209.165.200.227
Huartt.Ner                          0.0.0.0
ApHocle                              Brld!JE!
ApSubl'lode                         Not [:mf igured
OperationState                      UP
CAPllN'Path nru                     1485
Link!U:liting                       disabled
ApRole                              RootAP
ApBac:khaul                         802.l la
Ap8ac:khaulthannel                  5805
ApBac:khaulSlot                     1
ApBac:khaul llgEnabled              0
ApBac:l<haullxRate                  24000
Ethernet Brldglrg State             0
Public Safety State                 enabled
```

```
HJHAPlllehoi.I nesh adjacency ?
  alI      HESH Adjacency AlI
  child    HESH Adjacency Child
  parent MESH Adjacency Parent
                                                    OI
```

```
HJMap4#shou mesh status '%
 shou MESH Status
 MeshAP in state Maint
 Uplink Backbone: Virtual-DotllRadio0
 Dounlink Backbone: Dot11Radiol
 Configured BGN: HuckJr
       rxNeighReq 129790 rxNeighRsp 66976 txNeighReq 33938 txNeighRsp 129790
       rxNeighRsp 147275 txNeighUpd 202060
       nextchan 0 nextant 0 downAnt 0 downChan 0 curAnts 0
       nextNeigh l. malformedNeighPackets 4.poorNeighSnr 1
       blacklistPackets 0,insufficientMemory 0, authenticationFailures 0
       Parent Changes 3, Neighbor Timeouts 0
       Vector through 0017.94fe.c3bf:
              Vector ease 1 -1, FWD: 0017.94fe.c3bf
                                                    273949
```

```
HJNap4#shou mesh forwarding link
 Current mesh links:
----------------------
 End Point  : 0017.94fe.c3bf
 Adjacency  : Exists
 Channel    : 161 on Dot11Radiol
 Type       : 2
 State      : 4
 Bundle     : member
 Bridge     : 1
 swidb      : Virtual-Dot11Radio0
 port state : OPEN
                                                    273950
```

Mesh Access Point Debug Commands

You can enter these commands directly on the mesh access point using the AP console port or you can use the remote debug feature from the controller.

- **debug mesh ethernet bridging**—Debugs Ethernet bridging.
- **debug mesh ethernet config**—Debugs access and trunk port configuration associated with VLAN tagging.
- **debug mesh ethernet registration**—Debugs the VLAN registration protocol. This command is associated with VLAN tagging.
- **debug mesh forwarding table**—Debugs the forwarding table containing bridge groups.
- **debugs mesh forwarding packet bridge-group**—Debugs the bridge group configuration.

Defining Mesh Access Point Roles

By default, the AP1500s are shipped with a radio role set to MAP. Therefore, you must change the radio role on a mesh access point for it to function as RAP.

You can change this configuration on the mesh access point by statically setting them as rooftop access points or mesh access points with the **config ap role** {*rootAP* | *mesh AP* | *default*} command:

To change the radio role can also be changed using the GUI, follow these steps:

Procedure

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

Step 2 Click the name of the mesh access point that you want to change. Click the **Mesh** tab.

Step 3 From the AP Role drop-down list, choose **MeshAP** or **RootAP** to specify this mesh access point as a MAP or RAP, respectively.

Step 4 Click **Apply** to commit your changes. The mesh access point reboots.

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

Note
We recommend a Fast Ethernet connection between the MAP and controller when changing from a MAP to RAP. After a RAP-to-MAP conversion, the MAP's connection to the controller is a wireless backhaul rather than a Fast Ethernet connection. It is the responsibility of the user to ensure that the Fast Ethernet connection of the RAP being converted is disconnected before the MAP starts up so that the MAP can join over the air.

Backhaul Algorithm

A **backhaul** is used to create only the wireless connection between mesh access points.

The backhaul interface by default is 802.11a. You cannot change the backhaul interface to 802.11b/g.

The "auto" data rate is selected by default for AP1500s.

The backhaul algorithm has been designed to fight against stranded mesh access point conditions. This algorithm also adds a high-level of resiliency for each mesh node.

The algorithm can be summarized as follows:

- A MAP always sets the Ethernet port as the **primary backhaul** if it is UP; otherwise, it is the 802.11a radio (this feature gives the network administrator the ability to configure it as a RAP the first time and recover it in-house). For fast convergence of the network, we recommend that you do not connect any Ethernet device to the MAP for its initial joining to the mesh network.
- A MAP failing to connect to a WLAN controller on an Ethernet port that is UP, sets the 802.11a radio as the **primary backhaul**. Failing to find a neighbor or failing to connect to a WLAN controller via any neighbor on the 802.11a radio causes the **primary backhaul** to be UP on the Ethernet port again. A MAP gives preference to the parent which has the same BGN.
- A MAP connected to a controller over an Ethernet port does not build a mesh topology (unlike a RAP).
- A RAP always sets the Ethernet port as the **primary backhaul**.

Note Cisco Wave 2 APs operating as RAPs can fall back on Ethernet sooner than 15 minutes if the RAPs cannot find any valid uplink on the radio in 5 minutes' time. In such a case, the RAPs clear the blocked-listing on the wired port and try to fall back on the wired port.

- If the Ethernet port on a RAP is DOWN, or a RAP fails to connect to a controller on an Ethernet port that is UP, the 802.11a radio is set as the **primary backhaul**. Failing to find a neighbor or failing to connect to a controller via any neighbor on the 802.11a radio makes the RAP go to the SCAN state after 15 minutes and starts with the Ethernet port first.

Keeping the roles of mesh nodes distinct using the above algorithm greatly helps to avoid a mesh access point from being in an unknown state and becoming stranded in a live network.

Passive Beaconing (Anti-Stranding)

When enabled, passive beaconing allows a stranded mesh access point to broadcast its debug messages over-the-air using a 802.11b/g radio. A neighboring mesh access point that is listening to the stranded mesh access point and has a connection to a controller, can pass those messages to the controller over CAPWAP. Passive beaconing prevents a mesh access point that has no wired connection from being stranded.

Debug logs can also be sent as distress beacons on a nonbackhaul radio so that a neighboring mesh access point can be dedicated to listen for the beacons.

The following steps are automatically initiated at the controller when a mesh access point loses its connection to the controller:

- Identifies the MAC address of a stranded mesh access point
- Finds a nearby neighbor that is CAPWAP connected
- Sends commands through remote debug
- Cycles channels to follow the mesh access point

You only have to know the MAC address of the stranded AP to make use of this feature.

A mesh access point is considered stranded if it goes through a lonely timer reboot. When the lonely timer reboot is triggered, the mesh access point, which is now stranded, enables passive beaconing, the anti-stranding feature.

This feature can be divided into three parts:

- Strand detection by stranded mesh access point
- Beacons sent out by stranded mesh access point
  - Latch the 802.11b radio to a channel (1,6,11)
  - Enable debugs
  - Broadcast the standard debug messages as distress beacons
  - Send Latest Crash info file
- Receive beacons (neighboring mesh access point with remote debugging enabled)

Deployed mesh access points constantly look for stranded mesh access points. Periodically, mesh access points send a list of stranded mesh access points and SNR information to the controller. The controller maintains a list of the stranded mesh access points within its network.

When the **debug mesh astools troubleshoot** *mac-addr* **start** command is entered, the controller runs through the list to find the MAC address of the stranded mesh access point.

A message is sent to the best neighbor to start listening to the stranded access point. The listening mesh access point gets the distress beacons from the stranded mesh access point and sends it to the controller.

Once a mesh access point takes the role of a listener, it does not purge the stranded mesh access point from its internal list until it stops listening to the stranded mesh access point. While a stranded mesh access point is being debugged, if a neighbor of that mesh access point reports a better SNR to the controller than the current listener by some percentage, then the listener of the stranded mesh access point is changed to the new listener (with better SNR) immediately.

End-user commands are as follows:

- **config mesh astools** [**enable** | **disable**]—Enables or disables the astools on the mesh access points. If disabled, APs no longer sends a stranded AP list to the controller.
- **show mesh astools stats**—Shows the list of stranded APs and their listeners if they have any.
- **debug mesh astools troubleshoot** *mac-addr* **start**—Sends a message to the best neighbor of the *mac-addr* to start listening.
- **debug mesh astools troubleshoot** *mac-addr* **stop**—Sends a message to the best neighbor of the *mac-addr* to stop listening.
- **clear mesh stranded** [**all** | *mac of b/g radio*]—Clears stranded AP entries.

The controller console is swamped with debug messages from stranded APs for 30 minutes.

Dynamic Frequency Selection

This section describes the Dynamic Frequency Selection (DFS) functionality in RAP and MAP.

DFS in RAP

The RAP performs the following steps as a response to radar detection:

1. The RAP sends a message to the controller that the channel is infected with radar. The channel is marked as infected on the RAP and on the controller.
2. The RAP blocks the channel for 30 minutes. This 30-minute period is called the nonoccupancy period.
3. The controller sends a TRAP, which indicates that the radar has been detected on the channel. A TRAP remains until the nonoccupancy period expires.
4. The RAP has 10 seconds to move away from the channel. This period is called the channel move time, which is defined as the time for the system to clear the channel and is measured from the end of the radar burst to the end of the final transmission on the channel.
5. The RAP enters the quiet mode. In the quiet mode, the RAP stops data transmissions. Beacons are still generated and probe responses are still delivered. The quiet mode exists until the channel move time is over (10 seconds).
6. The controller picks up a new random channel and sends the channel information to the RAP.
7. The RAP receives the new channel information and sends channel change frames (unicast, encrypted) to the MAP, and each MAP sends the same information to its lower children down the sector. Each mesh access point sends the channel change frames once every 100 msecs for a total of five times.
8. The RAP tunes to the new channel and enters into the silent mode. During the silent mode, only the receiver is ON. The RAP keeps scanning the new channel for any radar presence for 60 seconds. This process is called channel availability check (CAC).
9. The MAP tunes to the new channel and enters into the silent mode. During the silent mode, only the receiver is ON. The MAP keeps scanning the new channel for any radar presence for 60 seconds.
10. If radar is not detected, the RAP resumes full functionality on this new channel and the whole sector tunes to this new channel.

DFS in MAP

The MAP performs the following steps as a response to radar detection:

1. The MAP sends a radar seen indication to the parent and ultimately to the RAP indicating that the channel is infected. The RAP sends this message to the controller. The message appears to be coming from the RAP. The MAP, RAP, and controller mark the channel as infected for 30 minutes.
2. The MAP blocks the channel for 30 minutes. This 30-minute period is called the nonoccupancy period.
3. The controller sends a TRAP, which indicates that the radar has been detected on the channel. The TRAP remains until the nonoccupancy period expires.
4. The MAP has 10 seconds to move away from the channel. This is called the channel move time, which is defined as the time for the system to clear the channel and is measured from the end of the radar burst to the end of the final transmission on the channel.
5. The MAP enters the quiet mode. In the quiet mode, the MAP stops data transmissions. Beacons are still generated and probe responses are still delivered. The quiet mode exists until the channel move time is over (10 seconds).

6. The controller picks up a new random channel and sends the channel to the RAP.
7. The RAP receives the new channel information and sends channel change frames (unicast, encrypted) to a MAP, and each MAP sends the same information to its lower children down the sector. Each mesh access point sends the channel change frames once every 100 msecs for a total of five times.
8. Each mesh access point tunes to the new channel and enters into the silent mode. During the silent mode, only the receiver is ON. There is no packet transmission. An AP keeps scanning the new channel for any radar presence for 60 seconds. This process is called the channel availability check (CAC). The MAP should not disconnect from the controller. The network should remain stable during this one-minute period.

DFS functionality allows a MAP that detects a radar signal to transmit that up to the RAP, which then acts as if it has experienced radar and moves the sector. This process is called the coordinated channel change. This functionally can be turned on or off on the controller. The coordinated channel change is enabled by default.

To enable DFS, enter the following command:

```
(Cisco Controller) > config mesh full-sector-dfs enable
```

To verify that DFS is enabled on the network, enter the following command:

```
(Cisco Controller) > show network summary
```

Note A MAP that detects radar should send a message to the RAP, unless the parent has a different BGN, in which case it does not send messages for a coordinated sector change. Instead, the MAP reenters the SCAN state and searches on nonradar seen channels for a new parent.

Note Ensure that none of your mesh access points are using a default BGN.

Note A repeated radar event on the MAP (radar triggers once, and then almost immediately again), causes the MAP to disconnect.

Preparation in a DFS Environment

This section describes how to prepare in a DFS environment:

- To verify that your controller is set to the correct country domain, enter the following command:

  ```
  (Cisco Controller) > show country
  ```

- To check the mesh access point country and the channel setting on the controller, enter the following command:

```
(Cisco Controller)> show ap config 802.11a ap-name
```

- To identify channels available for mesh, enter the following command:

```
(Cisco Controller)> show ap config 802.11a ap-name
```

Look for the allowed channel list.

```
Allowed Channel List..................... 100,104,108,112,116,120,124,
..................................... 128,132,136,140
```

- To identify channels available for mesh on the AP console (or use remote debug from the controller, enter the following command:

```
ap1520-rap # show mesh channels

HW: Dot11Radio1, Channels:
100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
```

An asterisk next to a channel indicates that radar has been seen on the channel.

- To invoke remote debug, enter the following commands:

```
(Cisco Controller) > debug ap enable ap-name
(Cisco Controller) > debug ap command command ap-name
```

- Debug commands to see radar detection and past radar detections on the DFS channel are as follows:

```
show mesh dfs channel channel-number
show mesh dfs history
```

Information similar to the following appears.

ap1520-rap # **show mesh dfs channel** 132

```
Channel 132 is available
Time elapsed since radar last detected: 0 day(s), 7 hour(s), 6 minute(s), 51 second(s).
```

The RAP should be run through the channels to determine whether there is active radar on each of the channels.

```
ap1520-rap # show mesh dfs channel 132

Radar detected on channel 132, channel becomes unusable (Time Elapsed: 0 day(s), 7
hour(s), 7 minute(s), 11 second(s)).
Channel is set to 100 (Time Elapsed: 0 day(s), 7 hour(s), 7 minute(s), 11 second(s)).
Radar detected on channel 116, channel becomes unusable (Time Elapsed: 0 day(s), 7
hour(s), 6 minute(s), 42 second(s)).
Channel is set to 64 (Time Elapsed: 0 day(s), 7 hour(s), 6 minute(s), 42 second(s)).
Channel 132 becomes usable (Time Elapsed: 0 day(s), 6 hour(s), 37 minute(s), 10
```

```
second(s)).
Channel 116 becomes usable (Time Elapsed: 0 day(s), 6 hour(s), 36 minute(s), 42
second(s)).
```

Monitoring DFS

The DFS history should be run every morning or more frequently to detect the radar. This information does not get erased and is stored on the mesh access point flash. Therefore, you only need to match the times.

```
ap1520-rap # show controller dot11Radio 1
```

Information similar to the following appears:

```
interface Dot11Radio1
Radio Hammer 5, Base Address 001c.0e6c.9c00, BBlock version 0.00, Software version 0.05.30
Serial number: FOC11174XCW
Number of supported simultaneous BSSID on Dot11Radio1: 16
Carrier Set: ETSI (OFDM) (EU) (-E)
Uniform Spreading Required: Yes
Current Frequency: 5540 MHz Channel 108 (DFS enabled)
Allowed Frequencies: *5500(100) *5520(104) *5540(108) *5560(112) *5580(116) *560
0(120) *5620(124) *5640(128) *5660(132) *5680(136) *5700(140)
* = May only be selected by Dynamic Frequency Selection (DFS)
Listen Frequencies: 5180(36) 5200(40) 5220(44) 5240(48) 5260(52) 5280(56) 5300(6
0) 5320(64) 5500(100) 5520(104) 5540(108) 5560(112) 5580(116) 5660(132) 5680(136
) 5700(140) 5745(149) 5765(153) 5785(157) 5805(161) 5825(165) 4950(20) 4955(21)
4960(22) 4965(23) 4970(24) 4975(25) 4980(26)
```

Note An asterisk indicates that this channel has DFS enabled.

Frequency Planning

Use alternate adjacent channels in adjacent sectors. If you have two RAPs deployed at the same location, you must leave one channel in between.

Weather radars operate within the 5600- to 5650-MHz band, which means that channels 124 and 128 might be affected, but also channels 120 and 132 might suffer from weather radar activity.

If the mesh access point does detect radar, the controller and the mesh access point both will retain the channel as the configured channel. The controller retains it in volatile memory associated with the mesh access point, and the mesh access point has it stored in its flash as configuration. After the 30 minute quiet period, the controller returns the mesh access point to the static value, regardless of whether the mesh access point has been configured with a new channel or not. In order to overcome this, configure the mesh access point with a new channel, and reboot the mesh access point.

Once radar is reliably detected on a channel, that channel, and the two surrounding channels, should be added to the RRM exclusion list, as follows:

```
(Cisco Controller) > config advanced 802.11a channel delete channel
```

A mesh access point goes to a new channel that is picked by RRM, and it does not consider excluded channels.

If a radar is detected on channel 124, for instance, channels 120, 124, and 128 should be added to the exclusion list. In addition, do not configure RAP to operate on those channels.

Good Signal-to-Noise Ratios

For European installations, the minimum recommendation is increased to 20 dB of signal-to-noise ratio (SNR). The extra dBs are used to mitigate the effects of radar interference with packet reception, which is not observed in non-DFS environments.

Access Point Placement

Collocated mesh access points should have a minimum of 10 feet (3.048 meters) of vertical separation or 100 (30.48 meters) feet of horizontal separation.

Bridge Group Name Misconfiguration

A mesh access point can be wrongly provisioned with a *bridgegroupname* and placed in a group other than it was intended. Depending on the network design, this mesh access point might or might not be able to reach out and find its correct sector or tree. If it cannot reach a compatible sector, the mesh access point can become stranded.

To recover a stranded mesh access point, the concept of default bridgegroupname has been introduced in the software. When a mesh access point is unable to connect to any other mesh access point with its configured bridgegroupname, it attempts to connect with the bridgegroupname of *default*.

The algorithm of detecting this strand condition and recovery is as follows:

1. Passively scans and finds all neighbor nodes regardless of their bridgegroupname.
2. The mesh access point attempts to connect to the neighbors heard with *my own bridgegroupname* using AWPP.
3. If Step 2 fails, attempts to connect with default bridgegroupname using AWPP.
4. For each failed attempt in Step 3, it adds the neighbor to an exclusion list and attempts to connect the next best neighbor.
5. If the AP fails to connect with all neighbors in Step 4, it reboots the mesh access point.
6. If connected with a *default* bridgegroupname for 15 minutes, the mesh access point goes into a scan state.

When an mesh access point is able to connect with the default bridgegroupname, the parent node reports the mesh access point as a default child/node/neighbor entry on the controller, so that a network administrator is Cisco Prime Infrastructure. Such a mesh access point behaves as a normal (nonmesh) access point and accepts any client, other mesh nodes as its children, and it passes any data traffic through.

Note Do not confuse an unassigned BGN (null value) with DEFAULT, which is a mode that the access point uses to connect when it cannot find its own BGN.

To check the current state of a mesh access point's BGN, enter the following command:

```
(Cisco Controller)> show mesh path Map3:5f:ff:60
```

```
00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106B), snrUp 48, snrDown 48, linkSnr
 49
00:0B:85:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B) snrUp 72, snrDown 63, linkSrn 57
00:0B:85:5F:FA:60 is RAP
```

To check the current state of a mesh access point's BGN, check the neighbor information for the mesh access point (GUI) as follows:

Choose **Wireless > All APs** > *AP Name* > *Neighbor info* .

Figure 54: Neighbor Information for a Child

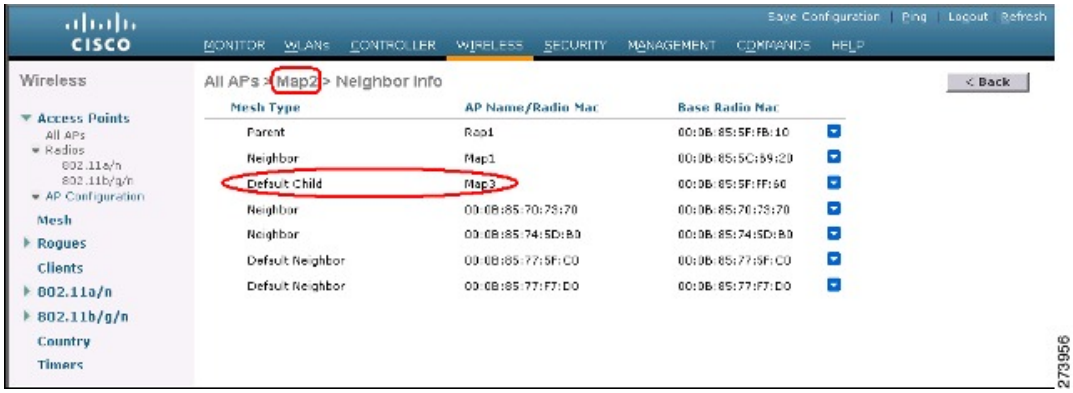


Figure 55: Neighbor Information for a Parent

Misconfiguration of the Mesh Access Point IP Address

Although most Layer 3 networks are deployed using DHCP IP address management, some network administrators might prefer the manual IP address management and allocating IP addresses statically to each mesh node. Manual mesh access point IP address management can be a nightmare for large networks, but it might make sense in small to medium size networks (such as 10 to 100 mesh nodes) because the number of mesh nodes are relatively small compared to client hosts.

Statically configuring the IP address on a mesh node has the possibility of putting a MAP on a wrong network, such as a subnet or VLAN. This mistake could prevent a mesh access point from successfully resolving the IP gateway and failing to discover a WLAN controller. In such a scenario, the mesh access point falls back

to its DHCP mechanism and automatically attempts to find a DHCP server and obtains an IP address from it. This fallback mechanism prevents a mesh node from being potentially stranded from a wrongly configured static IP address and allows it to obtain a correct address from a DHCP server on the network.

When you are manually allocating IP addresses, we recommend that you make IP addressing changes from the furthest mesh access point child first and then work your way back to the RAP. This recommendation also applies if you relocate equipment. For example, if you uninstall a mesh access point and redeploy it in another physical location of the mesh network that has a different addressed subnet.

Another option is to take a controller in Layer 2 mode with a RAP to the location with the misconfigured MAP. Set the bridge group name on the RAP to match the MAP that needs the configuration change. Add the MAP's MAC address to the controller. When the misconfigured MAP comes up in the mesh access point summary detail, configure it with an IP address.

Misconfiguration of DHCP

Despite the DHCP fallback mechanism, there is still a possibility that a mesh access point can become stranded, if any of the following conditions exist:

- There is no DHCP server on the network.
- There is a DHCP server on the network, but it does not offer an IP address to the AP, or if it gives a wrong IP address to the AP (for example, on a wrong VLAN or subnet).

These conditions can strand a mesh access point that is configured with or without a wrong static IP address or with DHCP. Therefore, you must ensure that when a mesh access point is unable to connect after exhausting all DHCP discovery attempts or DHCP retry counts or IP gateway resolution retry counts, it attempts to find a controller in Layer 2 mode. In other words, a mesh access point attempts to discover a controller in Layer 3 mode first and in this mode, attempts with both static IP (if configured) or DHCP (if possible). The AP then attempts to discover a controller in Layer 2 mode. After finishing a number of Layer 3 and Layer 2 mode attempts, the mesh access point changes its parent node and re-attempts DHCP discovery. Additionally, the software exclusion-lists notes the parent node through which it was unable to obtain the correct IP address.

Identifying the Node Exclusion Algorithm

Depending on the mesh network design, a node might find another node "best" according to its routing metric (even recursively true), yet it is unable to provide the node with a connection to the correct controller or correct network. It is the typical honeypot access point scenario caused by either misplacement, provisioning, design of the network, or by the dynamic nature of an RF environment exhibiting conditions that optimize the AWPP routing metric for a particular link in a persistent or transient manner. Such conditions are generally difficult to recover from in most networks and could blackhole or sinkhole a node completely, taking it out from the network. Possible symptoms include, but are not limited to the following:

- A node connects to the honeypot but cannot resolve the IP gateway when configured with the static IP address, or cannot obtain the correct IP address from the DHCP server, or cannot connect to a WLAN controller.
- A node ping-pongs between a few honeypots or circles between many honeypots (in worst-case scenarios).

Cisco mesh software resolves this difficult scenario by using a sophisticated node exclusion-listing algorithm. This node exclusion-listing algorithm uses an exponential backoff and advance technique much like the TCP sliding window or 802.11 MAC.

The basic idea relies on the following five steps:

1. Honeypot detection—The honeypots are first detected via the following steps:

   A parent node is set by the AWPP module by:

   - A static IP attempt in CAPWAP module.
   - A DHCP attempt in the DHCP module.
   - A CAPWAP attempt to find and connect to a controller fails.

2. Honeypot conviction—When a honeypot is detected, it is placed in a exclusion-list database with its conviction period to remain on the list. The default is 32 minutes. Other nodes are then attempted as parents in the following order, falling back to the next, upon failing the current mechanism:

   - On the same channel.
   - Across different channels (first with its own bridgegroupname and then with default).
   - Another cycle, by clearing conviction of all current exclusion-list entries.
   - Rebooting the AP.

3. Nonhoneypot credit—It is often possible that a node is not a really a honeypot, but appears to be due to some transient back-end condition, such as the following:

   - The DHCP server is either not up-and-running yet, has failed temporarily, or requires a reboot.
   - The WLAN controller is either not up-and-running yet, has failed temporarily, or requires a reboot.
   - The Ethernet cable on the RAP was accidentally disconnected.

     Such nonhoneypots must be credited properly from their serving times so that a node can come back to them as soon as possible.

4. Honeypot expiration—Upon expiration, an exclusion-list node must be removed from the exclusion-list database and return to a normal state for future consideration by AWPP.
5. Honeypot reporting—Honeypots are reported to the controller via an LWAPP mesh neighbor message to the controller, which shows these on the Bridging Information page. A message is also displayed the first-time an exclusion-listed neighbor is seen. In a subsequent software release, an SNMP trap is generated on the controller for this condition so that Cisco Prime Infrastructure can record the occurrence.

Figure 56: Excluded Neighbor

Because many nodes might be attempting to join or rejoin the network after an expected or unexpected event, a hold-off time of 16 minutes is implemented, which means that no nodes are exclusion-listed during this period of time after system initialization.

This exponential backoff and advance algorithm is unique and has the following properties:

- It allows a node to correctly identify the parent nodes whether it is a true honeypot or is just experiencing temporary outage conditions.
- It credits the good parent nodes according to the time it has enabled a node to stay connected with the network. The crediting requires less and less time to bring the exclusion-list conviction period to be very low for real transient conditions and not so low for transient to moderate outages.
- It has a built-in hysteresis for encountering the initial condition issue where many nodes try to discover each other only to find that those nodes are not really meant to be in the same network.
- It has a built-in memory for nodes that can appear as neighbors sporadically so they are not accidentally considered as parents if they were, or are supposed to be, on the exclusion-list database.

The node exclusion-listing algorithm guards the mesh network against serious stranding. It integrates into AWPP in such a way that a node can quickly reconverge and find the correct network.

Throughput Analysis

Throughput depends on packet error rate and hop count.

Capacity and throughput are orthogonal concepts. Throughput is one user's experience at node N and the total area capacity is calculated over the entire sector of N-nodes and is based on the number of ingress and egress RAP, assuming separate noninterfering channels.

For example, 4 RAPs at 10 Mbps each deliver 40 Mbps total capacity. So, one user at 2 hops out, logically under each RAP, could get 5 Mbps each of TPUT, but consume 40 Mbps of the backhaul capacity.

With the Cisco Mesh solution, the per-hop latency is less than 10 msecs, and the typical latency numbers per hop range from 1 to 3 msecs. Overall jitter is also less than 3 msecs.

Throughput depends on the type of traffic being passed through the network: User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). UDP sends a packet over Ethernet with a source and destination

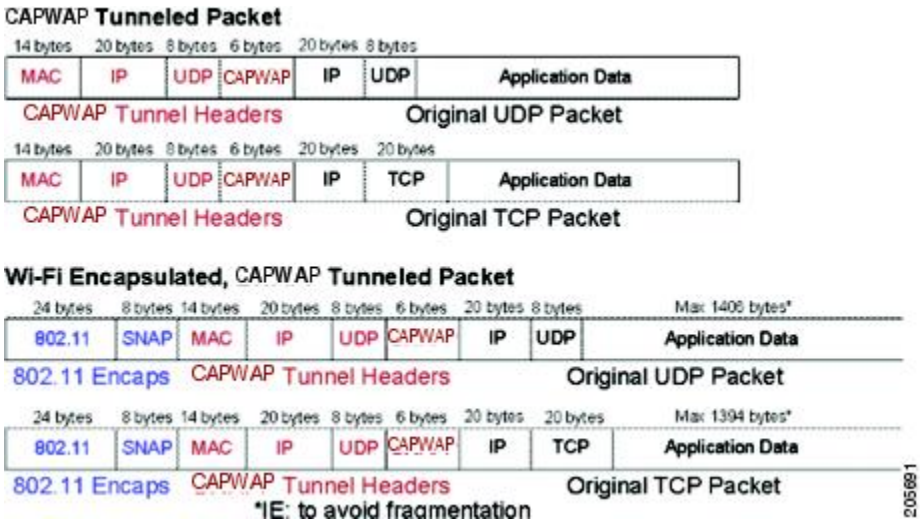
address and a UDP protocol header. It does not expect an acknowledgement (ACK). There is no assurance that the packet is delivered at the application layer.

TCP is similar to UDP but it is a reliable packet delivery mechanism. There are packet acknowledgments and a sliding window technique is used to allow the sender to transmit multiple packets before waiting for an ACK. There is a maximum amount of data the client transmits (called a TCP socket buffer window) before it stops sending data. Sequence numbers track packets sent and ensure that they arrive in the correct order. TCP uses cumulative ACKs and the receiver reports how much of the current stream has been received. An ACK might cover any number of packets, up to the TCP window size.

TCP uses slow start and multiplicative decrease to respond to network congestion or packet loss. When a packet is lost, the TCP window is cut in half and the back-off retransmission timer is increased exponentially. Wireless is subject to packet loss due to interference issues and TCP reacts to this packet loss. A slow start recovery algorithm is also used to avoid swamping a connection when recovering from packet loss. The effect of these algorithms in a lossy network environment is to lessen the overall throughput of a traffic stream.

By default, the maximum segment size (MSS) of TCP is 1460 bytes, which results in a 1500-byte IP datagram. TCP fragments any data packet that is larger than 1460 bytes, which can cause at least a 30-percent throughput drop. In addition, the controller encapsulates IP datagrams in the 48-byte CAPWAP tunnel header as shown in Figure 57: CAPWAP Tunneled Packets, on page 829. Any data packet that is longer than 1394 bytes is also fragmented by the controller, which results in up to a 15-percent throughput decrease.

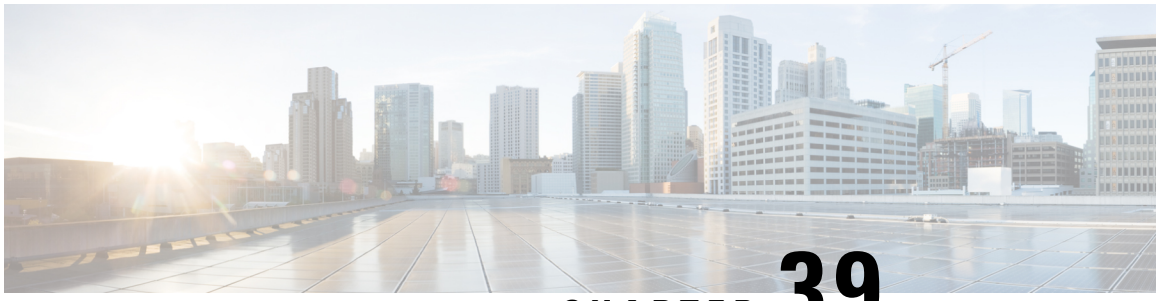
Figure 57: CAPWAP Tunneled Packets



PART VII

Client Network

- Client Traffic Forwarding Configurations, on page 833
- Quality of Service, on page 843
- WLANs, on page 887
- Per-WLAN Wireless Settings, on page 895
- WLAN Interfaces, on page 907
- WLAN Timeouts, on page 909
- WLAN Security, on page 915
- Client Roaming, on page 1017
- DHCP, on page 1031
- Client Data Tunneling, on page 1051
- AP Groups, on page 1071
- Workgroup Bridges, on page 1081
- Software-Defined Access Wireless, on page 1139



CHAPTER 39

Client Traffic Forwarding Configurations

- 802.3 Bridging, on page 833
- Bridging Link Local Traffic, on page 834
- IP-MAC Address Binding, on page 835
- TCP Adjust MSS, on page 836
- Passive Clients, on page 837

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 the destination MAC address, source MAC address, total packet length, and payload.

- By default, controllers 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 (GUI)

Procedure

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)

Procedure

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.

Bridging Link Local Traffic

This section contains the following subsections:

Configuring Bridging of Link Local Traffic (GUI)

Configure bridging of link local traffic at the local site by following these steps:

Procedure

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

Step 2 From the **Link Local Bridging** drop-down list, choose **Enabled** or **Disabled**.

Step 3 Click **Apply**.

Step 4 Click **Save Configuration**.

Configuring Bridging of Link Local Traffic (CLI)

Procedure

- Configure bridging of link local traffic at the local site by using this command:

  config network link-local-bridging {**enable** | **disable**}

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.

This section contains the following subsection:

Configuring IP-MAC Address Binding (CLI)

Procedure

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).

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?>
```

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.

Note The previously configured TCP Adjust MSS settings are carried forward when you upgrade the controller software. The default TCP Adjust MSS values are applied to new controller configurations only.

This section contains the following subsections:

Configuring TCP Adjust MSS (GUI)

Procedure

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. The recommended value is 1250.

Configuring TCP Adjust MSS (CLI)

Procedure

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. The recommended value is 1250.

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   -
```

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:

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.
- If ARP caching is enabled, APs reply to ARP requests on behalf of clients in locally-switched WLANs. If you have enabled passive clients for a WLAN and if an ARP request is received for an unknown client, the ARP packet is broadcast to all clients connected to the WLAN. However, if you have enabled AAA override for the WLAN, the ARP request for the unknown client is dropped by the AP because the AP does not have a mapping between the VLAN in which the ARP request is made and the WLAN to which the client is connected.

  Without WLAN-VLAN mapping, APs cannot find the corresponding WLAN for the VLAN of incoming ARP requests. Therefore, the APs cannot check if passive clients are enabled for the WLAN.

Configuring Passive Clients (GUI)

Before you begin

To configure passive clients, you must enable multicast-multicast or multicast-unicast mode.

Procedure

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.

Configuring Passive Clients (CLI)

Procedure

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
Controller 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, the controller reports IP conflict and sends GARP. This is not limited to two wired clients, but also to a wired client and a wireless client.

Configuring the Gratuitous ARP (GARP) Forwarding to Wireless Networks

Procedure

- To configure the gratuitous ARP (GARP) forwarding to wireless networks, enter this command:

  config advanced hotspot garp {**enable** | **disable**}

Enabling the Multicast-Multicast Mode (GUI)

Before you begin

To configure passive clients, you must enable multicast-multicast or multicast-unicast mode.

Procedure

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.

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)

Procedure

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.

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)

Procedure

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.

Multicast-to-Unicast Support for Passive Client ARPs

This feature is designed to function on the Cisco 5520 Controller. After the passive client feature is enabled on the controller, it accommodates non-Cisco WGBs so that all the traffic gets routed from the wired clients through the WGB and to the APs.

In this implementation, the broadcast ARP messages are sent to all the APs. When the Multicast-to-unicast mode is enabled on the Cisco 5520 Controller, the traffic is sent to the APs as Unicast packets using this mode.

Restrictions in Multicast-to-Unicast Support for Passive Client ARPs

- Supported on 5520 Controller only.
- A limitation of 10,000 packets per second is applied to avoid high CPU utilization.
- The passive client feature is supported on per WLAN basis.

Configuring Unicast Mode (GUI)

Procedure

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 passive-client unicast mode.

Step 3 Click **Advanced** tab.

Step 4 Check the **Passive Client** check box.

Step 5 Click **Apply**.

Step 6 Choose **Controller**.

Step 7 From the **ARP Unicast Mode** drop-down list, choose **Enable**.

Step 8 Save your configuration.

Configuring Unicast mode on Controller (CLI)

Procedure

Step 1 Enable passive client before enabling Unicast mode by entering this command:

config wlan passive-client enable *wlan-id*

Step 2 Enable Unicast packet forwarding by entering this command:

config network passive-client arp-unicast-forwarding enable

Step 3 View the status of ARP Unicast mode by entering this command:

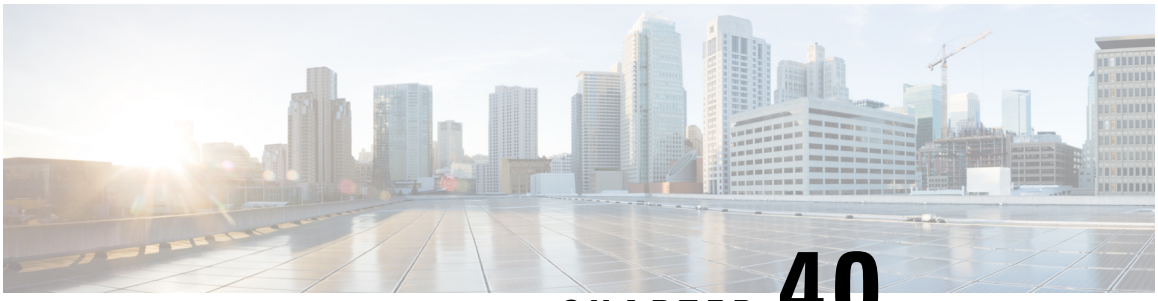
show network summary

Step 4 View the ARP statistics by entering this command:

show arp stats

Step 5 View the status of passive client by entering this command:

show wlan *wlan-id*



CHAPTER 40

Quality of Service

- Quality of Service, on page 843
- FastLane QoS, on page 856
- SIP (Media Session) Snooping, CAC, and Reporting, on page 865
- Voice and Video Parameters, on page 869
- SIP-based CAC, on page 881
- Enhanced Distributed Channel Access Parameters, on page 883

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:

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 35: 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
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 most significant 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:

Configuring QoS Profiles (GUI)

Procedure

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)

Procedure

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**}

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.

Procedure

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.

Procedure

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
...
```

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 (GUI)

Procedure

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).

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)

Procedure

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
```

QoS Map

The QoS Map feature maintains the QoS policies in situations where appropriate QoS markings that match the application type are not marked by clients or applications. The administrator gets to map the differentiated services code point (DSCP) to user priority (UP) values and also is able to mark from UP to DSCP in a controller.

With QoS in enabled state, the QoS feature is advertised by the AP in the frame. The map is propagated through a frame to a compatible device when it associates or re-associates with the network.

With QoS in disabled state, the default map is propagated to the AP and the clients from controller.

This feature is supported on all Cisco AP models.

This section contains the following subsections:

Guidelines and Restrictions for QoS Map

- You can configure QoS Map only when this feature is in disabled state.
- This feature does not function with non-801.11u supported hardware. The frames with QoS map is not sent to these clients, yet, the packets sent by these clients follow the DSCP-UP map that you have configured.
- Ensure that you configure all UP values from 0 to 7 before QoS Map is enabled.
- Ensure the DSCP range for each user priority is non-overlapping.
- Ensure the DSCP High Value is greater than or equal to the DSCP Low Value.
- You can configure up to 21 exceptions at a time.
- You must disable your network before you can enable QoS maps.
- The Trust DSCP Upstream feature does not have any dependency on the QoS Map feature. If you do not want to use any QoS Map features and want to leave it disabled, but do want to trust the upstream client DSCP markings, we recommend that you enable Trust DSCP Upstream using the CLI. Use of the CLI to enable or disable Trust DSCP Upstream circumvents the GUI restriction to disable the 802.11 networks.

Configuring QoS Map (GUI)

Before you begin

We recommend that you disable QoS Map to change the QoS map configuration. When the QoS map is disabled, the DSCP values reset to default values automatically.

Note

- To enable the QoS map after configuring the values, the following conditions must be met:
  - Configure all the UP values.
  - Do not overlap DSCP ranges for UP values. For example, if UP1 value range is 10 to 20, do not use any of the numbers within 10 and 20 for any other UP value range.

Procedure

Step 1 Disable the 802.11a/n/ac and 802.11b/g/n networks so that you can configure the QoS map.

To disable the radio networks, choose **Wireless > 802.11a/n/ac** or **802.11b/g/n > Network**, uncheck the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Step 2 Choose **Wireless** > **QoS** > **QoS Map** to open the **QoS map** page.

Step 3 To disable the QoS Map feature, perform the following steps:

a. From the **QoS Map** drop-down list, choose **Disable**.

b. To reset the DSCP Exception values, select the **Default** option.

The **Default** option resets the UP to DSCP and DSCP to UP table values to 255. This also adds DSCP UP exceptions if not present previously.

Step 4 To modify the **UP to DSCP Map**, perform the following steps:

a. From the **User Priority** drop-down list, select the value.

b. Enter the **DSCP Default**, **DSCP Start**, **DSCP End** values.

c. Click **Modify**.

Step 5 To create a DSCP exception, perform the following steps:

a. Enter the **DSCP Exception** value.

b. From the **User Priority** drop-down list, select the value.

c. Click **Add**.

Step 6 To delete a DSCP Exception, hover your cursor over the blue drop-down arrow for the DSCP Exception and click **Remove**.

Click **OK** when you are prompted to confirm your action.

Step 7 To clear the DSCP Exception list, click **Clear ALL**.

Step 8 Check or uncheck the **Trust DSCP UpStream** check box to enable or disable the marking of the upstream packets.

Step 9 To enable the QoS Map feature, choose **Enable** from the **QoS Map** drop-down list.

Step 10 Click **Apply**.

Step 11 Reenable the 802.11 networks.

To enable the radio networks, choose **Wireless > 802.11a/n/ac** or **802.11b/g/n > Network**, check the **802.11a** (or **802.11b/g**) **Network Status** check box.

Step 12 Save your configuration.

Configuring QoS Map (CLI)

Procedure

- Enable, disable or revert to default map by entering this command:

  config qos qos-map {**enable** | **disable** | **default**}

The default command resets the UP to DSCP and DSCP to UP table values to default values (255). This also adds DSCP UP exceptions if not present previously.

- Set DSCP range for UP by entering this command:

  config qos qosmap up-to-dscp-map *up dscp-default dscp-start dscp-end*

  You can run the above command in the following situations:

  - Clients are QoS map supportive and marks the DSCP or UP with unusual value and the clients
  - Clients are not QoS map supportive, then this allows the administrator to map particular UP to DSCP upstream and downstream of Client Packets

- Set an exception for DSCP by entering this command:

  config qos qosmap dscp-up-to-exception *dscp up*

  You can run the above command in situations when the client marks DSCP with an unusual value.

- Delete a specific DSCP exception by entering this command:

  config qos qosmap delete-dscp-exception *dscp*

  You can run the above command in situations when specific exceptions are to be deleted from the QoS map.

- Delete all exceptions by entering this command:

  config qos qosmap clear-all

  You can run the above command in a situation where all the values needs to be cleared from the map.

- Enable or disable marking of the upstream packets using the client DSCP by entering this command:

  config qos qosmap trust-dscp-upstream {**enable** | **disable** }

  You can run the above command in situations where the client marks DSCP and not UP, or marks UP to an unusual value. When in enabled state, it will use the DSCP to mark the upstream packets at AP instead of UP

- See the QoS mapping configuration by entering this command:

  show qos qosmap

FastLane QoS

Configuring Fastlane QoS (CLI)

The Fastlane QoS feature provides increased quality of service (QoS) treatment for iOS 10 or higher clients. This feature is disabled by default.

Note You should enable or disable this feature only during a maintenance window when not many clients are connected, as there will be a disruption in service when all the WLANs and the network are disabled and enabled again.

Restrictions on Fastlane QoS

- When Flex Local switching is enabled on the WLAN, default Flex AVC profile is not created and mapped to the WLAN, unlike AUTOQOS-AVC-PROFILE, which is created for central switching and mapped to a WLAN.

Enabling Fastlane QoS per WLAN

To enable the Fastlane QoS feature per WLAN, use **config qos fastlane enable** *wlan_id* command.

When you run the **config qos fastlane enable** *wlan_id* command, fastlane is activated on the target WLAN, which enables supporting iOS 10 devices to activate a QoS allowed list in their profile, if present. The command also runs the commands listed in the following table.

Note If the commands are executed, then Fastlane QoS feature is enabled and applied to the target WLAN. If a command that is associated with the Fastlane QoS feature fails while is being enabled on a WLAN, all the changes will be reverted to their original values, except for QoS map. The QoS map value will revert to the default value instead of the previously configured value. Also, the new AVC Profile will not be deleted; it will only be removed from the WLAN.

Table 36: Commands Executed for Enabling Fastlane QoS

Description	Commands
Temporarily disables 802.11a and 802.11b networks and WLANs.	• **config 802.11a disable network** • **config 802.11b disable network** • **config wlan disable all**
Configures the Platinum QoS profile to set unmarked (best effort) unicast packets, and multicast packets, to best effort over wifi link.	• **config qos priority platinum voice besteffort besteffort**
Disables 802.1p marking (all wired marking is DSCP-based).	• **config qos protocol-type platinum none**
Disables bandwidth limitation for UDP traffic.	• **config qos average-realtime-rate platinum per-ssid downstream 0**
Disables bandwidth limitation for UDP bursts.	• **config qos burst-realtime-rate platinum per-ssid downstream 0**

Description	Commands
Enables ACM for 5 GHz and 2.4 GHz.	• **config 802.11a cac voice acm enable** • **config 802.11b cac voice acm enable**
Limits allocation for voice traffic to 50 percent of available bandwidth on any 5 GHz or 2.4 GHz radio.	• **config 802.11a cac voice max-bandwidth 50** • **config 802.11b cac voice max-bandwidth 50**
Allocates 6 percent of the bandwidth to voice users for roaming.	• **config 802.11a cac voice roam-bandwidth 6** • **config 802.11b cac voice roam-bandwidth 6**
Sets the EDCA parameters to their values recommended by 802.11-2017.	• **config advanced 802.11b edca-parameter fastlane** • **config advanced 802.11a edca-parameter fastlane**
Enables expedited bandwidth for 5 GHz and 2.4 GHz.	• **config 802.11a exp-bwreq enable** • **config 802.11b exp-bwreq enable**
Configures the user priority (UP) to differentiated services code point (DSCP) maps.	• **config qos qosmap disable** • **config qos qosmap default** • **config qos qosmap up-to-dscp-map 0 0 0 7** • **config qos qosmap up-to-dscp-map 1 8 8 15** • **config qos qosmap up-to-dscp-map 2 16 16 23** • **config qos qosmap up-to-dscp-map 3 24 24 31** • **config qos qosmap up-to-dscp-map 4 32 32 39** • **config qos qosmap up-to-dscp-map 5 34 40 47** • **config qos qosmap up-to-dscp-map 6 46 48 62** • **config qos qosmap up-to-dscp-map 7 56 63 63** • **config qos qosmap clear all**

Description	Commands
Configures DSCP-to-UP mapping exceptions.	• **config qos qosmap dscp-to-up-exception 56 0** • **config qos qosmap dscp-to-up-exception 48 0** • **config qos qosmap dscp-to-up-exception 46 6** • **config qos qosmap dscp-to-up-exception 44 6** • **config qos qosmap dscp-to-up-exception 40 5** • **config qos qosmap dscp-to-up-exception 38 4** • **config qos qosmap dscp-to-up-exception 36 4** • **config qos qosmap dscp-to-up-exception 34 4** • **config qos qosmap dscp-to-up-exception 32 5** • **config qos qosmap dscp-to-up-exception 30 4** • **config qos qosmap dscp-to-up-exception 28 4** • **config qos qosmap dscp-to-up-exception 26 4** • **config qos qosmap dscp-to-up-exception 24 4** • **config qos qosmap dscp-to-up-exception 22 3** • **config qos qosmap dscp-to-up-exception 20 3** • **config qos qosmap dscp-to-up-exception 18 3** • **config qos qosmap dscp-to-up-exception 16 0** • **config qos qosmap dscp-to-up-exception 14 2** • **config qos qosmap dscp-to-up-exception 12 2** • **config qos qosmap dscp-to-up-exception 10 2** • **config qos qosmap dscp-to-up-exception 8 1**
Enables DSCP-Trust (new QoS maps).	• **config qos qosmap trust-dscp-upstream enable** • **config qos qosmap enable**
Creates the Application Visibility and Control (AVC) profile.	• **config avc profile AUTOQOS-AVC-PROFILE create**

Description	Commands
Configures AVC to mark voice applications and subcomponents to expedited forwarding (EF) (DSCP 46).	• **config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-phone-audio mark 46** • **config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-jabber-audio mark 46** • **config avc profile AUTOQOS-AVC-PROFILE rule add application ms-lync-audio mark 46** • **config avc profile AUTOQOS-AVC-PROFILE rule add application citrix-audio mark 46**
Configures AVC to mark multimedia conferencing applications to assured forwarding (AF) 41 (DSCP 34).	• **config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-phone-video mark 34** • **config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-jabber-video mark 34** • **config avc profile AUTOQOS-AVC-PROFILE rule add application ms-lync-video mark 34** • **config avc profile AUTOQOS-AVC-PROFILE rule add application webex-media mark 34**
Configures AVC to mark multimedia streaming applications to AF31 (DSCP 26).	• **config avc profile AUTOQOS-AVC-PROFILE rule add application citrix mark 26** • **config avc profile AUTOQOS-AVC-PROFILE rule add application pcoip mark 26** • **config avc profile AUTOQOS-AVC-PROFILE rule add application vnc mark 26** • **config avc profile AUTOQOS-AVC-PROFILE rule add application vnc-http mark 26**
Configures AVC to mark signaling protocols to CS3 (DSCP 24).	• **config avc profile AUTOQOS-AVC-PROFILE rule add application skinny mark 24** • **config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-jabber-control mark 24** • **config avc profile AUTOQOS-AVC-PROFILE rule add application sip mark 24** • **config avc profile AUTOQOS-AVC-PROFILE rule add application sip-tls mark 24**

Description	Commands
Configures AVC to mark transactional data applications to AF21 (DSCP 18).	• **config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-jabber-im mark 18** • **config avc profile AUTOQOS-AVC-PROFILE rule add application ms-office-web-apps mark 18** • **config avc profile AUTOQOS-AVC-PROFILE rule add application salesforce mark 18** • **config avc profile AUTOQOS-AVC-PROFILE rule add application sap mark 18**
Configures AVC to mark OAM applications to CS2 (DSCP 16).	• **config avc profile AUTOQOS-AVC-PROFILE rule add application dhcp mark 16** • **config avc profile AUTOQOS-AVC-PROFILE rule add application dns mark 16** • **config avc profile AUTOQOS-AVC-PROFILE rule add application ntp mark 16** • **config avc profile AUTOQOS-AVC-PROFILE rule add application snmp mark 16**
Configures AVC to mark bulk data applications marking to AF11 (DSCP 10).	• **config avc profile AUTOQOS-AVC-PROFILE rule add application ftp mark 10** • **config avc profile AUTOQOS-AVC-PROFILE rule add application ftp-data mark 10** • **config avc profile AUTOQOS-AVC-PROFILE rule add application ftps-data mark 10** • **config avc profile AUTOQOS-AVC-PROFILE rule add application cifs mark 10**
Configures AVC to mark scavenger applications to CS1 (DSCP 8).	• **config avc profile AUTOQOS-AVC-PROFILE rule add application netflix mark 8** • **config avc profile AUTOQOS-AVC-PROFILE rule add application youtube mark 8** • **config avc profile AUTOQOS-AVC-PROFILE rule add application skype mark 8** • **config avc profile AUTOQOS-AVC-PROFILE rule add application bittorrent mark 8**
Applies the platinum QoS profile to the WLAN.	• **config wlan qos** *wlan_id* **platinum**

Description	Commands
Applies the AVC profile AUTOQOS-AVC-PROFILE to the WLAN ID *wlan-id* if AVC visibility is enabled on the WLAN.	• **config wlan avc** *wlan_id***profile AUTOQOS-AVC-PROFILE enable**
Re-enables 802.11a and 802.11b networks and WLANs.	• **config 802.11a enable network** • **config 802.11b enable network** • **config wlan enable all**

Disabling Fastlane QoS in WLANs

To disable Fastlane QoS in WLANs, use the **config qos fastlane disable** *wlan_id* command.

When you disable fastlane for a target WLAN, supporting iOS 10 devices stop using a QoS allowed list for that WLAN. Disabling fastlane for a target WLAN also returns the WLAN configuration to QoS defaults as per the following table.

Note When the Fastlane QoS feature is disabled per WLAN, all the values will revert to the default state, except the WLAN status, which moves to the previous state.

While disabling Fastlane QoS in WLANs, if media stream is enabled, it will be disabled before enabling a Silver profile to QoS.

Table 37: Commands Executed for Disabling Fastlane QoS in WLAN

Description	Commands
Disables the WLANs to make changes to WLAN configuration. **Note** If Call Snooping and KTS are enabled, then they will be disabled.	• **config wlan disable** *wlan_id*
Applies the Silver (default) QoS profile to the WLAN .	• **config wlan qos** *wlan_id* **silver**
Removes the AVC profile AUTOQOS-AVC-PROFILE from the WLAN ID *wlan-id*, if attached.	• **config wlan avc** *wlan_id* **profile AUTOQOS-AVC-PROFILE disable**
Reverts the WLAN to the earlier state (if WLAN was in Enabled state before, it will revert to Enabled state and if WLAN was in Disabled state, it will revert to Disabled state).	• **config wlan enable** *wlan_id*

Disabling Fastlane QoS Globally

To disable Fastlane QoS globally, use the **config qos fastlane disable global** command.

When the Fastlane QoS feature is disabled globally, the controller QoS configuration will be reverted back to the default values shown in the following table.

Note Fastlane QoS must be disabled on all the WLANs before **config qos fastlane disable global** command is executed.

If a command associated with the Fastlane QoS feature fails while the command is being enabled globally, all the changes will be reverted to their original values, except QoS map, whose value is reverted to the default, instead of the previously configured value.

Table 38: Commands Executed for Disabling Fastlane QoS Globally

Description	Commands
Temporarily disable 802.11a and 802.11b networks to make changes to QoS Profiles.	• **config 802.11a disable network** • **config 802.11b disable network**
Disable all the WLANs to make changes to QoS profile.	• **config wlan disable all**
Reverts the Platinum QoS profile to the default QoS configuration.	• **config qos priority platinum voice voice voice** • **config qos protocol-type platinum none** • **config qos average-realtime-rate platinum per-ssid downstream 0** • **config qos burst-realtime-rate platinum per-ssid downstream 0**
Disables ACM for 2.4 GHz and 5 GHz. Also, reverts Video CAC to its defaults.	• **config 802.11a cac voice acm disable** • **config 802.11b cac voice acm disable** • **config 802.11a cac video max-bandwidth 5** • **config 802.11b cac video max-bandwidth 5**
Limits voice traffic to the default of the total bandwidth for 2.4 GHz and 5 GHz.	• **config 802.11a cac voice max-bandwidth 75** • **config 802.11b cac voice max-bandwidth 75**
Reverts roaming bandwidth for voice users to its default values.	• **config 802.11a cac voice roam-bandwidth 6** • **config 802.11b cac voice roam-bandwidth 6**

Description	Commands
Reverts the EDCA parameters to their defaults.	• **config advanced 802.11b edca-parameter wmm-default** • **config advanced 802.11a edca-parameter wmm-default**
Disables the expedited bandwidth for 2.4 GHz and 5 GHz.	• **config 802.11a exp-bwreq disable** • **config 802.11b exp-bwreq disable**
Disables the UP-to-DSCP maps.	• **config qos qosmap disable** • **config qos qosmap default**
Re-enable the 802.11a and 802.11b networks.	• **config 802.11a enable network** • **config 802.11b enable network**
Reverts the WLAN to the earlier state (if WLAN was in Enabled state before, it will revert to Enabled state and if WLAN was in Disabled state, it will revert to Disabled state.)	**config wlan enable *wlan-id***

Configuring Fastlane QoS (GUI)

Procedure

Step 1 Select **WLANs** to open the **WLANs** window.

Step 2 Select **QoS** to open the **WLANs > Edit** window.

Step 3 From the **Fastlane** drop-down, enable or disable Fastlane QoS.

Step 4 Click **Apply** to save your settings.

Disabling Fastlane QoS Globally (GUI)

Procedure

Step 1 Choose **Wireless > Advanced > QoS >Fastlane** to open the **Fastlane Configuration** window.

Step 2 Click **Apply** at the Revert Fastlane AutoQoS global parameters to defaults to disable Fastlane globally.

SIP (Media Session) Snooping, CAC, 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 SIP (Media Session) Snooping, CAC, and Reporting

SIP snooping is not supported in FlexConnect in Release 8.5 and later releases.

Configuring Media Session Snooping (GUI)

Procedure

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)

Procedure

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 39: 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.
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.

Error Code	Integer	Description
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.
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.

Error Code	Integer	Description
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.
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.

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 access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. It works by rejecting requested calls (traffic streams) if the channel lacks the capacity to service the request. It requires that WMM be enabled on the WLAN. CAC is also known as ACM (Admission Control).

The following two types of CAC are available:

- Load-based CAC (recommended): All channel utilization (QBSS) is considered, including interference and noise, as well as AP traffic.
- Static CAC: Only the traffic to and from this AP is considered when evaluating the channel's capacity.

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.

This section contains the following subsections:

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 833 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 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 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.

Table 40: TSPEC Request Handling Examples

CAC Mode	Reserved bandwidth for voice calls	Usage	Normal TSPEC Request	TSPEC with Expedited 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

[5] 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.

[6] 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.

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)

Procedure

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, 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. The **Voice** tab is displayed by default.

Step 4 (Optional) Check 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** field, 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** field, 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, check the **Expedited Bandwidth** check box. By default, this field is disabled.

Step 9 To enable SIP CAC support, check 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)** field, enter the bandwidth in kilobits per second.

The possible range is 8 to 64.

The default value is 64.

Note
The **SIP Bandwidth (kbps)** field 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)** field is set to 64. If you choose the SIP codec as G.729, the SIP Bandwidth (kbps) field is set to 8.

Step 12 In the **SIP Voice Sample Interval (msecs)** field, enter the value for the sample interval.

Step 13 In the **Maximum Calls** field, 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 Check 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, check 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.

Procedure

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 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.

Step 13 Configure voice automatically for a WLAN by entering this command:

config auto-configure voice cisco *wlan-id* **radio** {**802.11a** | **802.11b** | **all**}

Step 14 Enter the **save config** command to save your settings.

Configuring Video Parameters

Configuring Video Parameters (GUI)

Procedure

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.

Procedure

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)

Procedure

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)

Procedure

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.

SIP-based CAC

This section contains the following subsections:

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.

Procedure

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)

Procedure

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**}

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)

Procedure

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. The WMM option is default and we recommend this setting if you have SpectraLink phones deployed in your network.
- **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 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. This setting is not recommended because it is deprecated.

  Note
  If you deploy video services, admission control must be disabled.

- **Fastlane**—Enables fastlane EDCA parameters. This setting is recommended for use with Apple client devices.

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

Step 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)

Procedure

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 |fastlane**}

- **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.

- **Fastlane**—Enables Fast Lane EDCA parameters.

Step 4 View the current status of MAC (low latency 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**}

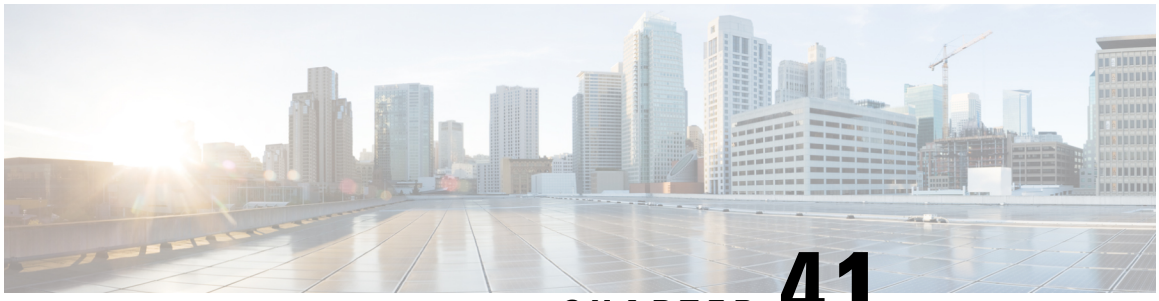
Note
The low latency MAC option is not supported.

This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight APs. This, in turn 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 41

WLANs

- Information About WLANs, on page 887
- Prerequisites for WLANs, on page 887
- Restrictions for WLANs, on page 888
- Creating and Removing WLANs (GUI), on page 888
- Enabling and Disabling WLANs (GUI), on page 890
- Editing WLAN SSID or Profile Name for WLANs (GUI), on page 890
- Creating and Deleting WLANs (CLI), on page 890
- Enabling and Disabling WLANs (CLI), on page 891
- Editing WLAN SSID or Profile Name for WLANs (CLI), on page 892
- Viewing WLANs (CLI), on page 892
- Searching WLANs (GUI), on page 892
- Assigning WLANs to Interfaces, on page 893

Information About WLANs

This feature enables you to control WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All access points can advertise up to 16 WLANs. However, you can create up to 4096 WLANs and then selectively advertise these WLANs (using profiles and tags) to different APs for better manageability.

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.

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.

  For more information about access point groups, see the *AP Groups* chapter.

- Controllers use different attributes to differentiate between WLANs with the same Service Set Identifier (SSID):

- WLANs with the same SSID and same Layer 2 policy cannot be created if the WLAN ID is lower than 17.
- Two WLANs with IDs that are greater than 17 and that have the same SSID and same Layer 2 policy are allowed if WLANs are added in different AP groups.

- We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that client traffic is kept separate from management traffic.

Restrictions for WLANs

- 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. For central switched WLAN, the profile name can be of 32 characters.
- Peer-to-peer blocking does not apply to multicast traffic.
- 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 VLAN0, and you cannot map VLANs 1002 to 1006.
- When creating a WLAN with the same SSID, you must create a unique profile name for each WLAN.
- When multiple WLANs with the same SSID get assigned to the same AP radio, you must have a unique Layer 2 security policy so that clients can safely select between them.
- Starting with Release 8.9, it is possible to delete a WLAN even if it is mapped to a MAC filter profile or a net user. However, after the WLAN is deleted, the user entries are retained. Prior to Release 8.9, it was not possible to delete a WLAN that is mapped to a MAC filter profile or a net user.
- All leading spaces in the profile and SSID names get truncated to one leading space. The truncation of leading spaces is an XML format limitation. Hence the truncation occurs during the controller's XML configuration file upload or download procedure on all AireOS controller releases.

Creating and Removing WLANs (GUI)

Procedure

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** field, 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** field, 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.

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, check 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)

Procedure

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**.

Editing WLAN SSID or Profile Name for WLANs (GUI)

Procedure

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.

Step 2 To edit the a WLAN profile or SSID, click the WLAN ID link in the **WLANs > Edit** page.

- In the **Profile Name** field, edit the WLAN profile name.
- In the **WLAN SSID** field, edit the WLAN SSID.

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

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

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.
- 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.

Editing WLAN SSID or Profile Name for WLANs (CLI)

- Edit a profile name or SSID associated to a WLAN:
  - Disable the WLAN first before changing the profile name or SSID by entering this command:

    config wlan disable *wlan_id*
  - Rename the WLAN profile name or SSID by entering this command:

    config wlan ssid *wlan_id ssid*

    config wlan profile *wlan_id profile-name*
- View the WLANs configured on the controller by entering this command:

  show wlan summary

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)

Procedure

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, check the **Profile Name** check box and enter the desired profile name in the edit box.
- To search for WLANs based on SSID, check the **SSID** check box and enter the desired SSID in the edit box.
- To search for WLANs based on their status, check 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:

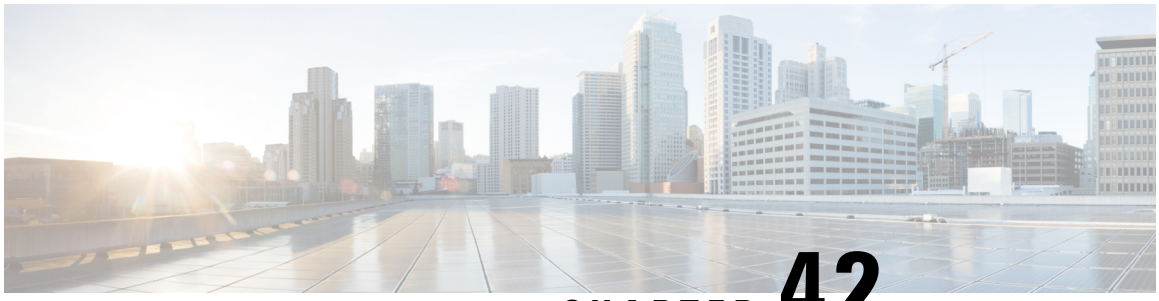
- Assign a WLAN to an interface by entering this command:

  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.



CHAPTER 42

Per-WLAN Wireless Settings

- DTIM Period, on page 895
- Cisco Client Extensions, on page 897
- Client Profiling, on page 898
- Client Count per WLAN, on page 902
- Limit Clients per WLAN per AP Radio, on page 904
- Disabling Coverage Hole Detection per WLAN, on page 905

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)

Procedure

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 Uncheck 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 Check the **Status** check box to reenable the WLAN.

Step 10 Click **Save Configuration**.

Configuring the DTIM Period (CLI)

Procedure

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*

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:

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.

Configuring CCX Aironet IEs (GUI)

Procedure

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 Check 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.

Procedure

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*

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

Information about Custom HTTP Port Profiling

This feature is designed to enable the controller to identify and profile clients connecting from ports apart from HTTP port 80.

This section contains the following subsections:

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.
- When local profiling is enabled, RADIUS profiling is not allowed on a 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 occur 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 because 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.
- This feature supports HTTP profiling based on custom HTTP port and only one custom HTTP port can be configured.

Configuring Client Profiling (GUI)

Procedure

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 HTTP, check 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 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**}

Configuring Custom HTTP Port for Profiling (GUI)

Note The HTTP port 80 is always open for gathering HTTP profiling data, irrespective of the custom HTTP port configuration.

Procedure

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

Step 2 Enter the port value under **HTTP Profiling Port** field.

Configuring Custom HTTP Port for Profiling (CLI)

Procedure

Step 1 Configure custom HTTP port by entering this command:

config network profiling http-port *port number*

The default port value is 80.

Step 2 View the configured HTTP profiling port and other inband connectivity settings by entering this command:

show network summary

The network configuration is displayed.

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 3000 total clients and these clients can be shared between enterprise users (employees) and guest users, so you can limit the guest WLAN to 500 clients. The number of clients that you can configure for each WLAN depends on the platform that you are using. Additionally, you can set a limit on the number of clients in a given WLAN that can associate to each AP's radio. For example, each radio supports up to 200 associations, but a guest WLAN may be configured for a maximum of 10 associations per radio.

This section contains the following subsections:

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.

Configuring the Client Count per WLAN (GUI)

Procedure

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)

Procedure

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)

Procedure

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)

Procedure

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.

Limit Clients per WLAN per AP Radio

Limit Clients per WLAN per AP Radio (GUI)

- With the AP in Local mode, the controller validates the association request of all clients. The controller drops a client association request if the configured limit has been reached.
- With the AP in FlexConnect mode, both connected (local or central switching, local or central authentication) and standalone mode (local switching, local authentication), the AP validates the client admission in the authentication or reassociation phase.

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the WLAN ID.

Step 3 On the **WLANs > Edit** page, click the **Advanced** tab.

Step 4 In the **Maximum Allowed Clients** field, enter the maximum number of clients that can be allowed to join the WLAN.

Note
If you enter a value of 0, this means that there is no restriction on the number of clients that are allowed to join the WLAN.

Step 5 In the **Maximum Allowed Clients Per AP Radio** field, enter the maximum number of clients that can be allowed to join the WLAN per AP radio.

Valid range is between 1 to 200 clients.

Step 6 Save the configuration.

Limit Clients per WLAN per AP Radio (CLI)

- With the AP in Local mode, the controller validates the association request of all clients. The controller drops a client association request if the configured limit has been reached.
- With the AP in FlexConnect mode, both connected (local or central switching, local or central authentication) and standalone mode (local switching, local authentication), the AP validates the client admission in the authentication or reassociation phase.

Procedure

Step 1 Configure the maximum number of clients that can be allowed to join the WLAN per AP radio by entering this command:

config wlan max-radio-clients *max-clients wlan-id*

Step 2 View the client information by entering these commands:

- On the controller console—**show client summary**
- On the Cisco Wave 2 AP console—**show dot11 clients**

Step 3 Enable debugging on the Cisco Wave 2 AP console by entering these commands:

- Enable 802.11 event level debugging—**debug dot11 events**
- Enable 802.11 information level debugging—**debug dot11 info**

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)

Procedure

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.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Disabling Coverage Hole Detection on a WLAN (CLI)

Procedure

Step 1 Disable coverage hole detection on a by entering this command:

config wlan chd *wlan-id* **disable**

Step 2 Save your settings by entering this command:

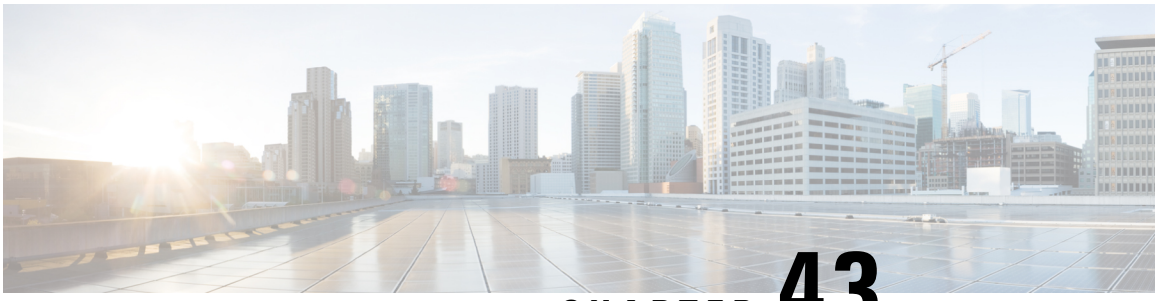
save config

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 43

WLAN Interfaces

- Multicast VLAN, on page 907

Multicast VLAN

If VLAN groups are in use, we recommend that you enable multicast VLAN to limit multicast on the air to a single copy on a predefined multicast VLAN.

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 VLAN 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.

If the WLAN is anchored, then the interface mapping at the anchored side is used for client connections. For anchored guest WLANs, it is a best practice to use a *black hole* dynamic interface at the foreign controller. For more information, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-6/b_Cisco_Wireless_LAN_Controller_Configuration_Best_Practices.html#concept_331FB2E819654D62BC998FF00BFA3FF3

This section contains the following subsections:

Configuring a Multicast VLAN (GUI)

Procedure

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.

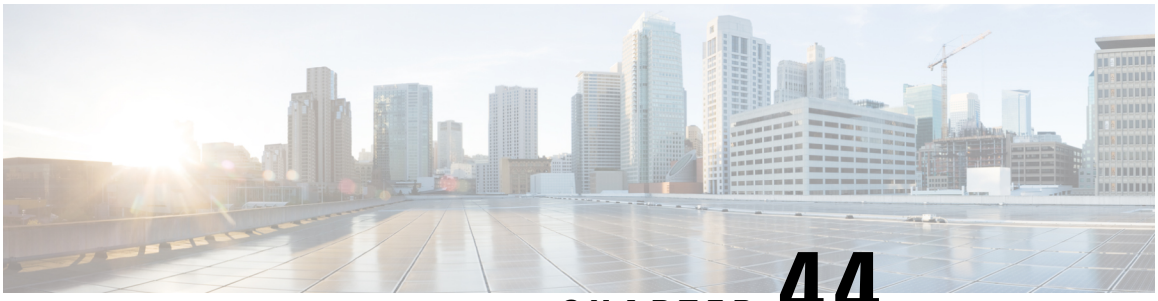
The Multicast Interface drop-down list appears.

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.



CHAPTER 44

WLAN Timeouts

- Client Exclusion Timeout, on page 909
- Session Timeouts, on page 909
- User Idle Timeout, on page 911
- User Idle Timeout per WLAN, on page 912
- Address Resolution Protocol Timeout, on page 913

Client Exclusion Timeout

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.

You can also enable or disable client exclusion on a per-WLAN basis. If enabled, you can configure the duration of the exclusion period. The activities that trigger client exclusion are configured globally.

Configuring Client Exclusion Timeout (CLI)

Procedure

- Configure the timeout for disabled clients by entering this command: command:

  config wlan exclusionlist *wlan-id timeout*

  The valid timeout range is between 1 and 2147483647 seconds. A value of 0 permanently disables the client.

- Verify the current timeout by entering this command:

  show wlan

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 802.1X 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 802.1X 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 client's PMK cache does not change to reflect the new session time out value.

Procedure

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)

Procedure

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 for WLANs that use 802.1X (EAP) security is 1800 seconds. For all other Layer 2 security types, the default value is 0 seconds.

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
```

User Idle Timeout

Configuring User Idle Timeout (GUI)

This configuration is applicable to all the WLAN profiles on the controller. You can also choose to configure the user idle timeout on a per-WLAN basis. The per-WLAN configuration overrides the global configuration.

Procedure

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

Step 2 In the **User Idle Timeout** field, enter the timeout value, in seconds. The valid range is 15 to 100000 seconds. The default value is 300 seconds.

Step 3 Save the configuration.

Configuring User Idle Timeout (CLI)

This configuration is applicable to all the WLAN profiles on the controller. You can also choose to configure the user idle timeout on a per-WLAN basis. The per-WLAN configuration overrides the global configuration.

Procedure

- Configure user idle timeout for all the WLAN profiles on the controller by entering this command:

config network useridletimeout *timeout -in-seconds*

The valid range is 15 to 100000 seconds. The default value is 300 seconds.

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 (GUI)

The WLAN configuration overrides the global timeout configuration.

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN.

Step 3 On the **WLANs > Edit** window, click the **Advanced** tab.

Step 4 Check the **Client user idle timeout** check box and enter a timeout value, in seconds. The valid range is 15 to 100000 seconds. The default value is 300 seconds.

Step 5 In the **Client user idle threshold** field, enter a threshold value, in bytes. This configures the threshold data sent by the client during the idle timeout for client sessions for the WLAN. If the client sends traffic less than the defined threshold, the client is removed upon timeout. The valid range for the threshold is 0 to 10000000 bytes. The default value is 0 bytes.

Step 6 Save the configuration.

Configuring Per-WLAN User Idle Timeout (CLI)

The WLAN configuration overrides the global timeout configuration.

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*

Address Resolution Protocol Timeout

The Address Resolution Protocol (ARP) timeout is used to delete ARP entries on controller for devices learned from the network.

There are four types of ARP entries:

- Normal type: Displayed as *Host* on the CLI
- Mobile client type: Displayed as *Client* on the CLI
- Permanent type: Displayed as *Permanent* on the CLI
- Remote type: Displayed as *Client* on the CLI

Only the Normal type ARP entry can be deleted. The other three entries cannot be deleted using the ARP timeout feature.

This section contains the following subsections:

Configuring ARP Timeout (GUI)

Procedure

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

Step 2 In the **ARP Timeout** field, enter the timeout value in seconds. By default, the timeout is set to 300 seconds; valid range is 10 to 2147483647 seconds.

Step 3 Save the configuration.

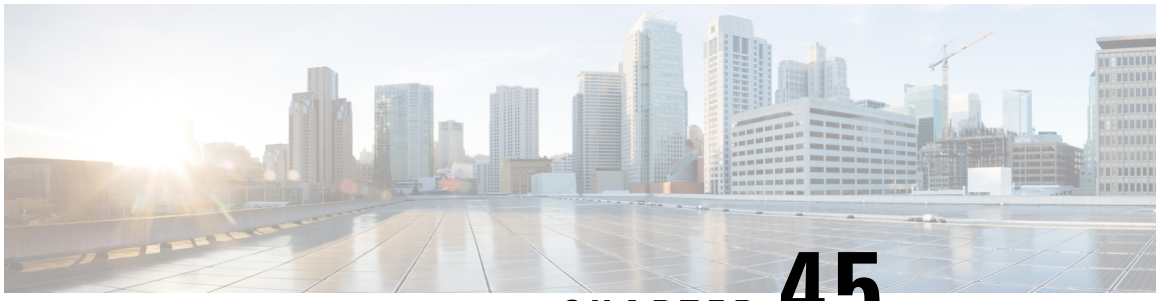
Configuring ARP Timeout (CLI)

Procedure

- Configure the ARP timeout value by entering this command:

  config network arptimeout *value-in-seconds*

  The default value is 300 seconds; the valid range is 10 to 2147483647 seconds.



CHAPTER 45

WLAN Security

- Layer 2 Security, on page 915
- Layer 3 Security, on page 935
- EAP and AAA Servers, on page 964
- Advanced WLAN Security, on page 985

Layer 2 Security

This section contains the following subsections:

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)

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.

MAC Filtering with Centrally Authenticated WLANs

After the initial 802.11 authentication exchange between the AP and the clients, the AP sends the client association request in CAPWAP to the controller. If the controller is using a local MAC filter list, it will immediately send a successful or failed association response. If external RADIUS is used, the controller sends an Access-Request to the AAA server, and based on the response from RADIUS, sends its association response to the client.

Note Wireless clients may time out their wait for association response within as little as 300 ms. Therefore, if you use an external RADIUS server with MAC filtering, ensure that the server responds within this timeframe.

Restrictions for MAC Filtering

- MAC filtering cannot be configured for Guest LANs.
- 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.

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.

Local MAC Filters

Controllers have built-in MAC filtering capability, similar to that provided by a RADIUS authorization server.

Prerequisites for Configuring Local MAC Filters

You must have AAA enabled on the WLAN to override the interface name.

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.

Protected Management Frames (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. They 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 an AP.

The 802.11w protocol applies only to a set of robust management frames 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:

Restrictions for Protected Management Frames (802.11w)

- With PMF settings set to Optional or Enabled, a wireless client may intermittently fail temporarily to reassociate to an access point. This impact will be mitigated by enabling **Fast Transition Over the Air**, and by setting the **PMF Comeback Timer** value to 1 second.
- The 802.11w standard is not supported .
- 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.

Configuring Protected Management Frames (802.11w) (GUI)

Procedure

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**.

Related Topics

Configuring Infrastructure MFP (GUI), on page 574

Configuring Protected Management Frames (802.11w) 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**}

Related Topics

Configuring Infrastructure MFP (CLI), on page 575

Fast Secure Roaming

802.11r Fast Transition

802.11r, which is the IEEE standard and generally recommended in order to speed roaming when using EAP, 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).

From Release 8.0, you can create an 802.11r WLAN that is also an WPAv2 WLAN. In earlier releases, you had to create separate WLANs for 802.11r and for normal security. Non-802.11r clients can now join 802.11r-enabled WLANs as the 802.11r WLANs can accept non-802.11r associations. If clients do not support mixed mode or 802.11r join, they can join non-802.11r WLANS. When you configure FT PSK and later define PSK, clients that can join only PSK can now join the WLAN in mixed mode.

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.

Note Over-the-Air is the preferred and recommended method compared to the Over-the-DS method.

Figure 58: 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.

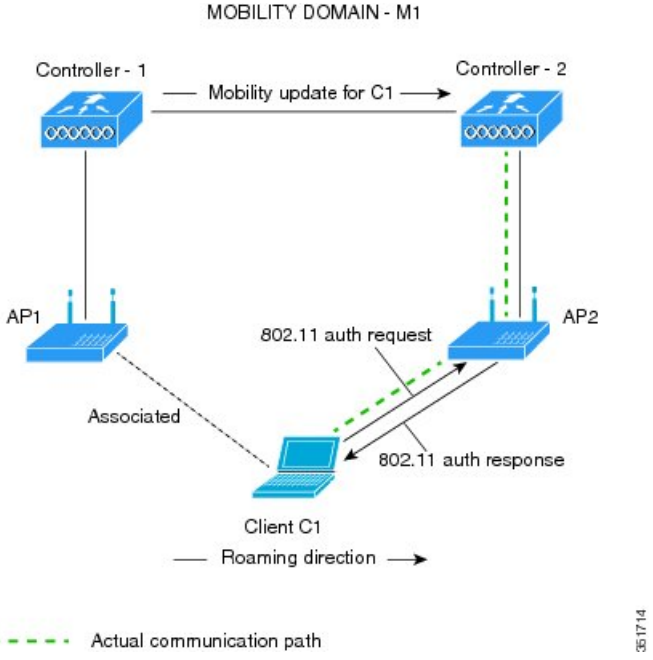
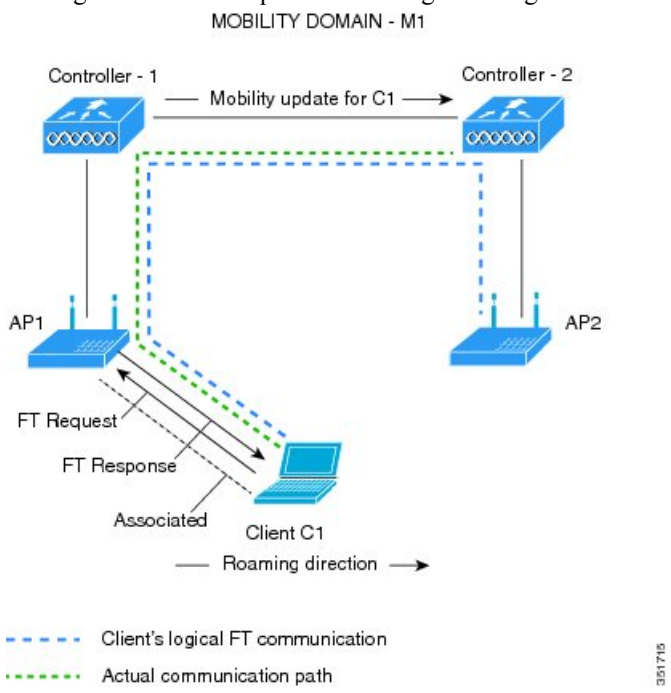


Figure 59: Message Exchanges when Over the DS client roaming is configured

This figure shows the sequence of message exchanges that occur when Over the DS client roaming is configured.



This section contains the following subsections:

Restrictions for 802.11r Fast Transition

- This feature is not supported on mesh access points.
- In 8.1 and earlier releases, this feature is not supported on access points in FlexConnect mode. In Release 8.2, this restriction is removed.
- 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.
- 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 controller 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.
- It is not possible to enable WPA1 encryption along with Fast Transition on a WLAN using the controller GUI. The workaround is to configure it using the controller CLI. For more information, see https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvp05137.
- 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.

  802.11i Opportunistic Key Caching (Proactive Key Caching) is supported only by Microsoft Windows clients. It is always enabled and cannot be disabled.

  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 controller allows a maximum of three Fast Transition handshakes with different APs.
- Disable the fast transition padding option for keys setting in the client to prevent the client from getting de-authenticated from an SSID with 802.11r Fast Transition enabled.
- 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.

Configuring 802.11r Fast Transition (GUI)

Procedure

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 Uncheck the **Over the DS** check box to enable Fast Transition Over the Air.

Fast Transition Over the Air is the recommended configuration for this feature.

This option is available only if you enable Fast Transition or if Fast Transition is adaptive.

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)

802.11r-enabled WLAN provides faster roaming for wireless client devices. However, if 802.11r is enabled on a WLAN and advertises fast transition (FT) and non-FT AKMs in Beacon and Probe RSN IE, some of the devices with bad implementation may not recognize FT/WPA2 authentication key-management (AKM) in RSN IE and fails to join. As a result, customers cannot enable 802.11r on the SSID.

To overcome this, Cisco Wireless infrastructure introduces adaptive 802.11r feature. When FT mode is set to adaptive, WLAN advertises 802.11r Mobility Domain ID on an 802.11i-enabled WLAN. Apple iOS10 client devices identifies the presence of MDIE on a 80211i/WPA2 WLAN and does a proprietary handshake to establish 802.11r association. Once the client completes successful 802.11r association, it will be able to do FT roaming as in a normal 802.11r enabled WLAN.

The FT adaptive is applicable only to selected Apple iOS10 devices. All other clients will continue to have 802.11i association on the WLAN.

Procedure

Step 1 To enable or disable 802.11r fast transition parameters, use the **config wlan security ft** {**adaptive** | **enable** | **disable**} *wlan-id* command.

Fast Transition adaptive option is enabled by default when you create a new WLAN, from the controller, Release 8.3, onwards. However, the existing WLANs will retain its current configuration when the controller upgrades to Release 8.3 from an earlier release.

Enable Fast SSID feature for allowing client devices a smother switching smoother switching from one WLAN to another..

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.

What to do next

- The tech support command output and xml config will not display fast transition information when it is disabled.
- The tech support command output and xml config will display Adaptive 802.11r information when it is enabled.
- To display a comprehensive view of the current controller configuration, use the **show run-config all** command.
- The fast transition adaptive mode is not supported on Releases prior to Release 8.3, the fast transition adaptive WLANs default to fast transition disable when the controller is downgraded from Release 8.3 to a previous release, and the fast transition adaptive configuration is invalidated.

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.

802.11i 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.

SKC is useful only in cases where you have a small number of clients, which roam among a small number of APs.

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)

Procedure

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

Cisco Centralized Key Management (CCKM)

Cisco Centralized Key Management (CCKM) is an older proprietary method of fast secure roaming that was supported with dynamic WEP, WPA1 & WPA2 EAP security. With WPA2, CCKM is supported only by Cisco wireless phones and Cisco WGBs. It has been superseded by the 802.11r FT standard.

CCKM uses a fast rekeying technique that enables clients to roam from one AP 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 AP 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.

If you enable CCKM, the functionality of APs 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.

For more information, see https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html#anc24.

Wi-Fi Protected Areas (WPA)

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.

Note WPA1 is deprecated. It may not be configured by itself, but only enabled if WPA2/CCMP128 (AES) is also enabled. WPA2 is the default. WPA3 is the emerging standard.

These standards provide for an authentication method and a cipher management method. The authentication methods supported are: 802.1X (a.k.a WPA Enterprise) and PSK.

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.

  In the 802.1X(Enterprise) authentication method, the clients use EAP (extensible authentication protocol) to authenticate with an authentication server. The authentication server can be an external RADIUS or LDAP server, or a local auth server running within the controller.

  To speed up roaming, a fast secure roaming method may optionally be deployed to bypass the authentication and key exchange phases.

- 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 (GUI)

Procedure

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
By default, WPA2 with CCMP128 is enabled. Optionally, WPA1 with CCMP128 and/or TKIP may be enabled, but WPA1 may not be configured with WPA2 disabled.

Note
Configure CCMP128(AES) for compatibility with greatest range of clients. Optionally, more secure ciphers (CCMP256, GCMP128, GCMP256) may be selected for greater security with recently released clients.

If using 802.1X (Enterprise) authentication, select 802.1X-SHA1 for compatibility with greatest range of clients. Or optionally, select 802.1X-SHA2 for use with recently released clients.

Step 6 Select the **WPA2 Policy-AES** check box to enable AES data encryption .

Note
Based on guidance from the Wi-Fi alliance (WFA), WPA/TKIP can only be configured on a secondary interface (CLI). Any previously saved TKIP configurations are retained upon upgrade and can be viewed on the CLI. This allows customers with Wi-Fi clients that only support WPA/TKIP to have a planned migration to devices that support AES.

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**.

Step 8 If you chose PSK, 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 Save the configuration.

Configuring WPA1+WPA2 (CLI)

Procedure

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
From Release 8.0, you cannot configure TKIP as a standalone encryption method. TKIP can be used only with the AES encryption method.

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

Wireless Encryption Protocol (WEP)

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.

Restrictions for Configuring Static WEP

- 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.

Configuring Dynamic WEP (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 WEP is deprecated and is only supported in Cisco Wave 1 (IOS-based) APs; not supported on Cisco Wave 2 or 802.11ax (Wi-Fi 6) APs.

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.)

MAC Authentication Failover to 802.1X Authentication

You can configure the controller to start 802.1X authentication when MAC authentication 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)

Procedure

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)

Procedure

To configure MAC authentication failover to 802.1X authentication, enter this command:

config wlan security 802.1X on-macfilter-failure {**enable** | **disable**} *wlan-id*

Identity PSK

This feature is designed to provide a simple and secured way for the growing number of devices to connect to the network. Some devices such as Internet of Things (IoT) clients may not support the 802.1x security protocol. These devices can connect to the network using the PSK authentication mechanism.

If all the clients are using the same key and if the key is shared with unauthorized users, then it leads to security breach.

The IPSK feature enables the administrator to configure WPA-PSK protocol-based unique pre-shared keys in the same SSID. This pre-shared key can be issued to an individual or group of users for their devices to connect to the network easily and safely. This also helps in identifying and managing a set of devices without affecting the other pre-shared key devices connected to the network. These keys can be configured with rules to authenticate and provide the appropriate level of access in the network.

Here, the AAA RADIUS server key is used to authenticate the client.

For documentation on Cisco ISE configuration, see the relevant administration guide at https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html.

This section contains the following subsections:

Prerequisites for Identity PSK

The RADIUS server must be configured to return the following Cisco AV pairs in its response to the MAC-filtering authentication request:

- psk-mode=ascii
- psk=cisco123

Key length must be between 8 and 63 characters for ASCII and 64 characters for HEX. If the key configured on the RADIUS server does not meet the length requirement, the client can be authenticated with PSK configured on the WLAN.

Configuring Identity PSK (GUI)

Procedure

Step 1 Choose **WLAN** to open the WLAN page.

Step 2 Create a new WLAN or click an existing WLAN.

Step 3 Check the **Status Enabled** check box.

Step 4 Choose **Security** > **Layer 2** tab.

Step 5 Choose **WPA+WPA2** or **WPA2+WPA3** from the **Layer 2 Security** drop-down list.

Step 6 In the **Security Type** drop-down list, select **Personal**.

Step 7 (Optional) Check the **MAC Filtering** check box.

Step 8 Check the **AutoConfig iPSK** check box.

Step 9 Choose **Security** > **AAA Servers** tab.

Step 10 Check the **Authentication Servers Enabled** check box.

Step 11 Select the **Server IP address and port number** from the drop-down list.

If the RADIUS server is not configured, the RADIUS server is selected from the global list.

Step 12 Choose **Advanced** tab.

Step 13 Check the **Allow AAA Override Enabled** check box to enable AAA override. The default value is disabled.

Step 14 Click **Apply**.

Configuring Identity PSK (CLI)

Procedure

- Enable MAC filtering by entering this command:
  config wlan mac-filtering enable *wlan-id*
- Enable AAA-override on a WLAN by entering this command:
  config wlan aaa-override enable *wlan-id*
- Enable RADIUS authentication on a WLAN by entering this command:
  config wlan radius_server auth enable *wlan-id*
- Enable PSK support on a WLAN by entering this command:
  config wlan security wpa akm psk enable *wlan-id*
- Configure the PSK pre-share key by entering this command:
  config wlan security wpa akm psk set-key *ascii/hex psk-key wlan-id*

Layer 3 Security

Layer 3 security takes effect only after Layer 2 is operational and also the wireless client has a working IP address. Layer 3 security is triggered by the client opening a web session (HTTP or HTTPS).

Note Layer 2 security should not be considered as a truly effective security method unless used in conjunction with a strong Layer 2 security method. This is because without Layer 2 security, the client's data can be captured in clear text over the air.

This section contains the following subsections:

With Layer 3 security, the client will issue a DNS query for a web server; the controller spoofs the DNS response, providing its own Virtual IP address. The client then opens a web connection (HTTP port 80 or HTTPS port 443) to that address. The controller redirects (to itself [Local Web Authentication] or to an external server [Central Web Authentication]), and then that dialog is used to authorize the client to connect to the network.

- Hijacking an initial HTTPS connection is an inherently problematic operation, as HTTPS is designed to prevent hijacking. In general, you can expect client browsers to prevent, or at least warn, the user against connecting.
- If the Layer 3 redirect goes to HTTPS rather than HTTP, the client browser is also likely to be warnted against connecting, unless the HTTPS server provides a valid certificate chain that is trusted by the client.

Types of Layer 3 Security

- Web Passthrough: This is a variation of the internal web authentication. It displays a page with a warning or an alert statement, but does not prompt for credentials. The user should click **ok**. You can enable email input, and the user can enter their email address, which becomes their username. When the user is connected, check your active clients list; that user is listed with the email address they entered as the username. For more information, see the Wireless LAN Controller 5760/3850 Web Passthrough Configuration Example.
- Local Web Authentication: Validates credentials against local database or RADIUS server. For more information, see https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/69340-web-auth-config.html.
- Redirect to External Web Authentication: With external web authentication, the login page used for web authentication is stored on an external web server. For more information, see https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71881-ext-web-auth-wlc.html.
- Central Webauth with Cisco ISE: 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. For more information, see Central Web Authentication, on page 954.

This section contains the following subsections:

Information About Web Authentication

For more information about web authentication, see https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/115951-web-auth-wlc-guide-00.html.

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.
- 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.

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)

Procedure

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)

Procedure

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

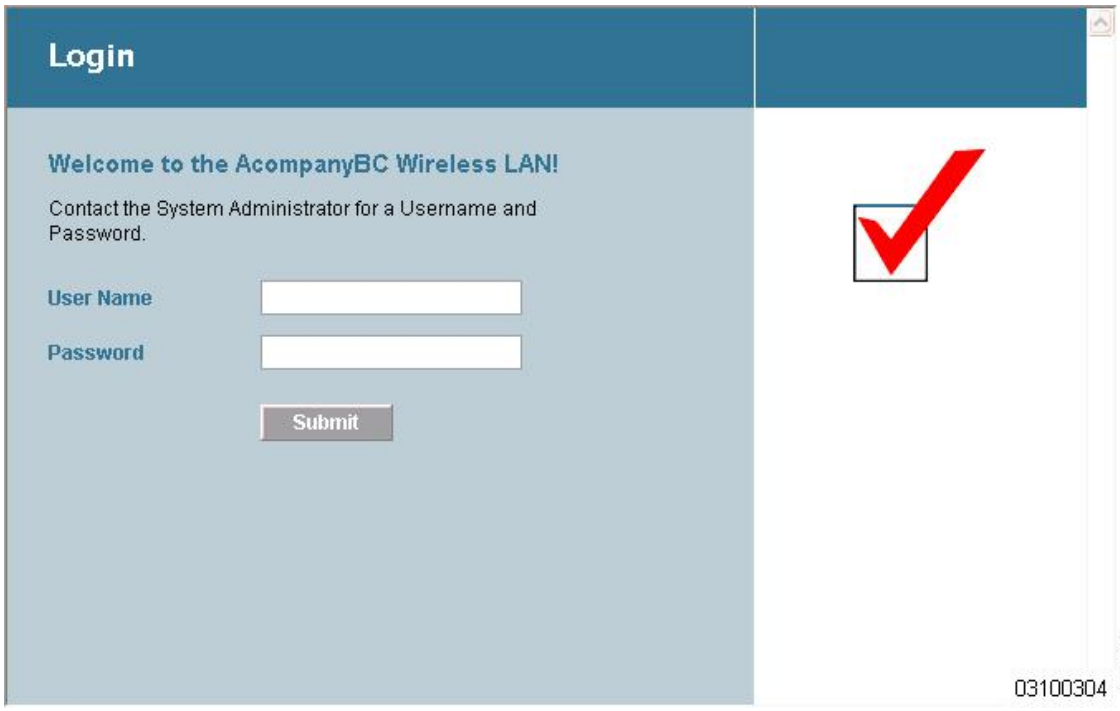
Note
If you ever want to remove this logo from the web authentication login page, enter the **clear webimage** command.

Step 10 Follow the instructions in the Verifying the Web Authentication Login Page Settings (CLI), on page 948 section to verify your settings.

Example: Modified Default Web Authentication Login Page Example

Figure 60: 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)

Procedure

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** field, 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** field, 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)

Procedure

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 948 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.

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.
- Ensure 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)

Procedure

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**

Step 5 In the **IP Address** field, 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 field.

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 field.

The range is 1 to 254 seconds.

The default is 6 seconds.

Step 8 In the **File Path** field, enter the path of the .tar file to be downloaded. The default value is "/."

Step 9 In the **File Name** field, 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** 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 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)

Procedure

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 61: 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

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)

Procedure

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)

Procedure

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*

Note
For the external web authentication URL, the CLI does not accept the *?* character. For example, if the URL is *https://example.com?text*, the CLI saves the URL as *https://example.comtext*. For more information, see CSCvu53350.

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

Captive Network Assistant Bypass

Many clients will attempt to determine whether their wireless network connection is being intercepted by Layer 3 security, in order to improve the user interaction experience. For example: Windows 10, Apple iOS, Firefox. Such a software interface is known as a Captive Network Assistant (CNA). In rare cases, the functionality of a CNA can cause problems with Layer 3 security; in such a situation, you can enable Captive Network Assistant Bypass (CNAB). With CNAB, the congtroller tries to trick the CNA into thinking that it is fully connected to the Internet, thus requiring the client to Layer-3 authenticate using a full browser session.

Note Enabling CNAB does not guarantee that all CNAs will fail to detect the Captive Portal because CNA implementations are continually refining their Captive Portal detection heuristics.

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.

Configuring Captive Network Assistant Bypass per WLAN (GUI)

Procedure

Step 1 Choose **WLANs** to open the **WLANs** page.

Step 2 Click the WLAN ID.

Step 3 Click the **Security** tab and then click the **Layer 3** tab.

Step 4 From the **Captive Network Assistant Bypass** drop-down list, choose:

- **None**: Global Captive Network Assistant Bypass setting is applied
- **Enable**: Captive Network Assistant Bypass is enabled for this particular WLAN
- **Disable**: Captive Network Assistant Bypass is disabled for this particular WLAN

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Configuring Captive Network Assistant Bypass per WLAN (CLI)

Procedure

- Enable, disable or activate global Captive Network Assistant Bypass per WLAN by entering this command:

  config wlan security web-auth captive-bypass {**none** | **enable** | **disable**} *wlan-id*

  By default, Captive Network Assistant Bypass per WLAN is in disabled state.

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.

Procedure

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.

Procedure

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
```

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 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.
- Inter-controller roaming with non-802.1X L2 security, with MAC filtering and CWA, is not supported prior to 8.9.

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 is 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.

Note Guest clients connecting to a web-auth WLAN in a CWA setup may also reach the internal virtual interface web-auth login page using port 80 or by using port 443 when the web authentication secure web is enabled in the Cisco AireOS controllers. This behavior is in line with how Cisco AireOS controllers handle all web authentication redirect scenarios and have no potential risk or vulnerability.

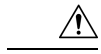
Authentication of Sleeping Clients

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.

The order of precedence is session timeout, sleeping client timeout, and user idle timeout. If the user idle timeout expires, then the sleeping client comes into play. If the sleeping client wakes up and if the sleeping client timeout has not expired, but if the session timeout has expired, the client must reauthenticate.

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.
- With Release 8.8.111.0, sleeping clients are supported in a scenario where both Layer 2 security and Layer 3 security are configured on a WLAN.
- 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.
- The number of sleeping clients that are supported depends on the controller platform:
  - Cisco 5520 Wireless Controller—25000
  - Cisco 8540 Wireless Controller—64000
  - Cisco Virtual Wireless LAN Controller—500

• Cisco Wireless Controller on Cisco Services-Ready Engine (SRE)—500

Configuring Authentication for Sleeping Clients (GUI)

Procedure

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*

Authenticating Sleeping Clients on L2+L3 Enabled WLANs

With this feature enhancement, the sleeping client functionality works even if L2 and L3 credentials are different.

This feature also supports a configuration which allows sleeping clients to be authenticated automatically when they wake up without the need for the user to try web access.

Although the security parameters have not changed, the feature functions with only 802.1X + web authentication setups.

Configuring Sleeping Client Authentication on L2+L3 Enabled WLANs (GUI)

Procedure

Step 1 Choose **WLANs** > **WLANs** to open the WLAN page.

Step 2 Click the WLAN-ID number of the WLAN to which you want to configure the feature.

Step 3 Choose the **Security** > **Layer 3** > tab from the **WLANs** > **Edit** page.

Step 4 Check the **Sleeping Client** check box to enable authentication for sleeping clients

Step 5 Enter the value for **Sleeping Client Timeout**,

This is the duration for which the sleeping clients are to be remembered before reauthentication is required. The default timeout is 12 hours.

Step 6 Check the **Sleeping Client Auto Authenticate** check box to enable auto authentication of the sleeping clients when they wake up .

Step 7 Save the configuration.

Configuring Sleeping Client Authentication on L2+L3 Enabled WLANs (CLI)

Procedure

- Enable or disable the auto authentication of the sleeping client on wake up without the need for web access by entering this command:

  config wlan custom-web sleep-client authenticate-without-trigger {**enable | disable**} *wlan-id*

  The default value is **Enabled**.

- View the status of the sleeping client authentication by entering this command:

  show wlan *wlan-id*

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.

Procedure

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)

Procedure

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)

Procedure

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
...
```

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.

- If web authentication redirect to HTTPS is enabled, then both the client HTTPS and client HTTP requests are redirected to HTTPS web authentication.

Note This enhancement was introduced in Release 8.0.

This section contains the following subsections:

Configuring Web Authentication Proxy (GUI)

Procedure

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 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 controller 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**

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.

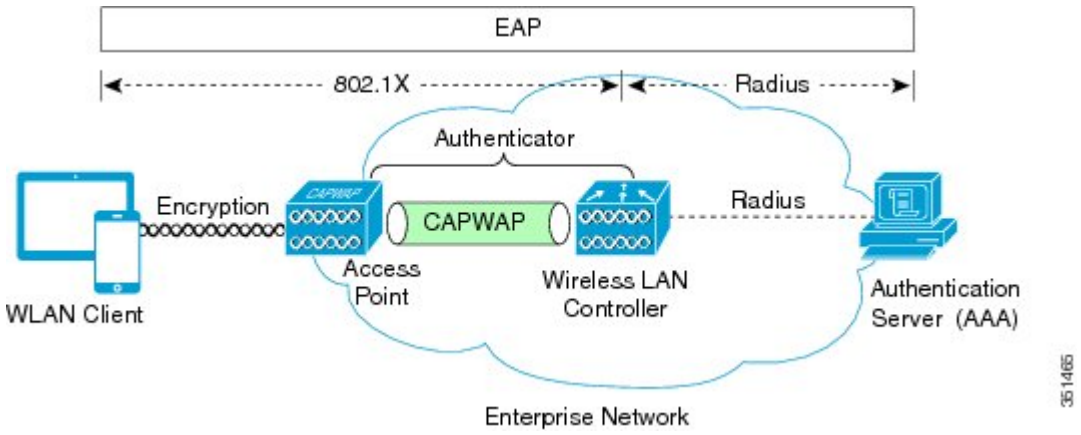
EAP and AAA Servers

This section contains the following subsections:

802.1X and Extensible Authentication Protocol

In order to provide enterprise-level WLAN security, 802.1X and Extensible Authentication Protocol (EAP) authentication mechanisms were implemented to provide mutual authentication of WLANs and WLAN client devices. The following figure shows the basic 802.1X and EAP authentication secure topology.

Figure 62: 802.1X and EAP Wireless LAN Security Topology



802.1X is an IEEE standard for port-based network access control and was adopted by the 802.11i security standard workgroup. The 802.1X standard provides authenticated access to 802.11 wireless LAN networks using the following logic:

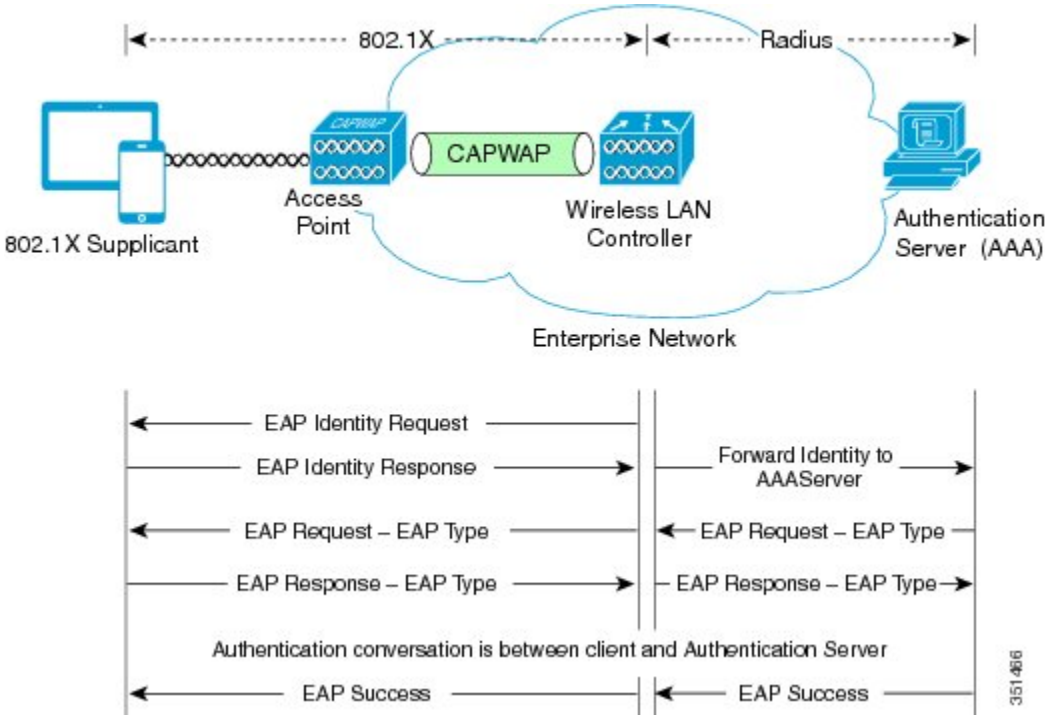
- A virtual port is created at the AP during the 802.11 association process for each WLAN client device.
- The AP then blocks all data frames on this virtual port except for 802.1X-based traffic.
- EAP authentication packets are carried in 802.1X traffic frames and are passed by the AP and Wireless LAN Controller to the AAA authentication server.
- Assuming EAP authentication is successful, the authentication server sends an EAP success message back to the Wireless LAN Controller and AP, which in turn pass the message on to the WLAN client device.

- The AP then allows data traffic (including voice and video) from the WLAN client device to flow through the virtual port.
- Before the virtual port opens to allow data traffic, data link encryption is established between the client device and the AP.

During the authentication process, a unique per-user per-session shared key is derived, and a portion of this key is used as a per-session encryption key.

The EAP authentication process supports a number of protocols, and which protocol is used ultimately depends on the capabilities of the WLAN client device supplicant and the WLAN infrastructure. Regardless of the EAP type that is used, all protocols generally behave as shown in the example EAP flow in the following figure:

Figure 63: EAP Protocol Flow



EAP as defined by RFC 3748 supports four packet types as part of the EAP authentication process:

- **EAP request**: The request packet that is sent by the authenticator (in the preceding figure, it is the Wireless LAN Controller and AP in combination) to the 802.1X supplicant (in the preceding figure, it is the WLAN client device). Each EAP request has a specific type that indicates what is being requested. In the example in the preceding figure, the first EAP request is for the WLAN client device identity, while the second EAP request is for the EAP type to be used for the authentication. A sequence number allows the authenticator and the peer to match an EAP response to each EAP request.
- **EAP response**: The response packet is sent by the WLAN client device to the AP and in turn to the controller, and uses a sequence number to match the initiating EAP request. In the case of an identity or type response, the response is forwarded by the controller to the authentication server.

- **EAP success**: Assuming that the WLAN client device or user has provided appropriate credentials during the authentication conversation, as shown in the preceding figure, the AAA server sends an EAP success packet to the controller, which in turn relays it through the AP to the WLAN client device.
- **EAP failure**: If the appropriate credentials are not provided at the WLAN client device or some other failure occurs, the AAA server sends an EAP failure packet to the controller, which relays it through the AP to the WLAN client device, resulting in failure of the authentication.

For more information, see https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-srnd/CCVP_BK_R7805F20_00_rtowlan-srnd_chapter_0100.html#CCVP_RF_8B1E3C6A_00.

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.

This section contains the following subsections:

Configuring LDAP (GUI)

Procedure

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 is displayed.
- To add an LDAP server, click **New**. The **LDAP Servers > New** page is displayed. 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** field. Both IPv4 and IPv6 addresses are supported.

Step 4 If you are adding a new server, enter the LDAP server's TCP port number in the **Port Number** field. The valid range is 1 to 65535, and the default value is 389.

Note
Only LDAP port 389 is supported on the controller. No other ports are supported for LDAP.

Step 5 From the **Server Mode (via TLS)** drop-down list, choose **Disabled** to establish LDAP connection (without secure tunnel) between LDAP server and the controller using TCP or **Enabled** to establish a secure LDAP connection using TLS.

Step 6 Check 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** field, 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** field, 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** field, 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** field, 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** field, 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** field, 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** field.
c) Highlight **LDAP** and click **>** to move it to the right **User Credentials** field. The database that is displayed at the top of the right **User Credentials** field is used when retrieving user credentials.

Note
If both LDAP and LOCAL appear in the right **User Credentials** field 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 is displayed, 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* **secure**— Adds an LDAP server for secure LDAP.
- **config ldap delete** *index*—Deletes a previously added LDAP server.
- **config ldap** {**enable** | **disable**} *index*—Enables or disables an LDAP server.
- **config ldap security-mode enable** *index*—Enables the LDAP server using index with existing commands.
- **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


Idx      Server Address      Port     Enabled  Secure
---      --------------      -----    ------  -------
1         2.3.1.4            389       No       No
2         2.3.1.5            389       Yes      No
```

- **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
```

```
(Cisco Controller)> show ldap 1
Server Index..................................... 1
Address.......................................... 9.1.0.100
Port............................................. 389
Server State..................................... Disabled
User DN.......................................... user1
User Attribute................................... user
User Type........................................ user
Retransmit Timeout............................... 2 seconds
Secure (via TLS)................................. Disabled
Bind Method ..................................... Anonymous
```

- **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}**

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 to authenticate users. Local EAP supports LEAP, EAP-FAST, EAP-TLS, P EAPv0/MSCHAPv2, and PEAPv1/GTC authentication between the controller and wireless clients.

This section contains the following subsections:

Related Topics

Downloading Device Certificates, on page 131

Restrictions for Local EAP

- Timer restrictions for local and central authentication using EAP: The EAP timeout cannot be configured on Wave 2 APs. Even though you can configure the EAP timeout on the controller, for Wave 2 APs, the EAP timeout is hardcoded to 30 seconds. This is due to the following reasons:
  - Clients get stuck in 8021X state indefinitely if AP moves from connected to standalone mode while EAP is in process.
  - Controller does not send EAP frames due to some issue, resulting in clients getting stuck indefinitely at AP.

  This has impact on clients, such as Windows clients, that wait for EAP identity request to pop up and are prompted for username and password. This issue is not seen on clients such as Apple, Samsung, Zebra, or WPA supplicants because they take the username and password beforehand.
- For mesh APs, you cannot configure EAP parameters. The mesh APs have the following static EAP configuration: EAP request timeout set to 60 seconds and the maximum number of EAP identity request retries set to 2.
- Legacy clients that require RC4 or 3DES encryption type 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.

Procedure

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** field, 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** field, 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** field, 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** field, 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).

This feature is no longer supported.

e) In the **Request Timeout** field, 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** field, 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, enable the feature if you want to ignore the EAP identity responses when enforcing the net user login limit.

h) In the **EAPOL-Key Timeout** field, enter the amount of time (in seconds) in which the controller attempts to send an EAP key over the LAN to wireless. The valid range is 200 to 5000 milliseconds, and the default setting is 1000 milliseconds.

i) In the **EAPOL-Key Max Retries** field, 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** field, 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** field, 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 is displayed again, click the name of your new profile. The **Local EAP Profiles > Edit** page is displayed.

e) Check 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 check 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, check 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, check the **Client Certificate Required** check box. If you want to use EAP-FAST with PACs instead of certificates, leave this check box unchecked, 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, check 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, check 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, check 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** fields, enter the key (in hexadecimal characters) used to encrypt and decrypt PACs.

c) In the **Time to Live for the PAC** field, 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** field, 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** field, enter the authority identifier of the local EAP-FAST server in text format.

f) If you want to enable anonymous provisioning, check 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, uncheck 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 is displayed, choose the **Security** > **AAA Servers** tabs to open the **WLANs > Edit (Security > AAA Servers)** page.
d) Uncheck the **Enabled** check boxes for RADIUS Authentication Servers and Accounting Server to disable RADIUS accounting and authentication for this WLAN.
e) Check 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 Enable EAP parameters 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 is displayed, choose the **Security** > **AAA Servers** tabs to open the **WLANs > Edit (Security > AAA Servers)** page.
d) Check the **Enable** check box to configure EAP parameters for this WLAN.
e) In the **EAPOL Key Timeout (200 to 5000 millisec)** field, enter the amount of time (in milliseconds) in which the controller attempts to send an EAP key over the WLAN to wireless clients using local EAP. The valid range is 200 to 5000 milliseconds and the default value is 1000 milliseconds.
f) In the **EAPOL Key Retries (0 to 4)** field, enter the maximum number of times that the controller attempts to send an EAP key over the WLAN to wireless clients using local EAP. The valid range is 0 to 4 retries and the default setting is 2 retries.
g) In the **Identity Request Timeout (1 to 120 sec)** field, enter the amount of time (in seconds) in which the controller attempts to send an EAP identity request to wireless clients within WLAN using local EAP. The valid range is 1 to 120 seconds and the default value is 30 seconds.
h) In the **Identity Request Retries (1 to 20 sec)** field, enter the maximum number of times that the controller attempts to retransmit the EAP identity request to wireless clients within WLAN using local EAP. The valid range is 1 to 20 retries, and the default setting is 2 retries.
i) In the **Request Timeout (1 to 120 sec)** field, enter the amount of time (in seconds) in which the controller attempts to send an EAP parameter request to wireless clients within WLAN using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.
j) In the **Request Retries (1 to 20 sec)** field, enter the maximum number of times that the controller attempts to retransmit the EAP parameter request to wireless clients within WLAN using local EAP. The valid range is 1 to 20 retries, and the default setting is 2 retries.
k) Click **Apply** to commit your changes.

Step 11 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.

Procedure

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 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 bcast-key-interval** *seconds*—Configures EAP-broadcast key renew interval time in seconds. The valid range is 120 to 86400 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. The valid range is 200 to 5000 milliseconds, and the default setting is 1000 milliseconds.

  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**}—

  Enable the feature if you want to ignore the EAP identity responses when enforcing the net user login limit. See the User Login Policies section for details.

Step 6 Specify values for the local EAP timers on a WLAN by entering these commands:

- **config wlan security eap-params {enable | disable}** *wlan_id*—Specifies to enable or disable SSID specific EAP timeouts or retries. The default value is disabled.
- **config wlan security eap-params eapol-key-timeout** *timeout wlan_id*—Specifies the amount of time (in milliseconds) in which the controller attempts to send an EAP key over the WLAN to wireless clients using local EAP. The valid range is 200 to 5000 milliseconds, and the default setting is 1000 milliseconds.
- **config wlan security eap-params eapol-key-retries** *retries wlan_id*—Specifies the maximum number of times that the controller attempts to send an EAP key over the WLAN to wireless clients using local EAP. The valid range is 0 to 4 retries, and the default setting is 2 retries.
- **config wlan security eap-params identity-request-timeout** *timeout wlan_id*—Specifies the amount of time (in seconds) in which the controller attempts to send an EAP identity request to wireless clients within WLAN using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.
- **config wlan security eap-params identity-request-retries** *retries wlan_id*—Specifies the maximum number of times that the controller attempts to retransmit the EAP identity request to wireless clients within WLAN using local EAP. The valid range is 1 to 20 retries, and the default setting is 2 retries.
- **config wlan security eap-params request-timeout** *timeout wlan_id*—Specifies the amount of time (in seconds) in which the controller attempts to send an EAP parameter request to wireless clients within WLAN using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.
- **config wlan security eap-params request-retries** *retries wlan_id*—Specifies the maximum number of times that the controller attempts to retransmit the EAP parameter request to wireless clients within WLAN using local EAP. The valid range is 1 to 20 retries, and the default setting is 2 retries.

Step 7 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 8 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 9 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 10 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 11 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 12 Save your changes by entering this command:

save config

Step 13 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 ...... 436973636f00000000000000000000000
     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 14 (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
```

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. Local network user entries can be used to authenticate clients through web authentication or local EAP.

This section contains the following subsections:

Configuring Local Network Users for the Controller (GUI)

Procedure

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**.

When admin modifies the credentials of a local network user, the user gets disassociated from the WLAN. Here, credentials refer to the change in password or wlan profile for that user.

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.

Note
If you are deleting a WLAN associated with network users, then the system prompts you to delete all network users associated with the WLAN before deleting the WLAN itself.

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* | **wlan-id** *wlan-id*}
    - *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.

    - *wlan-id*—Delete all the network users associated with the WLAN ID.

Note When a WLAN associated with network users is deleted, the system prompts to delete all network users associated with the WLAN first. After deleting the network users, you can delete the WLAN.

- 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

Uploading PACs for EAP-FAST

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.

PAC Provisioning and Device Enrolment

Controller device enrollment is initiated by controller as part of Protected Access Credential (PAC) provisioning with the Cisco ISE server. Controller initiates EAP-FAST and gets a PAC. This is accomplished by using the infrastructure of LOCAL-EAP EAP-FAST PAC provisioning. The PAC that is obtained uniquely maps to the device ID. If the device ID changes, the PAC data associated with the previous device ID is removed from the PAC store. PAC provisioning is triggered when a RADIUS server instance is enabled to provision the PAC.

Note Ensure that the Cisco ISE and the controller time are synchronized for PAC to be downloaded on controller appropriately.

In a High Availability (HA) setup, PACs are not shared over redundancy channel; instead, PAC download is reinitiated on a new active controller immediately after switchover.

This section contains the following subsections:

Uploading PACs (GUI)

Procedure

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** field, enter the name of the user who will use the PAC.

Step 4 In the **Validity** field, 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)** field, enter the IPv4/IPv6 address of the server.

Step 8 In the **File Path** field, enter the directory path of the PAC.

Step 9 In the **File Name** field, 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** 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 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)

Procedure

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.

Advanced WLAN Security

This section contains the following subsections:

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.

Most of the configuration to allow 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.

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. Use the following command to have multicast traffic forwarded for the overridden VLAN:

config flexconnect group *group-name* **multicast overridden-interface enable**

- 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)

Procedure

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**}

ISE NAC Support

The Cisco Identity Services Engine (ISE) is a next-generation, context-based access control solution that provides the functions of the 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 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.
- Inter-controller roaming with non-802.1X L2 security, with MAC filtering and CWA, is not supported prior to 8.9.

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 is 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.

Note Guest clients connecting to a web-auth WLAN in a CWA setup may also reach the internal virtual interface web-auth login page using port 80 or by using port 443 when the web authentication secure web is enabled in the Cisco AireOS controllers. This behavior is in line with how Cisco AireOS controllers handle all web authentication redirect scenarios and have no potential risk or vulnerability.

Local Web Authentication

Local web authentication is not supported for RADIUS NAC.

Table 41: ISE Network Authentication Flow

WLAN Configuration	CWA	LWA	Device Registration
RADIUS NAC Enabled	Yes	No	Yes
L2 PSK	802.1X	PSK	No
L3 None	N/A	Internal/External	N/A
MAC Filtering Enabled	Yes	No	Yes

Guidelines and Restrictions on ISE NAC Support

Guidelines

- When either an authentication or accounting RADIUS server fails, the corresponding server in the authentication or accounting server list will be made inactive. This ensures that client authentication and accounting occurs on the same IP authentication and accounting servers. However, the authentication and accounting servers should be added in the same order while configuring the RADIUS servers if they have to work together.
- When a client moves from one WLAN to another, the controller 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 controller before the idle timeout session expires, it is immediately moved to Run state. The client is validated if it reassociates with the controller after the session timeout.
- If you have two WLANs, and WLAN 1 is configured on a controller (WLC1) and WLAN2 is configured on another controller (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 controller 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.
- Remote LANs (RLANs) are 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)

Procedure

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*

Enabling ISE NAC on a WPA/WPA2-PSK WLAN

Information About Enabling ISE NAC on a WPA and WPA2-PSK WLAN

It is possible to enable both ISE NAC and WPA and WPA2-PSK on a WLAN.

This enhancement is introduced in Release 8.3. Prior to Release 8.3, it was not possible to enable both these configurations on the same WLAN.

A use case is Web redirect with PSK on controllers for the purpose of device onboarding. For example, on-board devices using an SSID with a PSK send the MAC address to Cisco ISE using central web authentication (CWA), and determine if it is registered.

Workflow

To support PSK along with ISE NAC, you must enable MAC filtering to facilitate a communication link to the AAA server to get redirect URL and preauthentication ACLs. The WLAN configuration that is supported is WPA and WPA-2 PSK + MAC filtering + ISE NAC.

1. A client joins the WLAN with Layer 2 authentication method, that is, PSK with the credentials created at the time of creating the WLAN.
2. Controller looks up the AAA server to check if MAC filtering is enabled. If yes, the AAA server provides the redirect URL and preauthentication ACLs. The client moves to central web authentication (CWA) state.
3. The client should log on via the redirect URL and authenticate using the available credentials. The CoA is then sent from the AAA server to controller.
4. As part of the CoA, controller triggers DISSOC to the client with the reason as UNSPECIFIED by starting a rejoin timer with 30 seconds.
5. The final authentication is a MAC authentication to which the final authorization results, such as the final VLAN and ACL, are returned.
6. Expecting the client to rejoin performing Layer 2 authentication generating PMK and GTK, thus the wireless encrypted link, the controller sends ACCESS REQ to the AAA server and related ACCESS RESP in which the controller provides the VLAN change or other enforcement attributes in the AAA server. With this attribute enforcement, the client moves to the Run state.

Additional References

- Web Authentication on WLAN Controller—http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/115951-web-auth-wlc-guide-00.html#anc17
- Central Web Authentication on the controller and ISE Configuration Example—http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

Enabling ISE NAC on WPA/WPA2-PSK WLAN (GUI)

Procedure

Step 1 Configure controller:

a) Add Cisco ISE as RADIUS server in controller with change of authorization (CoA) in Enabled state.

b) Configure a WLAN with Layer 2 security type set to **WPA+WPA2**, MAC filtering in Enabled state, Authentication Key Management set to **PSK**, and NAC state set to **ISE NAC**:

1. Choose **WLANs** and click the WLAN ID.
2. On the **WLANs > Edit** page, choose **Security** > **Layer 2** tab.
3. Set Layer 2 Security to **WPA+WPA2**.
4. Enable **MAC Filtering**.
5. Under **Authentication Key Management**, enable **PSK** and set the PSK format.
6. In the **Advanced** tab, set the **NAC State** to **ISE NAC**.

c) Create a preauthentication ACL to communicate with only the Cisco ISE server. For instructions on how to create an ACL, see (Link to be provided to the Configuring Access Control Lists chapter).

Note

- In addition to ISE traffic, allow other necessary traffic such as DNS, DHCP to be specified to permit DNS and DHCP traffic on the redirect ACL.
- If the APs are in FlexConnect mode, a preauth ACL is irrelevant. FlexConnect ACLs can be used to allow access for clients that have not been authenticated.

Step 2 Configure Cisco ISE:

a) Ensure that controller is in Cisco ISE.

b) Add an authentication profile.

c) Add an authorization profile.

d) Add postauthentication policies.

e) Add authorization policy.

Note

1. The first instance is when a user associates with the SSID and when the central web authentication profile is returned (unknown MAC address; therefore, you must set the user for redirection).
2. The second instance is when a user authenticated on the web portal, such that it matches the default rule (internal users) in this configuration (it can be configured to meet your requirements). It is important that the authorization part does not match the central web authentication profile again. Otherwise, there will be a redirection loop.

For instructions on Cisco ISE configuration, see http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html#anc6.

Client Exclusion Policies

Client exclusion policies allow wireless networks to block clients from associating based on various types of client misbehavior. You can configure the period of time during which clients are excluded or clients might be excluded indefinitely.

The controller maintains an exclusion list of MAC addresses, which blocks clients from associating with the controller. Clients can be automatically added to the exclusion list due to their misbehavior or can be manually added by MAC address. The automatically added clients can be automatically removed from the exclusion list based upon the WLAN's exclusion list timeout, or can be manually removed.

The criteria by which clients are excluded is configured globally on the controller. On each WLAN, exclusion may be enabled or disabled; if exclusion is enabled, the exclusion list timeout is configurable.

Additional Reference

For information about 802.1X client exclusion, see https://www.cisco.com/c/en/us/support/docs/lan-switching/8021x/214466-802-1x-client-exclusion-on-an-aireos-wlc.html.

This section contains the following subsections:

Configuring Client Exclusion Policies (GUI)

Procedure

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.

  Note
  In some configurations, 802.1X exclusion may not occur. For more information, see https://www.cisco.com/c/en/us/support/docs/lan-switching/8021x/214466-802-1x-client-exclusion-on-an-aireos-wlc.html.

- **Maximum 802.1x-AAA Failure Attempts**: Clients are excluded after a maximum number of 802.1X-AAA failure attempts with the RADIUS server. Valid range of maximum number of 802.1X-AAA failure attempts that you can configure is 1 to 10 with the default value being 3.
- **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)

Procedure

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 after a maximum number of 802.1X-AAA failure attempts with the RADIUS server by entering this command:

config wps client-exclusion 802.1x-auth max-1x-aaa-fail-attempts *num-of-attempts*

Valid range for the maximum number of 802.1X-AAA failure attempts with the RADIUS is 1 to 10 with the default value being 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*}

- **add**: Creates a local exclusion-list entry.
- **delete**: Deletes a local exclusion-list entry.
- **description**: Sets the description for an exclusion-list entry.

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 a list of FlexConnect clients that have been excluded in an AP locally by entering this command:

show flexconnect client exclusion-list

Information similar to the following appears:

```
cisco-ap#show flexconnect client exclusion-list
Client Exclusion List:
     Excluded Mac life    Type
8E:BB:02:65:55:AA    0  static
A0:B4:35:B1:AG:55    0  static
E8:02:FH:C4:6A:11   35 dynamic
```

Step 12 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
```

Configuring Client Exclusion Policies for a WLAN (GUI)

The 802.1X client exclusion feature prevents clients from sending authentication attempts for a period of time after excessive 802.1X authentication failures. You can configure client exclusion policies applicable to all clients by navigating to **Security** > **Wireless Protection Policies** > **Client Exclusion Policies** . This section provides instructions on how to configure client exclusion on a per-WLAN basis.

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN.

Step 3 On the **WLANs > Edit (Advanced)** page, click the **Advanced** tab.

Step 4 Locate the **Client Exclusion** label, check the check box adjacent to it to enable client exclusion policies, and enter the timeout value, in seconds. The timeout value represents the time period for which the excluded clients are prevented from sending 802.1X authentication attempts.

Step 5 Save the configuration.

Configuring Client Exclusion Policies for a WLAN (CLI)

The 802.1X client exclusion feature prevents clients from sending authentication attempts for a period of time after excessive 802.1X authentication failures. You can configure client exclusion policies applicable to all clients by entering the **config wps client-exclusion 802.1x-auth** {**enable** | **disable**} command. This section provides instructions on how to configure client exclusion policies on a per-WLAN basis.

Procedure

Step 1 Configure client exclusion policies for a WLAN by entering this command:

config wlan exclusionlist *wlan-id* {**enable** | **disable**}

Step 2 Configure the client exclusion list timeout period by entering this command:

config wlan exclusionlist *wlan-id timeout-in-seconds*

The timeout value represents the time period for which the excluded clients are prevented from sending 802.1X authentication attempts.

Step 3 Save the configuration by entering this command:

save config

Wi-Fi Direct Client Policy

Some clients support Wi-Fi Direct, which enables direct peer-to-peer connections; for example, from a PC to a printer. Wi-Fi Direct allows such a peer-to-peer connection simultaneously with an AP association.

Wi-Fi Direct Client Policy enables the network administrator to block associations from clients that have Wi-Fi Direct enabled.

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.
- 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)

Procedure

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)

Procedure

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.

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.

Note Peer-to-peer blocking feature is VLAN-based. WLANs using the same VLAN has an impact, if Peer-to-peer blocking feature is enabled.

Per WLAN, peer-to-peer configuration is pushed by the controller to FlexConnect AP.Peer-to-peer blocking is supported for clients that are associated with local and central switching WLANs. P2P blocking is supported for both locally switched and centrally switched WLANs.

Restrictions on Peer-to-Peer Blocking

- The Cisco controllers and APs supporting the IPSK-tag based P2P blocking feature are:
  - Cisco controllers—3504, 5520, 8540 Series controllers
  - Cisco APs—Cisco Wave 2 and 802.11ax APs.
- 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, with FlexConnect local switching, only clients connected to the same AP are blocked. FlexConnect ACLs can be used as a workaround for this limitation.
- For Flex+ local switching feature to function, ensure that the APs are not a part of the default flex-group.
- P2P forward-upstream action is not supported for anchored clients.

Configuring Peer-to-Peer Blocking (GUI)

Procedure

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.

- **Allow-Private-Group**—Applicable to PSK clients only. The traffic forwarding decision is taken based on the associated IPSK tags for the source and destination client devices.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Configuring Peer-to-Peer Blocking (CLI)

Procedure

Step 1 Configure a WLAN for peer-to-peer blocking by entering this command:

config wlan peer-blocking {**disable** | **drop** | **forward-upstream** | **allow-private-group**} *wlan_id*

Note
Allow-private-group is applicable to PSK clients only.

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
```

Step 4 See the ipsk-tag associated with the client by entering this command:

show client summary ipsk-tag

Peer-to-Peer Blocking Using IPSK Tags

P2P blocking is not applied as traffic does not get bridged across VLANs. IPSK-based peer-blocking is an exception, where the inter-VLAN client traffic is forwarded to upstream switch if the IPSK-tag matches and dropped otherwise.

The enhancement is supported on IPv4 and IPv6 protocols on central switching and Flex + local switching with the **Allow Private Group** enabled on the controller.

Table 42: IPSK Tag Traffic Flow

WLAN P2P configuration	IPSK Source device tag	IPSK Destination device tag	Traffic bridging decision	Result
Drop	Any	Any	Block	With this configuration, all the p2p traffic gets dropped.
Disable	Any	Any	Allow	With this configuration, all the p2p traffic gets bridged.
Up Stream	Any	Any	Forward up	With this configuration, all the p2p traffic gets forwarded to the next hop switch.

WLAN P2P configuration	IPSK Source device tag	IPSK Destination device tag	Traffic bridging decision	Result
Allow Private Group	T1	T2	Block	With this configuration, the p2p traffic with different tag values T1 and T2 gets dropped even if the clients are in different VLANs.
Allow Private Group	T	T	Allow	With this configuration, the p2p traffic with the same tag value T gets bridged. If the clients are in different vlans, the traffic gets forwarded to the upstream switch.

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.

Note The policy enforcement behavior in the Cisco AireOS Wireless Controller differs from that in the Cisco Embedded Wireless Controller.

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
- Select either AVC profile or role, or both based on local policy attributes defined in the AAA server.

  The following are the different ways by which local policies are applied based on a combination of AVC profile and role defined in the AAA server:

  - Both AVC profile and role are derived from the AAA server, the following options are available:
    - If AAA override is enabled, then AVC profile is prioritized and is applied.
    - If AAA override is disabled, then role matching is applied.
  - Only role is derived from the AAA server and role matching takes place, the following options are available:
    - If profile is defined in the policy, then role policy is applied.
    - If profile is not defined in the policy, then AVC profile defined in WLAN is applied.
  - Only AVC profile is derived from the AAA server, the following options are available:
    - If AAA override is enabled, then AVC profile received from the AAA server is applied.
    - If AAA override is disabled, then AVC profile defined on the WLAN is applied.

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.
- When local policy is configured for device type policy match and configured on a WLAN with guest anchor enabled, the AVC profile name from local policy is not applied at anchor.
- Local policies are enforced after profiling using OUI irrespective of DHCP or HTTP profiling. For more information, see CSCvp70783.

Table 43: 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.

Local Policy—Best Practices

Create and apply effective local policies for the clients on a WLAN, and the some of the recommended practices are listed below.

- We recommend you to have multiple policies on priority orders for different selection criteria on WLAN. The recommended priority order is:

  1. P1 policy with device type
  2. P2 policy with eap-type
  3. P3 policy with active hours

  For example a WLAN can have device-type policy as priority one, eap-type policy as priority 2 and so on and active hour policy should be the least priority always. If you want different policies matching with client better to create different WLAN as its always on priority base, the higher priority configured on WLAN will match and get applied to the client.

- We do not recommend having multiple policies of the same type on a single WLAN, nor recommend multiple active hour policies on a single WLAN. You should configure different WLANs with different active hour range to allow the client to join
- For the active hour policy, you should configure only the allowed range in the active hour because, other than active hours, the device does not allow the client to join. So, there is no need for a deny policy with active hours.

- We do not recommend having multiple active hour configurations on the same day

Use Case: Configure client behavior where the clients are allowed to join between 00:00-07:00 and 20:00-23:59 time on all days of the week and blocked during 07:01-19:59 time on all days.

Solution: You need to configure two WLANs:

- WLAN_1, with the policy as All days active hours 00:00-07:00 and allow IPv4 address
- WLAN_2 with the policy as All days active hours 20:00-23:59 and allow IPv4 address

Result: The clients can join WLAN_1 between 00:00 and 07:00. The clients can join WLAN_2 between 20:00 and 23:59. Other than these two-time slots, the client cannot join either WLAN_1 or WLAN_2.

Configuring Local Policies (GUI)

Procedure

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) From the **AVC Profile** drop-down list, choose an AVC profile to be applied based on the role defined in AAA.

k) In the **Active Hours** area, from the **Day** drop-down list, choose the days on which the policy has to be active.
l) Enter the **Start Time** and **End Time** of the policy.
m) Click **Add**.

The day and start time and end time that you specify is listed.

n) 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*
- Enable AVC profile—**config policy** *policy-name* **action avc-profile-name enable** *avc-profile-name*
- Disable AVC profile—**config policy** *policy-name* **action avc-profile-name disable**
- 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**}

Updating Organizationally Unique Identifier List

Updating Organizationally Unique Identifier List (GUI)

Procedure

Step 1 Copy the latest OUI list available at http://standards.ieee.org/develop/regauth/oui/oui.txt to the default directory on your server.

Step 2 Choose **Commands** > **Download File**.

The **Download file to Controller** page is displayed.

Step 3 From the **File Type** drop-down list, choose **OUI Update**.

Step 4 From the **Transfer Mode** drop-down list, choose the server type.

The server details are displayed on the same page.

Step 5 Click **Download**.

Step 6 After the download is complete, reboot the controller by choosing **Commands** > **Reboot**.

Step 7 If prompted to save your changes, click **Save and Reboot**.

Step 8 Click **OK**.

Updating Organizationally Unique Identifier List (CLI)

Procedure

Step 1 Copy the latest OUI list available at http://standards.ieee.org/develop/regauth/oui/oui.txt to the default directory on your server.

Step 2 Specify the server type by entering this command:

transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Specify the file type by entering this command:

transfer download datatype oui-update

Step 4 Begin the download of the file by entering this command:

transfer download start

Note
Follow the on-screen instructions to complete the download process.

Step 5 Reboot the controller by entering this command:

reset system

Step 6 See the updated OUI list by entering this command:

show profiling oui-string summary

Note

HA support for OUI update: HA link must be up while downloading the OUI file to the Active controller, so that the OUI update gets applied to the Standby controller as well.

Updating Device Profile List

Updating Device Profile List (GUI)

Procedure

Step 1 Copy the latest device profile list file to the default directory on your server.

Step 2 Choose **Commands** > **Download File**.

The **Download file to Controller** page is displayed.

Step 3 From the **File Type** drop-down list, choose **Device Profile**.

Step 4 From the **Transfer Mode** drop-down list, choose the server type.

The server details are displayed on the same page.

Step 5 Click **Download**.

Step 6 After the download is complete, reboot the controller by choosing **Commands** > **Reboot**.

Step 7 If prompted to save your changes, click **Save and Reboot**.

Step 8 Click **OK**.

Updating Device Profile List (CLI)

Procedure

Step 1 Copy the latest device profile list file to the default directory on your server.

Step 2 Specify the server type by entering this command:

transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Specify the file type by entering this command:

transfer download datatype device-profile

Step 4 Specify the file name by entering this command:

transfer download filename *device_profile-xml-file*

Step 5 Begin the download of the file by entering this command:

transfer download start

Note
Follow the on-screen instructions to complete the download process.

Step 6 Reboot the controller by entering this command:

reset system

Step 7 See the updated OUI list by entering this command:

show profiling policy summary

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)

Procedure

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)

Procedure

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*

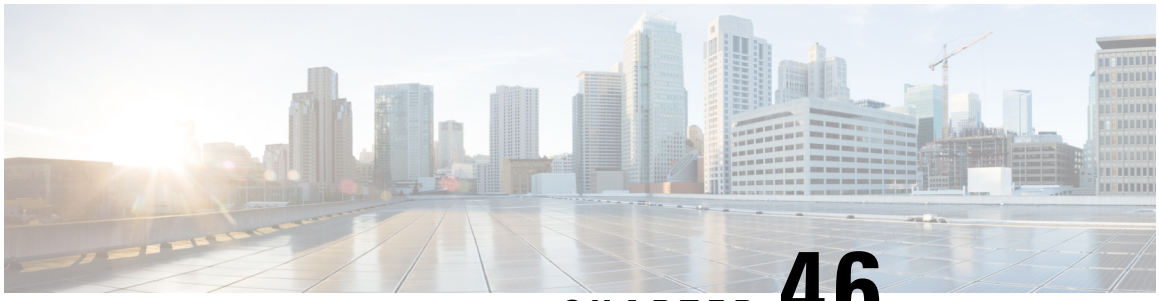
Note
Enter the **show guest-lan summary** command to see all wired guest LANs configured on the controller.

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*



CHAPTER 46

Client Roaming

In an 802.11 network with multiple APs, the selection of which AP to roam to is primarily made by the client. However, various configurations on the controller and APs can influence the client's roaming choices. Various protocols can inform the client regarding AP availability. Also, the wireless infrastructure can reject client association attempts in efforts to steer the client to a better AP.

- Fast SSID Changing, on page 1017
- 802.11k Neighbor List and Assisted Roaming, on page 1018
- 802.11v, on page 1020
- Optimized Roaming, on page 1024
- Band Select, on page 1026

Fast SSID Changing

By default, when a client roams between SSIDs, the controller enforces a delay of a few seconds before that client is permitted to associate to the new SSID.

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.

This section contains the following subsections:

Configuring Fast SSID Changing (GUI)

Procedure

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.

By default, fast SSID changing feature is in disabled state.

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

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

Configuring Fast SSID Changing (CLI)

Procedure

Step 1 Enable or disable fast SSID changing by entering this command:

config network fast-ssid-change {**enable** | **disable**}

By default, fast SSID changing feature is in disabled state.

Step 2 Save your changes by entering this command:

save config

802.11k Neighbor List and Assisted Roaming

The 802.11k standard allows an AP to inform 802.11k-capable clients of neighboring BSSIDs (APs in the same SSID). This can help the client to optimize its scanning and roaming behavior. Additionally, the Assisted Roaming Prediction Optimization feature can be used with non-802.11k clients, to discourage them from roaming to suboptimal APs.

Note We recommend not configuring two SSIDs with the same name in the controller, which may cause roaming issues.

Prediction Based Roaming - Assisted Roaming for Non-802.11k Clients

You can optimize roaming for non-802.11k clients by generating a prediction neighbor list for each client without sending an 802.11k neighbor list request. When prediction based roaming enables a WLAN, after each successful client association/re-association, the same neighbor list optimization applies on the non-802.11k client to generate and store the neighbor 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 the different neighbors as the clients usually probe before any association or re-association. This list is created with the most updated probe data and predicts the next AP that the client is likely to roam to.

The wireless infrastructure discourages 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.

- 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 activate.

For more information, see 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/Chapter-11.html#pgfId-1140097.

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.

Configuring Assisted Roaming (GUI)

Procedure

Step 1 Choose **WLANs**.

Step 2 In the **WLANs** window, click the WLAN ID.

Step 3 In the **WLANs > Edit** window, click the **Advanced** tab.

Step 4 In the **11k** area, check the **Neighbor List** and **Neighbor List Dual Band** check boxes.

Step 5 Check the **Assisted Roaming Prediction Optimization** check box if you want to optimize roaming for non-802.11k clients by generating a prediction neighbor list for each client without sending an 802.11k neighbor list request.

Step 6 Save the configuration.

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**}

802.11v

From Release 8.1, controller supports 802.11v amendment for wireless networks, which describes numerous enhancements to wireless network management.

One such enhancement is Network assisted Power Savings which helps clients to improve battery life by enabling them to sleep longer. As an example, mobile devices typically use a certain amount of idle period to ensure that they remain connected to access points and therefore consume more power when performing the following tasks while in a wireless network.

Another enhancement is Network assisted Roaming which enables the WLAN to send requests to associated clients, advising the clients as to better APs to associate to. This is useful for both load balancing and in directing poorly connected clients.

Enabling 802.11v Network Assisted Power Savings

Wireless devices consume battery to maintain their connection to the clients, in several ways:

- By waking up at regular intervals to listen to the access point beacons containing a DTIM, which indicates buffered broadcast or multicast traffic that the access point will deliver to the clients.
- By sending null frames to the access points, in the form of keepalive messages– to maintain connection with access points.
- Devices also periodically listen to beacons (even in the absence of DTIM fields) to synchronize their clock to that of the corresponding access point.

All these processes consume battery and this consumption particularly impacts devices (such as Apple), because these devices use a conservative session timeout estimation, and therefore, wake up often to send keepalive messages. The 802.11 standard, without 802.11v, does not include any mechanism for the controller or the access points to communicate to wireless clients about the session timeout for the local client.

To save the power of clients due to the mentioned tasks in wireless network, the following features in the 802.11v standard are used:

- Directed Multicast Service
- Base Station Subsystem (BSS) Max Idle Period

Directed Multicast Service

Using Directed Multicast Service (DMS), the client requests the access point to transmit the required multicast packet as unicast frames. This allows the client to receive the multicast packets it has ignored while in sleep mode and also ensures Layer 2 reliability. Furthermore, the unicast frame will be transmitted to the client at a potentially higher wireless link rate which enables the client to receive the packet quickly by enabling the radio for a shorter duration, thus also saving battery power. Since the wireless client also does not have to wake up at each DTIM interval in order to receive multicast traffic, longer sleeping intervals are allowed.

BSS Max Idle Period

The BSS Max Idle period is the timeframe during which an access point (AP) does not disassociate a client due to nonreceipt of frames from the connected client. This helps ensure that the client device does not send keepalive messages frequently. The idle period timer value is transmitted using the association and reassociation response frame from the access point to the client. The idle time value indicates the maximum time a client can remain idle without transmitting any frame to an access point. As a result, the clients remain in sleep mode for a longer duration without transmitting the keepalive messages often. This in turn contributes to saving battery power.

Restrictions

- If you have enabled optimized roaming, the controller sends a BSS Transition Management (BTM) query to forcibly roam a client. This will enable the dissociation imminent field, irrespective of the WLAN configuration. Load balancing and XOR roaming adhere to the disassociation imminent configuration of the WLAN.

This section contains the following subsections:

Prerequisites for Configuring 802.11v

- This feature is applicable to Apple clients like Apple iPad, iPhone and so on that run on Apple iOS version 7 or later.
- This feature supports local mode; also supports FlexConnect access points in central authentication modes only.
- Not all Cisco APs support all 802.11v features. For more information about which APs support 802.11v, see https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html.

Configuring 802.11v Network Assisted Power Savings (CLI)

Procedure

- Configure the value of BSS Max Idle period by entering these commands:
  - **config wlan usertimeout** *wlan-id*
  - **config wlan bssmaxidle** {**enable** | **disable**} *wlan-id*
- Configure DMS by entering this command:

  config wlan dms {**enable** | **disable**} *wlan-id*

Monitoring 802.11v Network Assisted Power Savings (CLI)

Execute the commands described in this section to monitor the DMS and BSS Max Idle time using the CLI.

- Display DMS information on each radio slot on an access point by entering the **show controller d1/d0 | begin DMS** command on the access point.
- Track the DMS requests processed by the controller by entering the following commands:
  - **debug 11v all** {**enable** | **disable**}
  - **debug 11v errors** {**enable** | **disable**}
  - **debug 11v detail** {**enable** | **disable**}
- Enable or disable 802.11v debug by entering the **debug 11v detail** command on the controller.
- Track the DMS requests processed by an access point by entering the **debug dot11 dot11v** command on the access point.

Configuration Examples for 802.11v Network Assisted Power Savings

The following example displays a sample output for the **show wlan** *wlan-id* command with 802.11v parameters:

```
WLAN Identifier.................4
Profile Name...................Mynet
802.11v Directed Multicast Service........Disabled
802.11v BSS Max Idle Service..............Enabled
802.11v BSS Max Idle Protected Mode..............Disabled
802.11v TFS Service..............Disabled
802.11v BSS Transition Service..............Disabled
802.11v WNM Sleep Mode Service..............Disabled
DMS DB is emptyTag: BSS Max Idle Period
Tag number: BSS Max Idle Period (90)
Tag Length: 3
BSS Max Idle Period (1000 TUS) :300
... ...0 = BSS Max Idle Period Options : Protected Keep-Alive Required:0
```

Enabling 802.11v BSS Transition Management

802.11v BSS Transtion is applied in the following three scenarios:

- Solicited request—Client can send an 802.11v Basic Service Set (BSS) Transition Management Query before roaming for a better option of AP to reassociate with.
- Unsolicited Load Balancing request—If an AP is heavily loaded, it sends out an 802.11v BSS Transition Management Request to an associated client.
- Unsolicited Optimized Roaming request—If a client's RSSI and rate do not meet the requirements, the corresponding AP sends out an 802.11v BSS Transition Management Request to this client.

Note 802.11v BSS Transition Management Request is a suggestion (or advice) given to a client, which the client can choose to follow or ignore. To force the task of disassociating a client, turn on the disassociation-imminent function. This disassociates the client after a period of time if the client is not reassociated to another AP.

Guidelines and Restrictions

- Client needs to support 802.11v BSS Transition.
- The disassociation imminent is set to **True** by default when optimized roaming is enabled. This value is set to **True** even when the disassociation imminent disabled in a WLAN.

Enable 802.11v BSS Transition Management on the Controller

To enable 802.11v BSS transition management on a controller, enter the following commands:

config wlan bss-transition enable *wlan-id*

config wlan disassociation-imminent enable *wlan-id*

Troubleshooting

To troubleshoot 802.11v BSS transition, enter the following command:

debug 11v all

Optimized Roaming

Optimized roaming resolves the problem of sticky clients that remain associated to access points that are far away and outbound clients that attempt to connect to a Wi-Fi network without having a stable connection. This feature disassociates clients based on the RSSI of the client data packets and data rate. The client is disassociated if the RSSI alarm condition is met and the current data rate of the client is lower than the optimized roaming data rate threshold. You can disable the data rate option so that only RSSI is used for disassociating clients.

Optimized roaming also prevents client association when the client's RSSI is low. This feature checks the RSSI of the incoming client against the RSSI threshold, which is configured in the same place as the Coverage Hole Detection. This check prevents the clients from connecting to a Wi-Fi network unless the client has a viable connection. In many scenarios, even though clients can hear beacons and connect to a Wi-Fi network, the signal might not be strong enough to support a stable connection.

You can also configure the client coverage reporting interval for a radio by using optimized roaming. The client coverage statistics include data packet RSSIs, Coverage Hole Detection and Mitigation (CHDM) pre-alarm failures, retransmission requests, and current data rates.

Optimized roaming is useful in the following scenarios:

- Addresses the sticky client challenge by proactively disconnecting clients.
- Actively monitors data RSSI packets.
- Disassociates client when the RSSI is lower than the set threshold.

This section contains the following subsections:

Restrictions for Optimized Roaming

- When basic service set (*BSS*) transition is sent to 802.11v-capable clients, and if the clients are not transitioned to other BSS before the disconnect timer expires, the corresponding client is disconnected forcefully. BSS transition is enabled by default for 802.11v-capable clients.
- We recommend that you do not use the optimized roaming feature with RSSI low check.

Configuring Optimized Roaming (GUI)

Procedure

Step 1 Choose **Wireless** > **Advanced** > **Optimized Roaming**. The Optimized Roaming page is displayed.

Step 2 To enable optimized roaming for an 802.11 band, check the **Enable** check box.

You can configure the optimized roaming interval and data rate threshold values only after you enable optimized roaming for an 802.11 band.

Step 3 In the **Optimized Roaming Interval** text box, enter a value for the interval at which an access point reports the client coverage statistics to the controller.

The client coverage statistics include data packet RSSIs, Coverage Hole Detection and Mitigation (CHDM) pre-alarm failures, retransmission requests, and current data rates. The range is from 5 to 90 seconds. The default value is 90 seconds.

Note
You must disable the 802.11a/b network before you configure the optimized roaming reporting interval. If you configure a low value for the reporting interval, the network can get overloaded with coverage report messages.

The access point sends the client statistics to the controller based on the following conditions:

- When **Optimized Roaming Interval** is set to 90 seconds by default.
- When **Optimized Roaming Interval** is configured (for instance to 10 secs) only during optimized roaming failure due to Coverage Hole Detection (CHD) RED ALARM.

Step 4 In the **Optimized Roaming Data Rate Threshold** text box, enter a value for the threshold data rate of the client.

The following data rates are available:

- 802.11a—6, 9, 12, 18, 24, 36, 48, and 54.
- 802.11b—1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, and 54.

Optimized roaming disassociates clients based on the RSSI of the client data packet and data rate. The client is disassociated if the current data rate of the client is lower than the Optimized Roaming Data Rate Threshold.

What to do next

Optimized roaming checks the client RSSI at the time of an association. This RSSI value is verified against the configured CHDM RSSI with a 6 db hysteresis. To verify the RSSI threshold configured for coverage hole detection, 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.

Configuring Optimized Roaming (CLI)

Procedure

Step 1 Enable optimized roaming by entering this command:

ap dot11 5ghz rrm optimized-roam

By default, optimized roaming is disabled.

Step 2 Configure the client coverage reporting interval for 802.11a networks by entering this command:

ap dot11 5ghz rrm optimized-roam reporting-interval *interval-seconds*

The range is from 5 to 90 seconds. The default value is 90 seconds.

Note
You must disable the 802.11a network before you configure the optimized roaming reporting interval.

Step 3 Configure the threshold data rate for 802.11a networks by entering this command:

ap dot11 5ghz rrm optimized-roam data-rate-threshold *mbps*

For 802.11a, the configurable data rates are 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54. You can configure DISABLE to disable the data rate.

Step 4 View information about optimized roaming for each band by entering this command:

show ap dot11 5ghz optimized-roaming

```
(Cisco Controller) > show ap dot11 5ghz optimized-roaming
802.11a OptimizedRoaming

  Mode                                  : Disabled
  Reporting Interval                    : 90 seconds
  Rate Threshold                        : Disabled
```

Step 5 View information about optimized roaming statistics by entering this command:

show ap dot11 5ghz optimized-roaming statistics

```
(Cisco Controller) > show ap dot11 5ghz optimized-roaming statistics
802.11a OptimizedRoaming statistics

  Disassociations                       : 0
  Rejections                            : 0
```

Band Select

Band select 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 select 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.

Band Select Algorithm

The band select 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 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.
- We recommend that you do not use Band Select in high-density areas such as stadiums.

Configuring Band Selection (GUI)

Procedure

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)

Procedure

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.

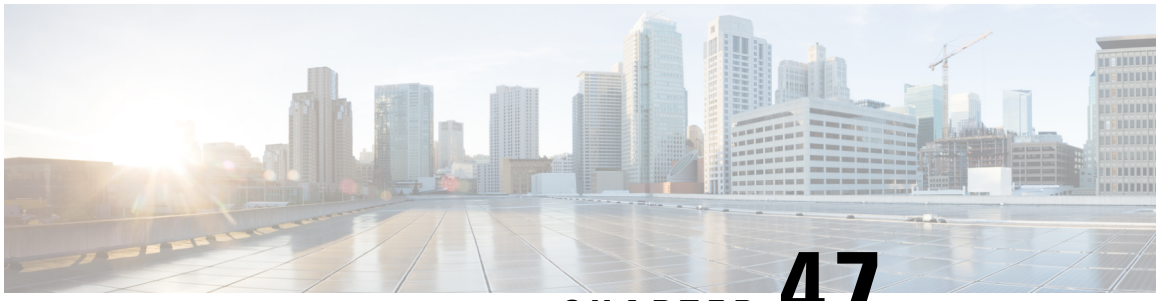
Step 9 Verify your settings by entering this command:

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 47

DHCP

- Information About Dynamic Host Configuration Protocol, on page 1031
- DHCP Proxy Mode, on page 1033
- DHCP Option 82, on page 1037
- DHCP Option 82 Link Select and VPN Select Suboptions, on page 1039
- Internal DHCP Server, on page 1043

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.

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 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.

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.

Note

- VRF is not supported in the internal DHCP servers.
- DHCPv6 is not supported in the internal DHCP servers.

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.
- 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. This 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.

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.

DHCP Proxy Mode versus DHCP Bridging Mode

When using external DHCP servers, the controller can operate in one of two modes: as a DHCP Relay or as a DHCP Bridge.

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 44: 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

DHCP Proxy Mode

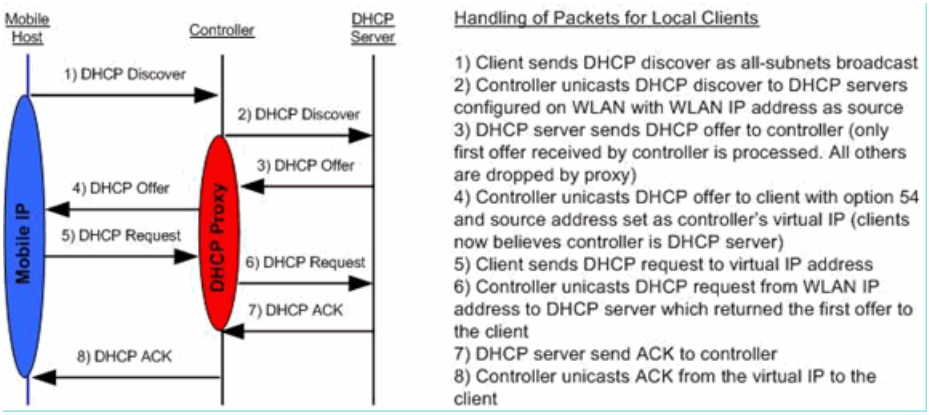
In DHCP Proxy Mode, the controller’s virtual IP address is used as the source IP address of all DHCP transactions to the client. As a result, the real DHCP server IP address is not exposed in the air. This virtual IP is displayed in debug output for DHCP transactions on the controller. However, use of a virtual IP address can cause issues on certain types of clients.

When multiple offers come from external DHCP servers, the DHCP proxy normally selects the first one that comes in and sets the IP address of the server in the client data structure. As a result, all following transactions go through the same DHCP server until a transaction fails after retries. At this point, the proxy selects a different DHCP server for the client.

DHCP proxy is enabled by default. All controllers in a mobility list must have the same DHCP proxy setting.

Note DHCP proxy must be enabled in order for DHCP option 82 to operate correctly.

Proxy Mode Packet Flow



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.
- Suppose an interface in an interface group is marked as *dirty*. If a client is mapped to this interface through its association with a WLAN mapped to the interface group, the client does not get mapped to a new interface in the interface group because the controller DHCP proxy does not update the client interface VLAN to a new interface. This has been observed in conditions in which the interface group is assigned through AAA override and the DHCP mode is aggressive. The workaround is to use a non-aggressive DHCP mode.

  For more information, see CSCvv74634.

Configuring DHCP Proxy (GUI)

Procedure

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)

Procedure

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)

Procedure

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)

Procedure

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)

For client associations to a WLAN that has DHCP required, the DHCP timeout controls how long the controller will wait, after a new association, for the client to complete DHCP. If the DHCP exchange is not completed within the timeout period, the controller deauthenticates the client. The default setting is the maximum of 120 seconds; we recommend that you do not reduce this value.

Procedure

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)

For client associations to a WLAN that has DHCP required, the DHCP timeout controls how long the controller will wait, after a new association, for the client to complete DHCP. If the DHCP exchange is not completed within the timeout period, the controller deauthenticates the client. The default setting is the maximum of 120 seconds; we recommend that you do not reduce this value.

Procedure

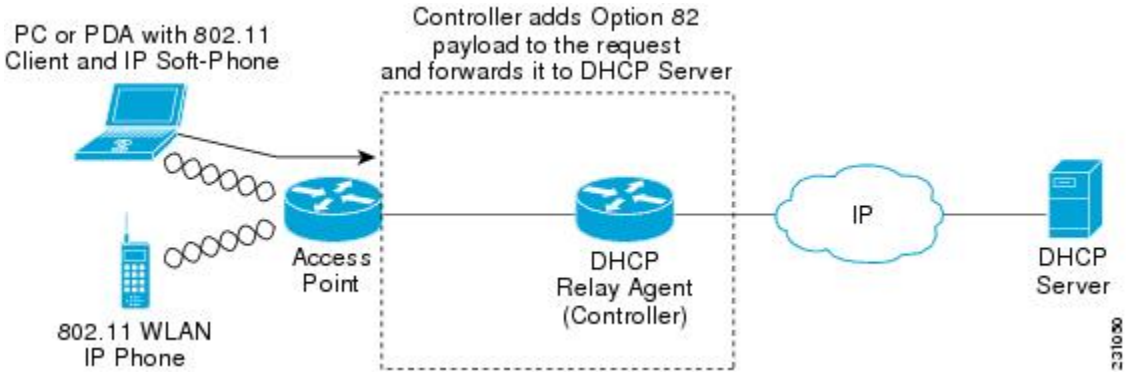
- Configure a DHCP timeout by entering this command:

  config dhcp timeout *seconds*

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 64: 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)

Procedure

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.

Configuring DHCP Option 82 Insertion in Bridge Mode (CLI)

Procedure

- Configure DHCP Option 82 insertion in Bridge mode on the management interface by entering this command:

  config interface dhcp management option-82 bridge-mode-insertion {**enable** | **disable**}

Note Enter the **show interface detailed management** command to see if DHCP Option 82 Bridge mode insertion is enabled or disabled on the management interface.

- Configure DHCP Option 82 insertion in Bridge mode on the dynamic interface by entering this command:

  config interface dhcp dynamic-interface *dynamic-interface-name* **option-82 bridge-mode-insertion** {**enable** | **disable**}

Note Enter the **show interface detailed** *dynamic-interface-name* command to see if DHCP Option 82 Bridge mode insertion is enabled or disabled on the dynamic interface.

DHCP Option 82 Link Select and VPN Select Suboptions

In a wireless environment, when a client requests a DHCP address, specify to the DHCP server the subnet from which the IP address has to be assigned, using the *giaddr* field in the DHCP DISCOVER packet. You can also use the giaddr field to specify the address that the DHCP server can use to communicate with the DHCP relay agent (controller). It is difficult to determine that the controller IP address in the subnet is reachable from the DHCP server. Hence, there is a need to send link-selection information that is distinct from the controller-reachable address to the DHCP server. Using the DHCP link select (DHCP option 82, suboption 5) configured on the controller interface, the link selection information distinct from controller's reachable address is sent to the DHCP server.

In a large network's wireless environment, the Cisco Network Registrar (CNR) server, which is a DHCP server, has multiple pools created based on VPN IDs or VRF names. Using these pools, you can assign IP address to a client with the help of the DHCP VPN Select option (DHCP option 82 and suboption 151). When you enable DHCP VPN Select (DHCP option 82 and suboption 151) on the controller interface, the controller sends the VPN ID or VRF name of the pool from which the IP address has to be assigned to the client. The DHCP VPN Select option enables easy-to-operate, shared usage of a centralized DHCP server, resulting in cost savings.

DHCP Link Select

Configure DHCP Link Select (DHCP option 82, suboption 5) on the management and dynamic interfaces of the controller. Before configuring DHCP Link Select on the controller interface, enable the DHCP proxy and DHCP option 82 on that interface.

When the Link Select option is enabled on the controller interface, suboption 5 is added to the packet with the IP address information that contains the desired subnet address for the corresponding client. The subnet address is the controller interface address mapped to the client VLAN interface. The DHCP server uses the subnet address to assign the IP address to the DHCP client.

DHCP VPN Select

Configure DHCP VPN Select (DHCP option 82, suboption 151) on the management and dynamic interfaces of the controller. Before configuring DHCP VPN Select on the controller interface, enable the DHCP proxy and DHCP option 82 on that interface.

You can configure different VPN IDs or VRF names on the same controller or different controllers using the VPN Select feature configured on the controller interface. Configuring the VPN Select feature, results in the DHCP server VPN pools having nonoverlapping addresses.

You must add VSS Control suboption 152 every time VSS suboption 151 is sent to the DHCP server. If the DHCP server understands and acts on VSS suboption 151, VSS Control suboption 152 is removed from the DHCP acknowledgment. If the DHCP server copies back VSS Control suboption 152 in the DHCP acknowledgment, it means that the DHCP server does not have the required support for the VSS suboption.

Mobility Considerations

Same Subnet

VPN ID or VRF name mapping to a WLAN should be the same on all the controllers in a mobility group. For example, if WLAN1 interface maps to VPN ID 1 and WLAN2 interface maps to VPN ID 2 maps on WLC A, then WLC B should also have WLAN1 interface mapping to VPN ID 1 and WLAN2 interface mapping to VPN ID 2. This way, when client L2 roams to another controller, the roamed controller's DHCP configuration will ensure that the client is assigned an address from the same VPN.

Different subnet mobility

With L3 mobility, all the DHCP DISCOVER packets are sent to the anchor and the assignment of the original VPN is ensured.

Auto anchor mobility

All the DHCP DISCOVER packets are sent to the anchor and the assignment of the original VPN is ensured.

Prerequisites for DHCP Option 82 Link Select and VPN Select

- The DHCP mode should be set to proxy.
- The DHCP external server should be configured.
- DHCP Option 82 must be enabled on the controller.
- The interface being configured should not be of type service or virtual.
- The relay source interface name should be a valid interface with IP address configured.

Note Proxy mode is not supported for IPv6.

Configuring DHCP Option 82 Link Select and VPN Select (GUI)

Procedure

Step 1 Choose **Controller** > **Interfaces**.

Step 2 Select the interface you want to configure the DHCP option-82 link select or VPN select.

You can configure the DHCP option-82 link select on the management 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 the Enable DHCP Option 82 check box to enable DHCP option 82 on the interface.

Step 4 Select the Enable DHCP Option 82-Link Select check box to enable link select on the interface.

Step 5 From the Link Select relay source drop-down list, choose **management** or **dynamic** to enable link select on the interface.

When link select is enabled, you can select any interface as relay source management and dynamic interface configured on the controller.

Step 6 Select the Enable DHCP Option 82-VPN Select check box to enable VPN select on the management interface.

When VPN select is enabled, you can configure either VRF Name or VPN ID. If you try to configure both the options, you are prompted with an error message.

Step 7 In the VPN Select - VRF name text box, enter the VRF name.

Step 8 In the VPN Select - VPN ID text box, enter the VPN ID.

VPN ID should be provided in format of xxxxxx:xxxxxxxx.

Step 9 Click **Apply**.

Configuring DHCP Option 82 Link Select and VPN Select (CLI)

Procedure

Step 1 Configure the dynamic interface using the following commands:

- **config interface dhcp dynamic-interface** *interface-name* { **option-82** | **primary** | **proxy-mode** }

Step 2 Configure DHCP Option 82 on a dynamic interface using the following commands:

- **config interface dhcp dynamic-interface** *interface-name* **option-82** { **enable** | **disable** | **linksel** | **vpnsel** }

Step 3 Configure Link Select suboption 5 on a dynamic interface using the following commands:

- **config interface dhcp dynamic-interface** *interface-name* **option-82 linksel** { **enable** | **disable** | **relaysrc** }
- To enable link select on the dynamic interface, first you need to enter the **config interface dhcp dynamic-interface** *interface-name* **option-82 linksel relaysrc** command followed by the **config interface dhcp dynamic-interface** *interface-name* **option-82 linksel enable** command.

Step 4 Configure VPN Select suboption 151 on a dynamic interface using the following commands:

- **config interface dhcp dynamic-interface** *interface-name* **option-82 vpnsel** { **enable** | **disable** | **vrfname** *vrf-name* | **vpnid** *vpn-id* }

  The value of *vpn-id* is denoted in the *oui:vpn-ndex* format *xxxxxx:xxxxxxxx*.

  You can configure either VPN ID or VRF name for VPN Select on the dynamic interface. If VPN ID is already configured and you try to configure VRF name, then the earlier configuration is cleared when VPN select is disabled.

  VRF name is denoted as a string of seven octets.

  To enable VPN select on a dynamic interface, first you need to enter the **config interface dhcp dynamic-interface** *interface-name* **option-82 vpnsel vpnid** *vpn-id* or **config interface dhcp dynamic-interface** *interface-name* **option-82 vpnsel vrfname** *vrfname* command followed by the **config interface dhcp dynamic-interface** *interface-name* **option-82 vpnsel enable** command.

Step 5 Configure Link Select suboption 5 on a management interface using the following commands:

- **config interface dhcp management option-82 linkselect** { **enable** | **disable** | **relaysrc** } *interface-name*
- To enable link select on the management interface, enter the **config interface dhcp management option-82 linkselect relaysrc** command followed by the **config interface dhcp management option-82 linkselect enable** command.

Step 6 Configure VPN Select suboption 151 on a management interface using the following commands:

- **config interface dhcp management option-82 vpnselect** { **enable** | **disable** | **vpnid** *vpn-id* | **vrfname** *vrf-name* }

  VPN ID value is denoted in the *oui:vpn-ndex* format *xxxxxx:xxxxxxxx*.

You can configure either VPN ID or VRF name for VPN select on the management interface. If VPN ID is already configured and you try to configure VRF name, then the earlier configuration is cleared when VPN select is disabled.

VRF name is denoted as a string of seven octets.

To enable VPN select on the management interface, enter the **config interface dhcp management option-82 vpnsel vpnid** *vpn-id* or **config interface dhcp management option-82 vpnselect vrfname** *vrf-name* command followed by the **config interface dhcp management option-82 vpnsel enable** command.

Step 7 Save the configuration using the following command: **save config**

Step 8 To view the details of the Link Select settings or the VPN Select interface settings, enter the following command: **show interface detailed**

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

Per WLAN DHCP Servers

By default, when using DHCP proxy mode, a WLAN's clients use the DHCP servers that are configured on the mapped interfaces. You can override the interface's DHCP servers by configuring per-WLAN DHCP servers.

This section contains the following subsections:

Restrictions for Configuring Internal DHCP Server

- You can configure up to 16 Internal DHCP scopes.
- Internal DHCP Server is not supported on the following controllers:
- You must configure DHCP Proxy Mode to use the Internal DHCP Server.

- 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.

Configuring DHCP Scopes (GUI)

Procedure

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** field, 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** field, 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** field, 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** field, 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** field, enter the subnet mask assigned to all wireless clients.

Step 9 In the **Lease Time** field, 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** field, 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** field, 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** field, 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** field, 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)

Procedure

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
```

Configuring DHCP Per WLAN (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.

Procedure

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, uncheck 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, check the **DHCP Server Override** check box and enter the IP address of the desired DHCP server in the **DHCP Server IP Addr** field. 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, check 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, check the **Status** check box and click **Apply** to reenable the WLAN.

Step 11 Click **Save Configuration**.

Configuring DHCP Per WLAN (CLI)

Procedure

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*

DHCP Release Override on Cisco APs

If you are using Microsoft Windows Server 2008 R2 or 2012 as the DHCP server and after an AP or a controller reboot, the AP might fail to associate with the controller because of no valid IP address. This can be caused due to an interoperability issue with the Microsoft server.

When a controller is rebooted, the AP tries to associate with the controller. During this time, the AP keeps renewing the IP address. Every time the AP releases the current DHCP lease, the AP sends out 3 DHCP release packets. This functionality of sending 3 DHCP release packets is common across all Cisco IOS software-based products. Cisco DHCP servers running on various Cisco devices release the IP address when they get the first DHCP release message but ignore the later messages. However, the Microsoft DHCP server marks the AP as BAD_ADDRESS when it receives the second and the third DHCP release packets.

A workaround for this issue is to configure DHCP release override and set the number of DHCP releases sent by AP to 1, on a Cisco AP or all APs by entering this command:

config ap dhcp release-override enable {*cisco-ap* | **all**}

Note We recommend that you use this configuration only in highly reliable networks.

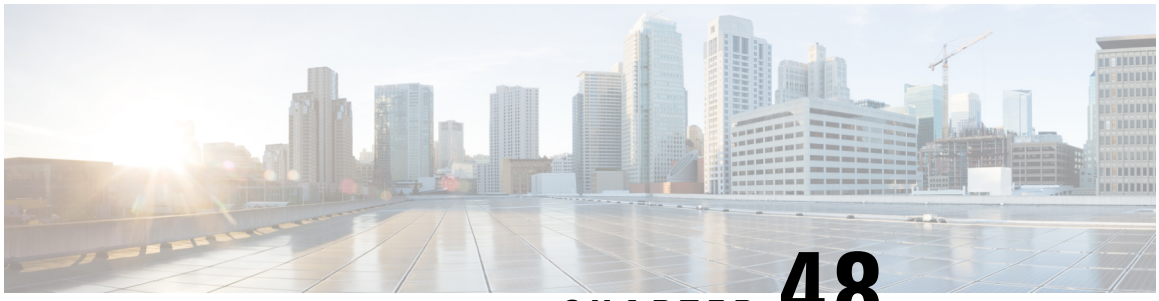
For more information about this issue, see the CSCuv61271 caveat.

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.



CHAPTER 48

Client Data Tunneling

- Ethernet over GRE Tunnels, on page 1051
- Proxy Mobile IPv6, on page 1062

Ethernet over GRE Tunnels

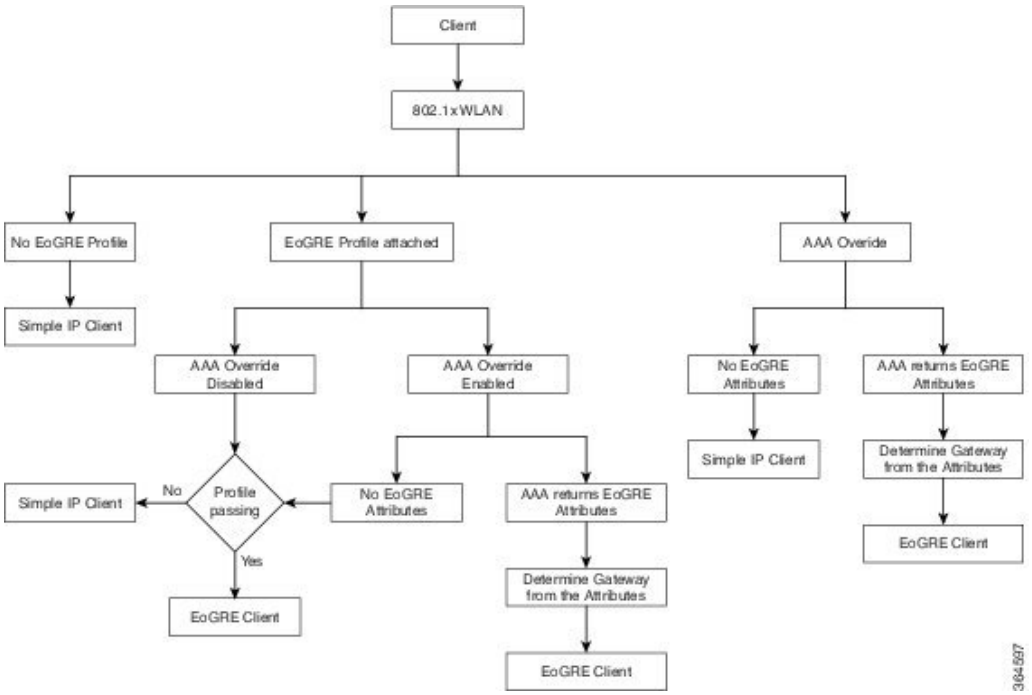
Ethernet over GRE (EoGRE) is an aggregation solution for aggregating Wi-Fi traffic from hotspots. This solution enables customer premises equipment (CPE) devices to bridge the Ethernet traffic coming from an end host, and encapsulate the traffic in Ethernet packets over an IP GRE tunnel. When the IP GRE tunnels are terminated on a service provider broadband network gateway, the end host's traffic is terminated and subscriber sessions are initiated for the end host.

High Availability (HA) is supported for EoGRE IPv4 and IPv6 tunnel configuration. In addition, Client SSO is supported for IPv4 and IPv6 EoGRE tunnel clients.

For more information about designing and deploying EoGRE on controller and Cisco FlexConnect APs, see the EoGRE Deployment Guide.

EoGRE on 802.1X Authentication-based WLANs

Figure 65: Workflow of EoGRE on 802.1X Authentication-based WLANs

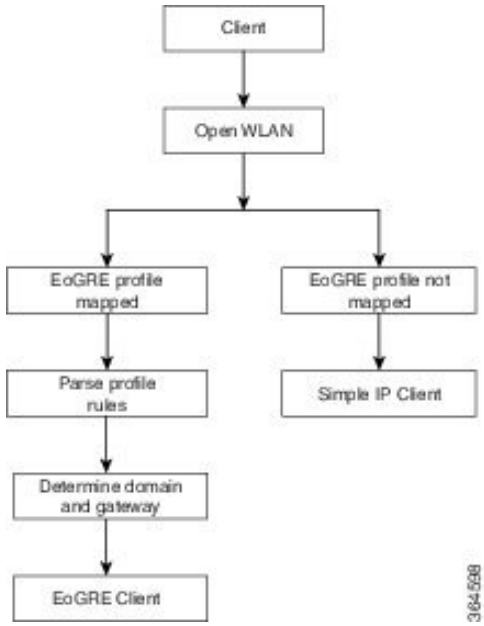


802.1X Authentication	Switching	AP Mode	EoGRE	SimpleIP
Central+No FlexConnect Backup RADIUS Server	Local	Connected	Clients can join as EoGRE.	Clients can join as SimpleIP.
Central+No FlexConnect Backup RADIUS Server	Local	Standalone	New clients cannot join; existing clients should work.	New clients cannot join; Existing clients should work.
Central+No FlexConnect Backup RADIUS Server	Local	Boot in standalone	Clients cannot join.	Clients cannot join.
Local AP Auth+No FlexConnect Backup RADIUS Server	Local	Connected	Clients become SimpleIP.	Clients join as SimpleIP.
Local AP Auth+No FlexConnect Backup RADIUS Server	Local	Standalone	Clients become SimpleIP.	Existing and new clients work as expected.
Local AP Auth+No FlexConnect Backup RADIUS Server	Local	Boot in standalone	Clients become SimpleIP.	Clients can join.

802.1X Authentication	Switching	AP Mode	EoGRE	SimpleIP
Central+FlexConnect Backup RADIUS Server	Local	Connected	Clients join as EoGRE.	Existing and new clients work as expected.
Central+FlexConnect Backup RADIUS Server	Local	Standalone	Existing clients continue as EoGRE; new Client joins as SimpleIP.	Existing and new clients work as expected.
Central+FlexConnect Backup RADIUS Server	Local	Boot in standalone	Clients become SimpleIP.	Existing and new clients work as expected.

EoGRE on Open Authentication-based WLANs

Figure 66: Workflow of EoGRE on Open Authentication-based WLANs



Note For open WLANs, the EoGRE profile must have only one rule, which is a * rule. Mapping of a profile that has multiple rules to an open authentication WLAN is not supported. All clients should be EoGRE clients.

Open Authentication	Switching	AP Mode	EoGRE
Central	Local	Connected	Client will join as EoGRE.

Open Authentication	Switching	AP Mode	EoGRE
Central	Local	Standalone	New clients cannot join. Existing clients should work.
Central	Local	Boot in Standalone	Clients cannot join.

Changing the Tunnel Source

Prior to Release 8.2, the management IP address was used as the tunnel endpoint. Release 8.2 has enabled the specification of any L3 dynamic interface other than the management interface as a tunnel endpoint, if need be.

Support for IPv6

In Release 8.3, support is added for client IPv6 traffic and IPv6 address format for the EoGRE tunnel gateway. Client IPv6 traffic is supported on both IPv4 and IPv6 EoGRE tunnels. A maximum of eight different client IPv6 addresses are supported per client. Controllers send all the client IPv6 addresses that they have learned to the Accounting server in the accounting update message. All RADIUS or Accounting messages exchanged between controllers and tunnel gateways or RADIUS servers are outside the EoGRE tunnel.

CAPWAP	EoGRE	Remarks
CAPWAPv4	EoGREv4	Accounting IP expected to be CAPWAPv4 (controller IP)
CAPWAPv4	EoGREv6	Accounting IP expected to be CAPWAPv4 (controller IP)
CAPWAPv6	EoGREv4	Accounting IP expected to be CAPWAPv6 (controller IP)
CAPWAPv6	EoGREv6	Accounting IP expected to be CAPWAPv6 (controller IP)

One-to-One Mapping of WLAN with EoGRE VLAN

The EoGRE implementation for open WLANs is limited to 10 WLANs per VLAN per controller. This limitation can be overcome by having a one-to-one mapping between open WLANs and EoGRE VLANs.

A one-to-one mapping of a WLAN with an EoGRE VLAN can be achieved by overriding the EoGRE VLAN configuration within the WLAN. All the existing rules are still applicable, but when the EoGRE VLAN override option is enabled, the VLAN ID that you specify will be overridden with the EoGRE VLAN ID that is configured in the tunnel profile that is mapped to the WLAN.

The order of precedence is as follows:

1. If the AAA override option is enabled on the WLAN, the AAA values are applied.
2. If the EoGRE VLAN configuration override option is enabled, the EoGRE VLAN configuration values are applied on the VLAN ID that is specified.
3. Network Access Identifier (NAI) is matched in the EoGRE profile rule.

Related Documentation

- Ethernet over GRE Tunnels
- Service Provider Wi-Fi: Support for Integrated Ethernet Over GRE
- Intelligent Wireless Access Gateway Configuration Guide

Restrictions for EoGRE Tunneling

- On Cisco vWLC, EoGRE tunneling is supported only in local switching mode.
- EoGRE feature is not supported in Cisco Aironet 702, 801, 802, 1520 Access Points.
- It is not possible to edit or delete a tunnel profile if the profile is associated with a WLAN. You must first dissociate the profile from the WLAN and then edit or delete the profile.
- It is not possible to edit or delete a tunnel gateway if the gateway is already associated with a domain. You must first dissociate the tunnel gateway from the domain and then edit or delete the tunnel gateway.
- It is not possible to edit or delete a domain if the domain is already associated with a tunnel profile rule. You must first dissociate the domain from the tunnel profile rule and then edit or delete the domain.
- If the domain is modified on the fly, the client associated with the domain is deauthenticated.
- We recommend that you do not have firewall that could block ICMP packets.
- Tunnel Gateway (TGW) as AAA and RADIUS realm feature on WLAN should not be used together.
- Tunnel Gateway (TGW) as AAA is not supported on EoGRE for FlexConnect APs.
- Tunnel EoGRE gateway statistics are not synced to the standby controller.
- Due to SNMP limitation, tunnel gateway names can be up to 127 characters only.
- For open WLANs, the profile must have only one rule, which is a * rule. Mapping of a profile that has multiple rules to an open authentication WLAN is not supported.
- EoGRE client gets IPV6 address from local switching VLAN.
- Broadcast/Multicast traffic on Local Switching VLAN reaches EoGRE clients.
- FlexConnect+Bridge Mode is not supported.
- Standalone mode: EoGRE client Fast Roaming is not supported.
- WebAuth is not supported.
- FlexConnect AP Local Authentication is not supported.
- FlexConnect AP Backup RADIUS server is not supported.
- EoGRE client with Static IP is not supported.
- FlexConnect ACL on the WLAN does not work for EoGRE clients.
- After Fault Tolerance, client type is SimpleIP. It is changed to EoGRE after a period of 30 seconds.
- MTU of AP gateway should be 1500 bytes.

- Lightweight APs support Path MTU only for EoGREv6. For EoGREv4, it is not supported.
- For EoGRE clients, the TrustSec SGT/Policy Enforcement might not work as expected because it is not supported for any tunneled traffic, including the Layer3 mobility tunnel.

  For tunneled traffic, the source SGT tag is not encoded in the CMD header (CMD header itself not added); the unknown SGACL policy (0,DGT) is applied at the policy enforcement point.
- EoGRE IPv6 Restrictions:
  - EoGRE client gets IPv6 address from local switching VLAN
  - DHCP Option 82 configuration is not supported on IPv6 clients.
  - Applications such as RADIUS, FTP, TFTP, SFTP, LDAP, SXP, syslog, and so on, are supported on only management IPv6 address.
  - Dynamic IPv6 AP-manager interface is not supported.
  - Dynamic interface with IPv6 supports only as tunnel interface.
  - Maximum number of dynamic interface to which IPv6 address can be assigned is16.
  - The IPv6 link local addresses are common for all switched virtual interfaces (SVI) on a switch. Due to this, configuring an IPv6 address on dynamic address fails. To overcome this issue, you must explicitly configure link local address on the uplink switch for SVI. Each SVI should have unique link local address configuration.
  - The IP packets on IPv6 tunnels has a maximum size limit of 1280 bytes on controller.
- When AAA override for a WLAN is enabled, the domain passed through AAA server should be attached to a second WLAN. This is applicable for APs that are in Local and FlexConnect modes. This is required so that the gateways mapped to the domain in AAA server become operational in Local mode in controller and are downloaded to AP in FlexConnect mode.
- Clients connecting to Wave 2 APs get an IP address from the native VLAN in the conditions described in CSCvu46349.

Configuring EoGRE on the Controller (GUI)

Procedure

Step 1 Create tunnel gateways and configure heartbeats:

a) Choose **Controller** > **Tunneling** > **EoGRE**.

b) Select the **Interface Name**.

Interface present on the controller to be used as a source of the tunnel.

c) Set the **Heartbeat Interval**. The default interval is 60 seconds.

The controller sends keepalive pings every 60 seconds.

d) Set **Max Heartbeat Skip Count**. The default value is set to 3.

If the TGW does not reply after three keepalive pings, the controller marks the TGW as nonoperational. The number of skip count decides how many times the TGW can skip consecutive replies, before the controller knows that the TGW is nonoperational.

e) Specify a **TGW Name**.
f) Specify the **TGW IP Address**.

Both IPv4 and IPv6 address formats are supported. You can create up to 10 such tunnel gateways.

g) Specify a **Domain Name**.
h) Specify the tunnel gateway that you created and its role as either primary/active or secondary/standby gateway, and click **Add**.

If the tunnel gateway is reachable, the state should be displayed as UP under the **TGW List**.

Click **Get Statistics** to view tunnel gateway statistics.

Domain represents a virtual collection of one or more tunnels used for redundancy purposes. Up to 16 tunnels can exist in a domain. If one tunnel fails, the traffic is redirected to another TGW.

In a domain, the primary gateway is active by default. When the primary gateway is not operational, the secondary gateway becomes the active gateway. Clients will have to associate again with the secondary gateway. During and after failover, controller continues to ping the primary gateway. When the primary gateway is operational again, the primary gateway becomes the active gateway. Clients then fall back to the primary gateway. The same option is available for the TGW from FlexConnect in local switched mode. EoGRE tunnels can be DTLS encrypted CAPWAP IPv4 or IPv6.

Step 2 Create a tunnel profile:

a) Choose **Controller** > **Tunneling** > **Profiles**.
b) Specify a profile name and click **Add**.

The profile name is displayed under **Profile List**.

Step 3 Define a tunnel profile rule:

a) Click the tunnel profile that you created.
b) Under the **Rule** tab, to map a specific realm to the profile, enter the realm name. A realm is a string after @, for example, user_name@realm. To match any **Realm**, use *, which means all realms are accepted.
c) Choose **Tunnel Type** as **EoGRE**.
d) Set **VLAN** to **0**.
e) Choose the **Gateway Domain** that you created in Step 1.
f) Click **Add** to add the rule to the tunnel profile.

Step 4 Specify tunnel parameters:

a) Under the **Tunnel Parameters** tab, check the **Gateway as AAA Proxy** and **Gateway as Accounting Proxy** (optional) check boxes to configure a tunnel gateway as a AAA proxy and as an Accounting proxy.
b) (Optional) Check the **DHCP Option-82** check box.

Note
DHCP Option 82 configuration is not supported on IPv6 clients.

c) Choose the DHCP Option 82 format as either **Binary** or **ASCII**.
d) Specify the **DHCP Option 82 Delimiter**. The default is ;.
e) Specify the **Circuit-ID** and **Remote-ID** information. You can choose up to five fields each and sort them accordingly.

f) Click **Apply**.

Step 5 Create RADIUS Authentication or Accounting servers or both by specifying the tunnel gateway IP addresses that you specified in Step 1 as the server IP addresses, and enable **Tunnel Proxy**.

For instructions on how to create RADIUS servers, see the *Configuring RADIUS* chapter under *Security Solutions*.

Step 6 Associate the tunnel profile to the WLAN:

a) Choose **WLANs** and click the WLAN ID to which the tunnel profile has to be associated.
b) In the **Advanced** tab, under **Tunneling**, choose the **Tunnel Profile**.
c) (Optional) You can choose to enable AAA Override for the WLAN, which means that the controller is allowed to accept the attributes returned by the RADIUS server.
d) Save the configuration.

Step 7 Verify if the tunnel is correctly configured:

a) Choose **Controller** > **Tunneling** > **Profiles**.
b) Verify if the profile name is mapped to the correct WLAN.

Step 8 Verify the gateway statistics:

a) Choose **Controller** > **Tunneling** > **EoGRE**.
b) Click **Get Statistics**.

Configuring EoGRE on the Controller (CLI)

Procedure

- Configure keepalive ping parameters by entering these commands:
  - **config tunnel eogre heart-beat interval** *seconds*
  - **config tunnel eogre heart-beat max-skip-count** *number*
- Add new EoGRE tunnel gateways, or delete or modify existing gateways, by entering these commands:
  - **config tunnel eogre gateway add** *name* {**ipv4-address** | **ipv6-address**} *ip-addr*
  - **config tunnel eogre gateway delete** *name*
  - **config tunnel eogre gateway modify** *name* {**ipv4-address** | **ipv6-address**} *ip-addr*
- Configure EoGRE tunnel gateway domain by entering these commands:
  - **config tunnel eogre domain** {**create** | **delete**} *domain-name*
  - **config tunnel eogre domain** {**add** | **remove**} *domain-name gateway-name*
- Add primary gateway name to a domain by entering the following command. Secondary gateway is selected automatically after the primary gateway is added.
  - **config tunnel eogre domain primary** *domain-name gateway-name*

In a domain, the primary gateway is active by default. When the primary gateway is not operational, the secondary gateway becomes the active gateway. Clients will have to associate again with the secondary gateway. During and after failover, controller continues to ping the primary gateway. When the primary gateway is operational again, the primary gateway becomes the active gateway. Clients then fall back to the primary gateway. The same option is available for the TGW from FlexConnect in local switched mode. EoGRE tunnels can be DTLS encrypted CAPWAP IPv4 or IPv6. This feature is supported on all Wave 1 and Wave 2 APs that are supported in this release.

- Configure tunnel profiles by entering these commands:
  - **config tunnel eogre profile** {**create** | **copy** | **delete** | **rule** | **eogre**}

  Follow the instructions displayed in the CLI to configure each parameter.
- Configure the gateway as AAA proxy by entering these commands:
  - **config tunnel profile eogre** *profile-name* **gateway-radius-proxy** {**enable** | **disable**}
  - **config tunnel profile eogre** *profile-name* **gateway-radius-proxy accounting** {**enable** | **disable**}
- Configure DHCP Option 82 for the tunnel profile by entering these commands:

Note DHCP Option 82 configuration is not supported on IPv6 clients.

  - **config tunnel profile eogre** *profile-name* **DHCP-Opt-82** {**enable** | **disable**}
  - **config tunnel profile eogre** *profile-name* **DHCP-Opt-82 format** {**binary** | **ascii**}
  - **config tunnel profile eogre** *profile-name* **DHCP-Opt-82 delimiter** *character*
  - **config tunnel profile eogre** *profile-name* **DHCP-Opt-82** {**circuit-id** | **remote-id**} *supported-parameter*
- Configure EoGRE tunnel interface by entering the following command:
  - **config tunnel eogre interface** *interface-name*

Note Before configuring the interface for the tunnel source, disable the WLAN associated with the interface.

- View details about EoGRE tunneling by entering these commands:
  - **show tunnel eogre** {**domain** | **gateway**} **summary**

Note The **show tunnel eogre gateway summary** command lists details of only the FlexConnect central switching clients and Local Mode AP clients. To view the details of FlexConnect local switching clients, use the **show ap eogre gateway** *ap-name* command.

- **show tunnel eogre summary**
- **show tunnel eogre statistics**
- **show tunnel eogre gateway statistics**
- **show tunnel profile summary**
- **show tunnel profile detail** *profile-name*

Configuring EoGRE for FlexConnect APs (GUI)

- Ensure that the APs are in FlexConnect mode.
- The tunnel configurations made for the controller also applies to Cisco FlexConnect APs when the tunnel profile is associated with a WLAN.
- Path MTU discovery is supported on FlexConnect APs

Procedure

Step 1 Choose **WLANs** > **WLANs**.

Step 2 Click the WLAN ID.

Step 3 In the **Advanced** tab under **FlexConnect**, enable **FlexConnect Local Switching**.

Note
Only FlexConnect Local Switching option has to be configured on the FlexConnect AP or FlexConnect Group to enable FlexConnect AP tunnel.

Step 4 Save the configuration.

Step 5 To view the statistics per gateway, choose **Wireless** > **All APs** > **AP name** > **FlexConnect** > **Tunnel Gateway List** and click **Get Statistics**.

Configuring EoGRE for FlexConnect APs (CLI)

- Ensure that the APs are in FlexConnect mode.
- The tunnel configurations made for controller also applies to Cisco FlexConnect APs when the tunnel profile is associated with a WLAN.

Procedure

Step 1 Enable Local Switching on FlexConnect APs associated with a WLAN by entering this command:
config wlan flexconnect local-switching *wlan-id* **enable**

Step 2 Monitor the EoGRE configurations by entering this command:

show ap eogre {**domain** | **gateway**} *ap-name*

Note
The **show ap eogre gateway** *ap-name* command lists details of FlexConnect local switching clients. To view the details of FlexConnect central switching clients and Local Mode AP clients, use the **show tunnel eogre gateway summary** command.

To see the tunnel gateway statistics in controller, use the **show tunnel eogre gateway statistics** command.

To see the tunnel gateway statistics in AP, use the **show ap eogre statistics** *ap-name* command.

One-to-One Mapping of WLAN with EoGRE VLAN (GUI)

Before you begin

- Ensure that you have created an EoGRE tunnel profile.
- Ensure that the WLAN is in disabled state before you proceed with this procedure.

Procedure

Step 1 Choose **WLANs** and click the WLAN ID.
Step 2 Click the **Advanced** tab and scroll down to the **Tunneling** section.
Step 3 Select the tunnel profile.
Step 4 Check the **EoGRE VLAN Override** check box to enable the EoGRE VLAN override feature on the WLAN.
Step 5 In the **EoGRE VLAN Override ID** field, enter the VLAN ID that should be overridden with the EoGRE VLAN ID configured in the tunnel profile.
Step 6 Save the configuration.

One-to-One Mapping of WLAN with EoGRE VLAN (CLI)

Before you begin

- Ensure that you have created an EoGRE tunnel profile.
- Ensure that the WLAN is in disabled state before you proceed with this procedure.

Procedure

Step 1 Enable the EoGRE VLAN override feature on a WLAN by entering this command:

config wlan tunnel eogre-vlan-override *wlan-id* **enable**

Step 2 Configure the VLAN ID that should be overridden with the EoGRE VLAN ID configured in the tunnel profile by entering this command:

config wlan tunnel eogre-vlan-override *wlan-id vlan-id*

Step 3 Monitor the configuration on the WLAN by entering this command:

show wlan *wlan-id*

Step 4 View the client details, including the EoGRE VLAN ID being used, by entering this command:

show client detail *client-mac-addr*

What to do next

You can troubleshoot issues related to this feature by using the **debug client** *client-mac-addr* command:

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 Controller implements the MAG functionality.

For PMIPv6 clients, the controller 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.

MAG on AP is supported on FlexConnect mode APs in a locally switched WLAN. For PMIPv6 clients, all the data traffic from clients is tunneled to the LMA in the Generic Routing Encapsulation (GRE) tunnel established between the MAG and the LMA. Similarly, all the packets received from the LMA in the GRE tunnel are routed to the wireless client.

After the 802.1X authentication is complete, the Cisco AP starts PMIPv6 signaling for the client. In a MAG-on-AP scenario, the Cisco AP starts PMIPv6 signaling. In a MAG-on-controller scenario, the controller starts PMIPv6 signaling.

Fast Roaming with Central Association

Fast roaming is supported when central association is enabled on WLANs. When central association is enabled, all key cachings occur on the controller. When a PMIPv6 client roams from one AP to another on the same mobility domain, the controller sends the PMIPv6 parameters of the client to a new AP in PMIPv6 tunnel payload to start PMIPv6 signaling. Also, the controller sends the PMIPv6 tunnel payload to the old AP to tear down the Generic Routing Encapsulation (GRE) tunnel for the client with the LMA. Fast roaming is supported in both intra-controller and inter-controller roaming scenarios and mobility messages are added to send PMIPv6 parameters from one controller to another during roaming.

Client roaming from third-party MAG to Cisco AP-MAG is similar to a new client joining; a client roaming away from a Cisco AP-MAG to a third-party MAG is similar to a client leaving, and therefore, requires no special handling.

With Cisco APs in FlexConnect mode, all reassociation requests from clients are handled by the Cisco APs themselves. However, if central association is enabled, all reassociation requests are handled by the controller.

Dynamic AAA Attributes

The dynamic AAA attributes that are supported are listed below:

Type	Attribute	Value	Description	Controller 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	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	Controller 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)
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 controller (Mandatory). **Note** The GRE tunnel creation is still static.
26/9/1	mn-service	ENUM: "IPv4"	Type of client	Only IPv4 is supported.

Changing the Tunnel Endpoint

In releases prior to Release 8.2, the management IP address was used as the tunnel endpoint. Release 8.2 added the capability to specify a tunnel endpoint, other than management interface.

Note This feature currently supports EoGRE and PMIPv6 types of tunnels for mobility tunnel termination.

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 MAG on AP is supported only when AP is in FlexConnect mode and WLAN is configured for FlexConnect Local Switching. If the WLAN is configured for Central Switching, MAG on controller is used.
- PMIPv6 on FlexConnect ACL with local switching is not supported.
- MAG on AP is not supported for clients in a centrally switched WLAN.
- IPv6 addresses on dynamic interfaces are not supported.
- Intercontroller roaming from PMIPv6 to non-PMIPv6 WLANs is not supported.

Configuring Proxy Mobile IPv6 (GUI)

Procedure

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.
- **Interface**—Interface on the the controller used as a source for PMIPv6 tunneling.
- **MAG APN**—Access Point Name (APN) if you have subscribed to a MAG.

  MAG can be configured for one of the following roles:

  - 3gpp—Specifies the role as 3GPP (Third Generation Partnership Project standard)
  - lte—Specifies the role as Long Term Evolution (LTE) standard
  - wimax—Specifies the role as WiMax
  - wlan—Specifies the role as WLAN

  By default, the MAG role is WLAN. However, for lightweight access points, the MAG role should be configured as 3GPP. If the MAG role is 3GPP, it is mandatory to specify an APN for the MAG.
- **Maximum Bindings Allowed**—Maximum number of binding updates that the controller can send to the MAG. The valid range is between 0 and 40000.
- **Binding Lifetime**—Lifetime, in seconds, of the binding entries in the controller. 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 controller. 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 controller 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 controller 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 controller 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 controller 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 controller 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 controller.
   - **Member IP Address**—IP address of the LMA connected to the controller.
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)

Procedure

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.

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*

- Add an APN for a MAG by entering this command:

  config pmipv6 mag apn *apn-name*

  A MAG can be configured for one of the different roles:

  - 3gpp—Specifies the role as 3GPP (Third Generation Partnership Project standard)
  - lte—Specifies the role as Long Term Evolution (LTE) standard
  - wimax—Specifies the role as WiMax
  - wlan—Specifies the role as WLAN

  Note
  By default, the MAG role is WLAN. However, for the lightweight access points, the MAG role should be configured as 3GPP. If the MAG role is 3GPP, it is mandatory to specify an APN for the MAG.

- Delete an APN by entering this command:

  config pmipv6 delete mag apn *apn-name*

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 {**enable** | **disable**} {*wlan-id* | **all**}

- Configure the profile name for a PMIPv6 WLAN by entering this command:

  config wlan pmipv6 profile-name {**none** | *name*} *wlan-id*

Step 6 Configure a PMIPv6 interface name by entering this command:

config pmipv6 interface *interface-name*

Note
Before configuring the interface for the tunnel source, you should disable the WLAN associated with the interface.

Step 7 Save your changes by entering this command:

save config

Step 8 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:

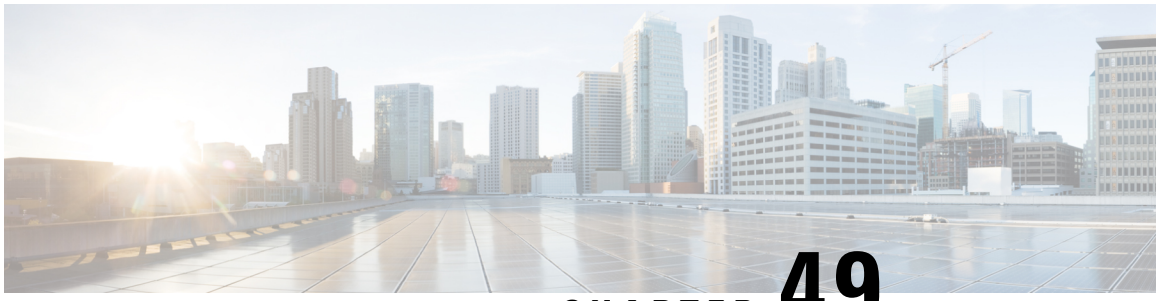
  show pmipv6 mag bindings {**lma** *lma-name* | **nai** *nai-name*}
- See statistical information about MAG by entering this command:

  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 49

AP Groups

- Access Point Groups, on page 1071
- 802.1Q-in-Q VLAN Tagging, on page 1077
- Captive Portal Configuration for AP Groups, on page 1079

Access Point Groups

AP groups are logical groupings of APs within a geographic area such as a building, floor, or remote branch office that share common WLAN, RF, Hotspot 2.0 and location configurations. AP groups are useful in a Cisco wireless network deployment because they allow network administrators to assign specific configurations to different groups of APs. For example, AP groups can be used to control which WLANs are advertised in different buildings in a campus, the interface or interface group WLAN clients are assigned or the RRM and 802.11 radio parameters for radios in specific coverage areas to support high-density designs.

The following AP group specific configurations are supported:

- CAPWAP Preferred Mode: Used to determine if APs prefer IPv4 or IPv6 CAPWAP modes.
- NAS-ID: Used by the controller for RADIUS authentication and accounting.
- WLAN: WLAN assignments, interface or interface group mappings and NAC state.
- RF Profile Assignments: 802.11, RRM, high density and client load balancing configurations.
- Hotspot 2.0: 802.11u venue configuration and languages.
- Location: Hyperlocation configuration.

By default, each AP is automatically assigned to a default AP group named *default-group* and WLANs IDs 1 to 16 map to this default group. You must define a custom AP group for WLANs with IDs greater than 16. You must manually assign APs to custom AP groups. The default group cannot be deleted.

For more information about designing and configuring AP groups, see "AP Groups" in the *Enterprise Mobility Design Guide*:

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/cuwn.html#pgfId-1281292

This section contains the following subsections:

Restrictions for Configuring Access Point Groups

- If you create a WLAN with an ID that is greater than 16, in the default access point group, the WLAN SSID is not be broadcast by APs in the default group.
- If you configure an AP group with an interface mapped to a WLAN, where the interface is the same as is globally mapped for the WLAN, and you reconfigure the global WLAN to map to a different interface, the AP group's WLAN's interface mapping is changed accordingly. For more information, see CSCvb47834.
- 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.
- 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.
- The values of the USB module/External module in the AP *default-group* can be modified. However, these changes are valid only for the current session, and the values reset to default during the next controller reboot. Also, these values are not included during the export and import of the configuration file.

Configuring Access Point Groups

Procedure

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)

Procedure

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** field, enter the group's name.

Step 4 In the **Description** field, enter the group's description.

Step 5 In the **NAS-ID** field, 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 is displayed 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.

Note
Custom configurations on the *default-group* are not saved and are valid till the next controller reboot only.

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 field 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 Check 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 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 is displayed as `default-group`.

Step 17 Check 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, check 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, check the check box to the left of the access point name and click **Remove APs**. To select all of the access points at once, check 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

Note
This step is applicable to the following modules:

- AoA-based which is applicable for AP3600 and AP3700 with Hyperlocation module
- PRL-based which is applicable for AP without module (AP700/AP1700/AP2600/AP2700/AP3600/AP3700) as well as AP3600 and AP3700 with NOS module

In the **Location** tab, do the following:

a) Enable or disable Hyperlocation.

Based on AP and installed module, checking the **Enable Hyperlocation** check box enables different location service (PRL-based or AoA-based).

b) Enter **Packet Detection RSSI Minimum (dBm)** value.

This is the minimum level at which a data packet can be heard by the WSM modules for use in location calculations. The default values is –100 db.

We recommend that this value be increased if you want to have only strong signals used in calculating locations.

c) Enter **Scan Count Threshold for Idle Client Detection** value.

The Scan Count Threshold represent the number of off-channel scan cycles the AP will wait before sending a Block Acknowledgment Request (BAR) to idle clients. The default value of 10 corresponds to approximately 40s, depending on the number of channels in the off channel scan cycle.

d) Enter the IP address of the **NTP Server**.

This is the IP address of the NTP server that all AP that are involved in this calculation need to sync to.

We recommend that you use the same NTP server as is used by the general controller infrastructure. The scans from multiple AP needs to be synced up for the location to be accurately calculated. An IPv4 address is required.

Note
For more information about Cisco Hyperlocation solution, see this document.

Step 20 In the **RF Profile** tab, choose the RF profile for APs with 802.11a and 802.11b radios and click **Apply**. Applying an RF profile results in a reboot of all the APs associated with the AP group.

Step 21 [Optional] In the **Ports/Module** tab do the following:

a. Check the **USB Module** check box to enable USB module for the AP group.

b. Click **Apply**.

Step 22 Click **Save Configuration**.

Creating Access Point Groups (CLI)

Procedure

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**}

- **802.11a-only**: All enabled rates in 5 GHz; 2.4 GHz is disabled.
- **802.11bg** and **802.11g-only**: All enabled rates in 2.4 GHz; 5 GHz is disabled.
- **all**: All enabled rates in 2.4 GHz and 5 GHz.

Note
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 [Optional] To configure the USB module for the AP group, enter this command:

config wlan apgroup port usb-module *default-group* {**enable** | **disable**}

Step 9 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:

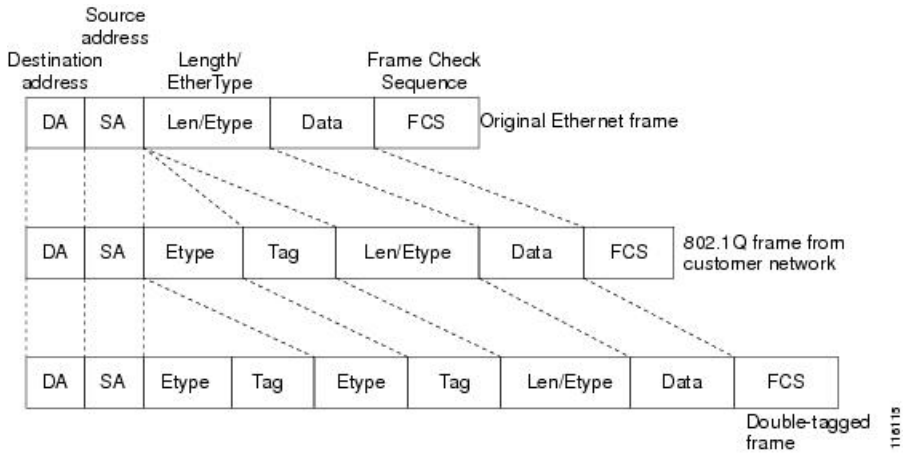
  debug group {**enable** | **disable**}

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 67: 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)

Procedure

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 Check the **Enable Client Traffic QinQ** check box to enable 802.1Q-in-Q VLAN tagging for the AP group.

Step 5 Check 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** field, enter the VLAN ID for 802.1Q-in-Q VLAN tagging.

Step 7 Click **Apply**.

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

Procedure

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
```

Captive Portal Configuration for AP Groups

This feature enables you to configure multiple web authentication URLs (including external captive URLs) for the same SSID based on an AP group. The default setting is to use the Global URL for authentication. The override option is available at WLAN and AP Group level.

The order of precedence is:

1. AP Group
2. WLAN
3. Global config

This table shows the URL authentication matrix based on the override options set in the controller.

Table 45: Authentication URL Based on the Override Settings

Global at WLAN level	Global at AP Group level	Custom Authentication URL
Enabled	Enabled	Globally configured URL
Disabled	Enabled	WLAN configured URL
Enabled	Disabled	AP Group Level configured URL

Global at WLAN level	Global at AP Group level	Custom Authentication URL
Disabled	Disabled	AP Group Level configured URL

Restrictions for Captive Portal Configuration for AP Groups

- This configuration is supported in a standalone controller only.
- Export-Anchor configuration is not supported.

Configuring Captive Portal for an AP Group (GUI)

Procedure

Step 1 Choose **WLANs** > **Advanced** > **AP Groups** to open the **AP Groups** page.

Step 2 Click the AP group name to open the corresponding **AP Group** > **Edit** page.

Step 3 Check the **Custom Web Override-Global** check box to enable the custom authentication website.

Note
You cannot enable this option on the default AP group.

Step 4 Enter the authentication URL in the **External Web auth URL** field.

Step 5 Save the configuration.

Configuring Captive Portal for an AP Group (CLI)

Procedure

- Configure the AP group custom-web by entering this command:

  config wlan apgroup custom-web global *ap-groupname* {**enable | disable**}

- Configure an external web authentication URL for an AP Group by entering this command:

  config wlan apgroup custom-web ext-webauth-url {**add** *apgroupname ext-webauth-url* | **delete** *apgroupname*}

- View the WLAN AP group settings by entering this command:

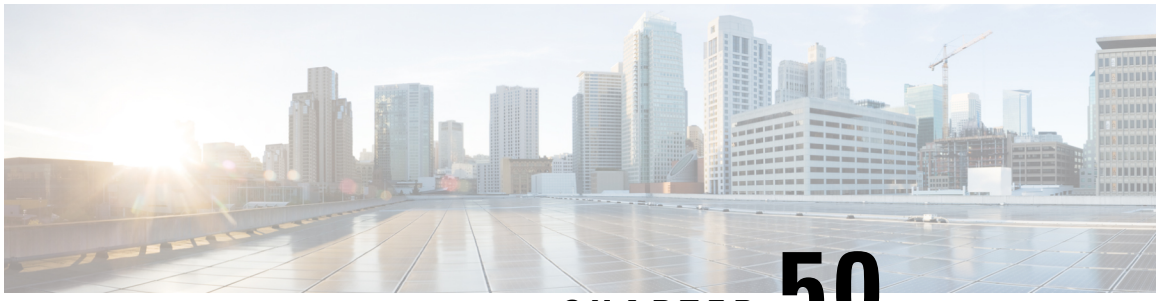
  show wlan apgroups

- Enable debugging for up to 10 clients by entering this command:

  debug client *mac-addr*

- Enables [disables] debugging for the client web authentication redirect by entering this command:

  debug web-auth redirect {**enable | disable**} **mac** *mac-addr*



CHAPTER 50

Workgroup Bridges

- Cisco Workgroup Bridges, on page 1081
- Non-Cisco Workgroup Bridges, on page 1128
- Cisco Wave 2 Access Points as Workgroup Bridges, on page 1129

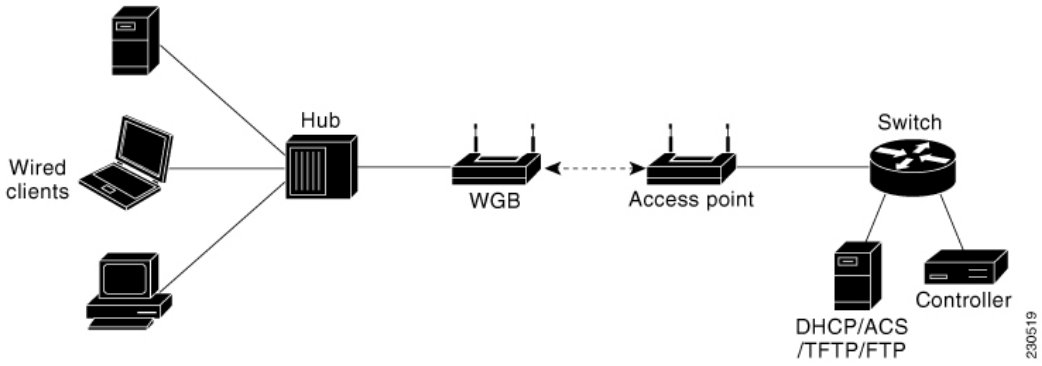
Cisco Workgroup Bridges

A workgroup bridge (WGB) is a Cisco access point that can be configured in a mode that permits it to associate with a wireless infrastructure, providing network access on behalf of wired clients. The WGB mode is supported on autonomous IOS (Wave 1) APs and on some Wave 2 APs.

A Cisco WGB provides information about its wired clients via Internet Access Point Protocol (IAPP) messaging. This enables the wireless infrastructure to know the MAC addresses of the WGB's wired clients. Up to 20 wired clients are supported behind a Cisco WGB.

In 8.10 release, the following APs support WGB operational mode: 2800, 3800, 4800, 1560 and 6300.

Figure 68: WGB Example



Note If the lightweight access point fails, the WGB attempts to associate to another access point.

- The following features are supported for use with a WGB:
  - Guest N+1 redundancy

  - Local EAP
  - Open, WPA+TKIP, WPA2+AES, LEAP, EAP-FAST, PEAP, 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.

This section contains the following subsections:

Guidelines and Restrictions for Cisco Workgroup Bridges

- The WGB can associate only with Cisco lightweight access points.
- The following features are not supported for use with a WGB:
  - Idle timeout
  - Web authentication
- Aironet WGBs are not supported if the parent AP is configured for FlexConnect local switching with local authentication, if the parent AP is a Wave 2 AP (that is, 802.11ac Wave 2 or 802.11ax). For more information, see CSCvh22645.
- 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 deauthenticate a WGB record from a controller, all of the WGB wired clients' entries 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.
- Associating a WGB to a WLAN that is configured for Adaptive 802.11r is not supported.

Workgroup Bridge (WGB) Downstream Broadcast On Multiple VLANs

Release 8.3 provides an enhancement to broadcast traffic support on multiple 802.1Q VLAN workgroup bridge (WGB) deployments that traverse mesh networks and in Local mode. Specifically, support for WGB downstream broadcasts over multiple VLANs (to differentiate and prioritize traffic); and, bridging of VLAN traffic to wired clients connected to the WGB. Applications for this functionality are commonly found in the transportation and mining industries. For more information, see CSCub87583.

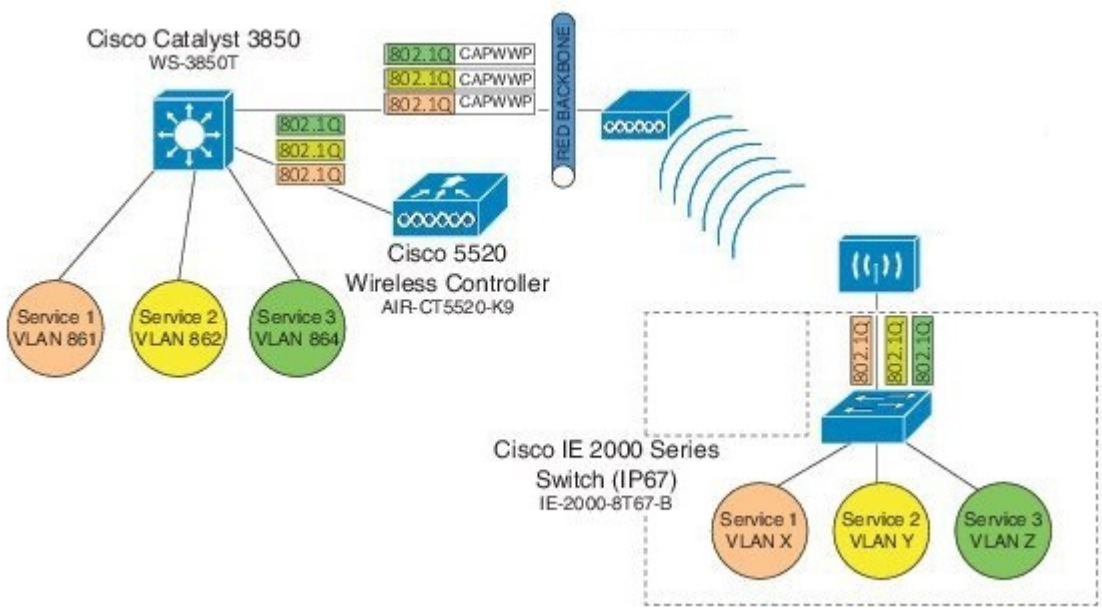
Supported platforms:

- Access point (AP) and WGB support:
  - IW3700 Series

Supported AP mode:

- Local mode
- Bridge mode

Figure 69: Workgroup Downstream Broadcast on Multiple VLAN



Prerequisites

You need to create the dynamic interfaces and bind them to the interface group before you proceed with the configuration.

1. Create the dynamic interfaces, by choosing **CONTROLLER** > **Interfaces** > **New** on controller. Add any dynamic interface that needs to support the downstream broadcast on Multiple VLANs feature into the interface group.
2. Bind the dynamic interfaces with Interface Groups, by choosing **CONTROLLER** > **Interface Groups** > **Add Group** on controller.
3. Bind the Interface Groups to WLAN. Choose **WLAN**. Under the specific WLAN General confirmation tab, choose the proper interface group.

Cisco Wireless Controller Configuration (CLI Only)

To enable or disable the downlink broadcast packet VLAN tagging on a WLAN (new command):

`(Cisco Controller) >`**config wlan wgb broadcast-tagging** {**enable** | **disable**} *wlan-id*

Note This feature is disabled by default.

Note To enable this feature, you need to enable **Broadcast Forwarding** on controller, by choosing **Controller** > **General** and choose **Enabled** from the **Broadcast Forwarding** drop-down list.

Note To enable this feature, you should also configure the AP Multicast Mode to Multicast rather than Unicast, by clicking **Controller** > **General** > **AP Multicast Mode** and choosing **Multicast**, and then assign Multicast Group Address.

WGB Configuration (CLI Only)

You can configure the following on Workgroup Bridges:

- Broadcast Tagging
- Native VLANs

By default, Broadcast Tagging is disabled.

By default, only Native VLAN broadcasts can be forwarded to wired clients in Native VLANs.

You use the no command to disable VLAN configurations on the WGB as shown in the examples below.

Note When you have multiple VLAN configurations on WGB, you need to configure the encryption cipher mode and keys as the following example shows:

```
encryption vlan 861 mode ciphers aes-ccm
encryption vlan 862 mode ciphers aes-ccm
encryption vlan 864 mode ciphers aes-ccm
```

Then, you should configure the encryption cipher mode globally on the multicast or broadcast interface by entering the following command:

```
encryption mode ciphers aes-ccm
```

VLAN Broadcast Tagging Configuration

- To enable broadcast tagging on a VLAN (new command):

  `(WGB) (config)#`**workgroup-bridge unified-vlan-client broadcast-tagging**

- To disable broadcast tagging on a VLAN:

  `(WGB) (config)#`**no workgroup-bridge unified-vlan-client broadcast-tagging**

Note The **no workgroup-bridge unified-vlan-client broadcast-tagging** command will disable **workgroup-bridge unified-vlan-client** as well. Make sure you have **workgroup-bridge unified-vlan-client** configured properly to enable the multiple vlan feature.

Reliable WGB Downstream Broadcast for Multiple VLANs

Release 8.10.130.0 provides an enhancement for the Workgroup Bridge (WGB) Downstream Broadcast On Multiple VLANs, on page 1083 feature, which was first introduced in Release 8.3. Legacy broadcast without 802.11 ACK mechanism's may have more chance to cause packet loss over the air. With reliable downstream broadcast feature, broadcast packet can be converted to unicast packet. Hence the Root AP will receive the ACK for converted broadcast packet and retransmit in case of missing ACK.

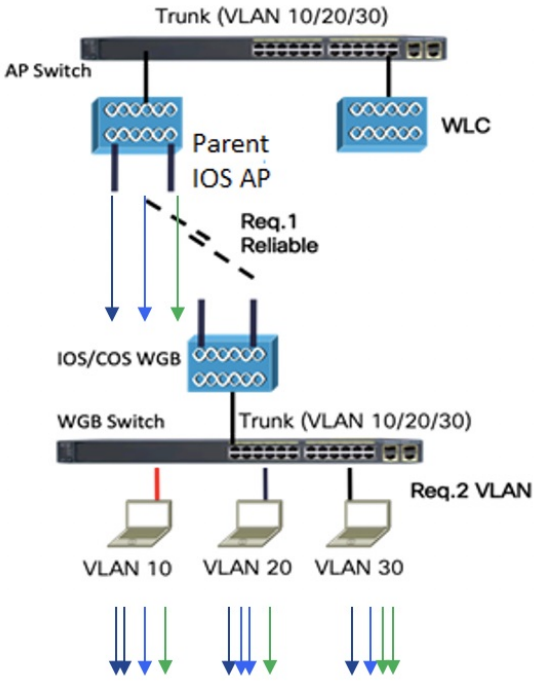
The converted unicast packet's header will be changed from 3-address to 4-address format. WGB's MAC address will be used as receiver address (RA) instead of broadcast address and special multicast address with VLAN information will be used as destination address (DA). This BC2UC conversion for multiple VLAN's is possible for WGB and its wired clients. Since the converted packet is a unicast packet, Root AP will receive the ACK for each packet and retransmit based on the retry logic by the Root AP for every ACK which is not received for this broadcast to unicast conversion.

Note This enhancement is for WGB and its wired clients. It will not impact the non-WGB wireless clients.

- Supported AP platforms:
  - Cisco Industrial Wireless 3700 Series Access Points
  - Cisco Aironet 1570 Series Access Points
- Supported WGB platforms:
  - Cisco Industrial Wireless 3700 Series Access Points
- Supported AP modes:
  - Local
  - Bridge

As shown in the following figure, a WGB with wired clients of three different VLANs (VLAN 10, 20, and 30) joins the IOS AP wireless network. The broadcast traffic from AP to WGB will be transmitted to the clients with corresponding VLAN and retransmission will happen if traffic is lost on air.

Figure 70: WGB Bridged Network



The Receiver address (RA) of legacy broadcast packet is FF:FF:FF:FF:FF:FF and there will not be any retransmission if the packet is lost in the air. The reliable downstream broadcast feature replaces this RA with WGB address and Destination address (DA) with special multicast address 01:00:5e:80:xx:xx. This will make the packet as a unicast packet and enables ACK mechanism. The packet will be retransmitted when the ACK is not received.

The multicast address **01:00:5e:80:xx:xx** is introduced to transmit the VLAN information between AP and WGB. The VLAN value is embedded in 2 LSB of this multicast address. Both IOS and COS WGB support to decode this type of packet.

Root AP will make "N" copies for single broadcast packet for "N" WGBs associated to it on the specific VLAN. Also, non-converted packet will be sent for the benefit of non-WGB clients. Broadcast packets will not get converted if there is no WGBs associated on the specific VLAN.

QOS behavior:

- The new packet is a 802.11e Qos data.
- The 802.11e QoS priority of reliable broadcast packets will follow multicast default priority value from WLAN's QOS configuration.

The configuration similarities and changes between Release 8.10.130.0 and Release 8.3 are as following:

- **Similarities:**
  - Dynamic interface for all VLANs must be created on the controller. It is necessary for multi-vlan support in both Release 8.10.130.0 and Release 8.3.
  - Broadcast-tagging configurations are same on controller and WGB for both Release 8.10.130.0 and Release 8.3.

- **Changes:**
  - Interface-group must be configured in Release 8.3 to support downstream multiple VLANs. But in 8.10.130.0, it can be supported with or without interface-group configuration on the WLAN.
  - Broadcast packets are converted to multicast packets by Root AP in Release 8.3. While in Release 8.10.130.0, broadcast packets will be converted to unicast packets by Root AP.

The following figures illustrate an example of 802.11 packet forwarding from VLAN 106 (0x006a). The receiver address changes from FF:FF:FF:FF:FF:FF to the MAC address of WGB Radio (d4:c9:3c:e3:16:ec), and the destination address changes from FF:FF:FF:FF:FF:FF to 01:00:5E:80:**00**:**6a** (the last two bytes in MAC address represents corresponding VLAN in hexadecimal).

Figure 71: Normal Broadcast Packet

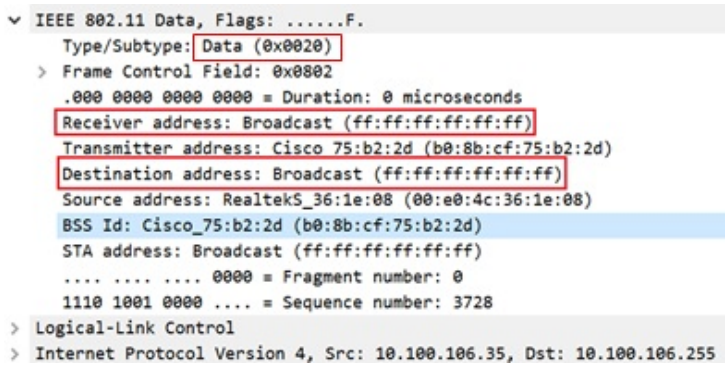
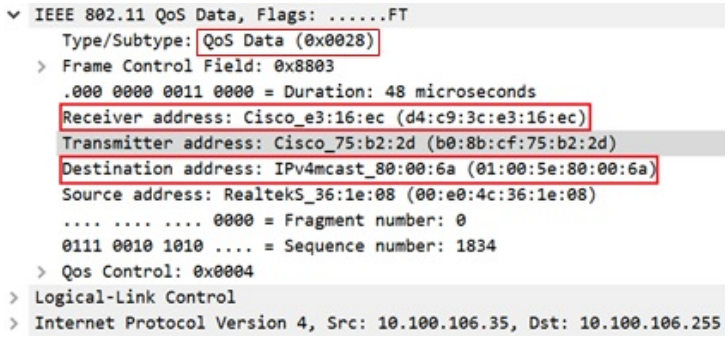


Figure 72: Reliable Broadcast Packet



Controller Configuration

This section provides the basic configuration for AireOS controller.

- To enable or disable reliable broadcast traffic for IOS AP, configure broadcast-tagging on the WLAN from AireOS controller:

  ```
  (Cisco Controller)> config wlan wgb broadcast-tagging <enable|disable> <wlan-id>
  ```

- To support reliable broadcast feature, basic broadcasting forwarding and global multicast feature should be enabled on controller first. The following commands are for basic broadcast forwarding and global multicast configuration.
  - To enable global broadcast forwarding:

```
(Cisco Controller)> config network broadcast enable
```

- To configure AP multicast mode:

```
(Cisco Controller)> config network multicast mode multicast multicast_Group_Address
```

WGB Configuration

To support multiple VLAN on IOS WGB, the following CLI should be configured on WGB:

```
WGB(config)#workgroup-bridge unified-vlan-client
```

To enable broadcast tagging on a VLAN:

```
WGB(config)#workgroup-bridge unified-vlan-client broadcast-tagging
```

To disable broadcast tagging on a VLAN:

```
WGB(config)#no workgroup-bridge unified-vlan-client broadcast-tagging
```

WGB will received both FF:FF:FF:FF:FF:FF and 01:00:5e:80:xx:xx packet on the native VLAN. By default, WGB will forward the normal broadcast (FF:FF:FF:FF:FF:FF) and discard the reliable broadcast (01:00:5e:80:xx:xx). If the CLI is enabled, WGB will forward the reliable broadcast (01:00:5e:80:xx:xx) to corresponding VLAN's wired client and discard the normal broadcast (FF:FF:FF:FF:FF:FF).

Troubleshooting Reliable Broadcast

This section describes the troubleshooting of reliable broadcast on controller, Root AP, and WGB.

- Troubleshooting on controller:
  - Use the **show wlan** <*wlanid*> command to check if broadcast tagging is enabled.

```
(WLC) > show wlan 3
Universal Ap Admin.............................. DisabledBroadcast
Tagging.............................. Enabled
```

  - Use **debug capwap payload enable** to check the mgid information sent to AP.

```
*spamApTask0: Feb 19 18:14:51.384: b0:8b:cf:75:b2:20 L2_MCAST_MGID_INFO : payload
0 addOrDelete 1, mgidByte[0] 0, mgidByte[1] 10
*spamApTask0: Feb 19 18:14:51.384: b0:8b:cf:75:b2:20 MCAST_MGID_INFO_PAYLOAD vapId
 3, isL3Mgid FALSE, numOfMgid 1, vlanInterfaceId 10
```

  - Use the **debug pem events** command to check the association of WGB and its wired clients.

```
*iappSocketTask: Feb 19 14:05:38.379: 00:e0:4c:53:44:58 sending to spamAddMobile
(wgb wired client) vlanId 106 mgid 11 numOfMgid 1
```

- Troubleshooting on Root AP:
  - Use the **show capwap mcast mgid all** command to display L2 MGID information.

```
IOS-AP#show capwap mcast mgid all
L2 MGID Information:
 L2  MGID = 0       WLAN bit map (all slots) = 0x0001 VLAN ID = 103
  Slot map/tx-cnt: R0:0x0001/3446 R1:0x0001/3446 R2:0x0001/0
 L2  MGID = 1       WLAN bit map (all slots) = 0x0001 VLAN ID = 0
  Slot map/tx-cnt: R0:0x0001/7828 R1:0x0001/7828 R2:0x0000/0
 L2  MGID = 11      WLAN bit map (all slots) = 0x0001 VLAN ID = 106
  Slot map/tx-cnt: R0:0x0001/14 R1:0x0001/14 R2:0x0001/0
```

- Use the **show capwap mcast mgid id** <*mgid value*> command to display the details of a specific MGID.

```
IOS-AP#show capwap mcast mgid id 11
L2 MGID = 11     WLAN bit map (all slots) = 0x0001 VLAN ID = 106
  Slot map/tx-cnt: R0:0x0001/979 R1:0x0001/979 R2:0x0001/0

rx pkts = 979
tx packets:
wlan  :     0     1     2     3     4     5     6     7     8     9    10    11
 12    13    14    15
slots0 :     0     0     0     0     0     0     0     0     0     0     0     0
   0     0     0     0
slots1 :   979     0     0     0     0     0     0     0     0     0     0     0
   0     0     0     0
slots2 :     0     0     0     0     0     0     0     0     0     0     0     0
   0     0     0     0
 Reliable BCAST Clients: 1 Client: d4c9.3ce3.16ec    --- SlotId: 1   WlanId: 0
ConvertedBCASTtx: 263
```

- Use the **debug capwap mcast** command to get the information of WGB and its wired clients added to the BC2UC client list.

```
*Dec 19 21:09:29.795: CAPWAP MCAST: capwapAddEntryToL2MgidList:Added new client
d4c9.3ce3.16ec to mgid 11 list of vlan 105, Total clients in this list: 1.
*Dec 19 21:10:56.491: CAPWAP MCAST: capwapAddEntryToL2MgidList:Added new client
d4c9.3ce3.16ec to mgid 10 list of vlan 106 for wired client f076.1cdc.b22c, Total
clients in this list: 1.
```

- Use **debug dot11 dot11radio <0|1> trace print xmt** to check the transmission of original and converted broadcast packet.

```
Converted Packet(4-address format):
*May  6 14:04:40.859: 613B6145 t a8.1b2s0  - 8803 000 48B89C 75B22C m01005E 16F0
361E08 q4 l92
   IP 10.100.106.255 < 10.100.106.56 f1-0-0 id 0 ttl64 sum 50AA prot 1 len 84
  ICMP ping code 0 chk F4D7, id 20765 seq 330
  CF77 B25E 0000 0000 6F17 0100 0000 0000 1011 1213 1415 1617 1819 1A1B 1C1D

Original packet (3-address format):
*May  6 14:04:40.859: 613B6204 t 18     0  - 0802 000 mFFFFFF 75B22C 361E08 C020
l92
   IP 10.100.106.255 < 10.100.106.56 f1-0-0 id 0 ttl64 sum 50AA prot 1 len 84
  ICMP ping code 0 chk F4D7, id 20765 seq 330
```

- Troubleshooting on WGB:
  - Use the **show running-config** command to check the status of **workgroup unified-vlan-client** and **workgroup-bridge unified-vlan-client broadcast-tagging**.
  - Use the **debug dot11 forwarding** command to check whether the IOS WGB has recovered the VLAN information from converted broadcast packet.

```
*Sep 15 02:54:24.775: Unified WGB convert specific mcast+vlan pak to
ffff.ffff.ffff:0080.483f.d5f6 on Virtual-Dot11Radio0 received,
link 7, dest_vlan_id 0x402F  <- 2F (Vlan id)
```

  - Use the **debug dot11 events** command to check whether the IOS WGB has received the original broadcast packet and dropped.

```
*Feb  4 17:41:19.081: Unified WGB drop original none-tagged bcast pak from source
00e0.4c36.1e08, ethertype: 0x0800, linktype: 7
```

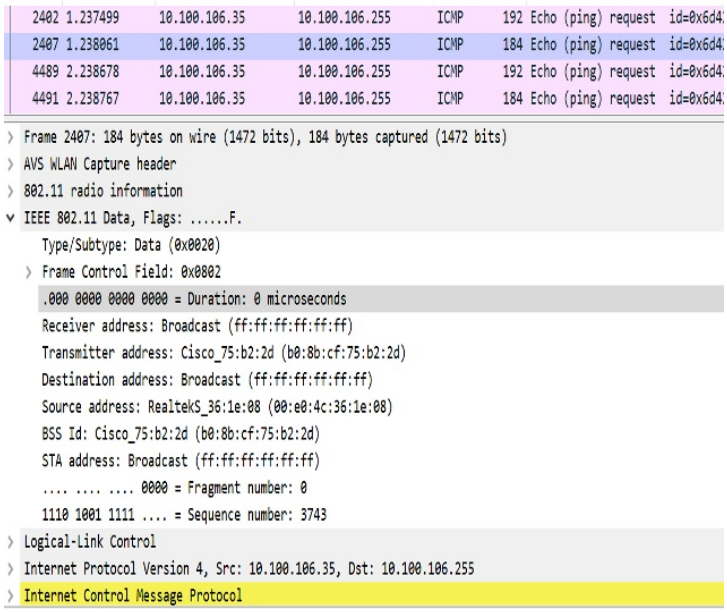
- Use the **debug dot11 dot11radio <0|1> trace print rcv** command to check converted packets and original packets.

```
Converted Packet:
*Nov 27 15:27:23.727: CB8823A0 r  m6-2   24/128/128/128 71- 8803 02C 48B89C AD9A70
 m01005E 06A0 392AC9 q4 l92
 4500 0054 0000 4000 4001 56C9 0A64 6719 0A64 67FF 0800 2E6A 1556 03BF
 B74B DE5D 0000 0000 5604 0600 0000 0000 1011 1213 1415 1617 1819 1A1B 1C1D
 1E1F 2021 2223 2425 2627 2829 2A2B 2C2D 2E2F 3031 3233 3435 3637 4860 6C3D

Original Packet:
*Nov 27 15:27:23.727: CB88246F r 18      21/128/128/128 74- 0802 000 mFFFFFF AD9A70
 392AC9 4610 l92
 4500 0054 0000 4000 4001 56C9 0A64 6719 0A64 67FF 0800 2E6A 1556 03BF
 B74B DE5D 0000 0000 5604 0600 0000 0000 1011 1213 1415 1617 1819 1A1B 1C1D
 1E1F 2021 2223 2425 2627 2829 2A2B 2C2D 2E2F 3031 3233 3435 3637 0000 0000
```

Use Sniffer to capture packet over the air or on the wired side when the detailed packet information is needed.

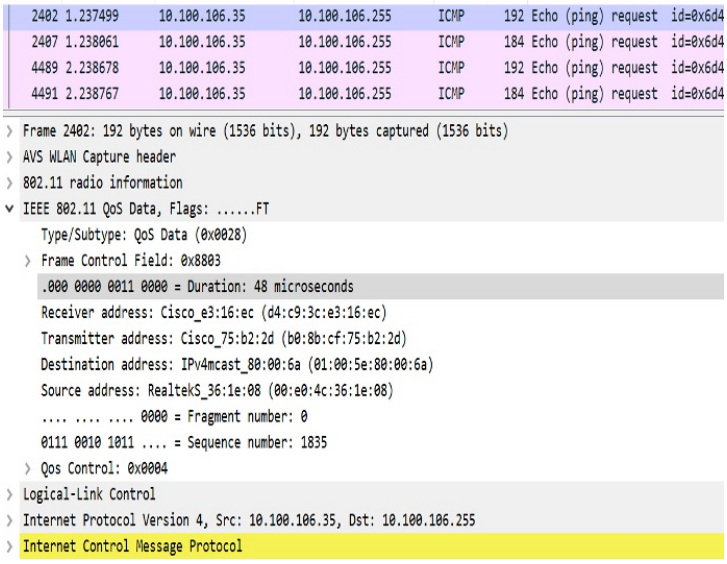
The following figure shows the original packet details.

Figure 73: Original Packet



The following figure shows the converted packet details.

Figure 74: Converted Packet



Parallel Redundancy Protocol Enhancement on AP and WGB

Cisco Wireless Release 8.4 provides the Parallel Redundancy Protocol (PRP) enhancement to improve wireless network availability for wired clients behind Workgroup Bridge (WGB), and improve the roaming performance by allowing wired clients to have dual wireless connections.

PRP allows a data communication network to prevent data transmission failures by providing two alternate paths for the traffic to reach its destination. Two Ethernet networks (LANs) with similar topologies are completely separated.

A device that requires protection for data across the network connects to the two independent networks (LAN-A and LAN-B) is called a Dual Attached Node implementing PRP (DANP). A DANP source sends two frames simultaneously on both LANs. A DANP destination receives both frames and discards the duplicating. If one LAN fails, a DANP destination can still receive a frame from the other LAN.

Non-redundant endpoints in the network that attach only to either LAN-A or LAN-B are known as Singly Attached Nodes (SANs). A Redundancy Box (RedBox) is used when a single interface node must be attached to both networks. Such a node can communicate with all other nodes. The switch implements RedBox functionality is a PRP switch.

To implement the PRP function for this release, you need to connect the AP and WGB to a PRP switch. The PRP switch is to offload PRP processing. AP or WGB is to keep dual wireless connections. You can have two WGBs interconnected through an external PRP switch and wirelessly connected to a single fixed AP or two fixed APs. Two WGBs can roaming between APs. Redundant packet transmissions can be supported over either single or both 2.4 GHz and 5 GHz. The infrastructure side also needs a PRP switch for AP side.

For the application where both WGBs may roam at the same time, the roaming coordination feature is introduced to avoid roaming gaps and guarantee staggered roaming. In this release, only dual radio links roaming coordination across two WGBs is supported for roaming coordination.

Supported platforms and AP mode:

- Controller and AP on the infrastructure side—FlexConnect AP mode (central authentication, local switching), the following IOS-based platforms are supported: IW3702, 2700, 3700, and 1570 series.

- WGB on the client side—Only supported for IW3700 Series
- Roaming coordination—Only supported for IW3700 Series

Sample Network Configuration

General guidelines for this configuration:

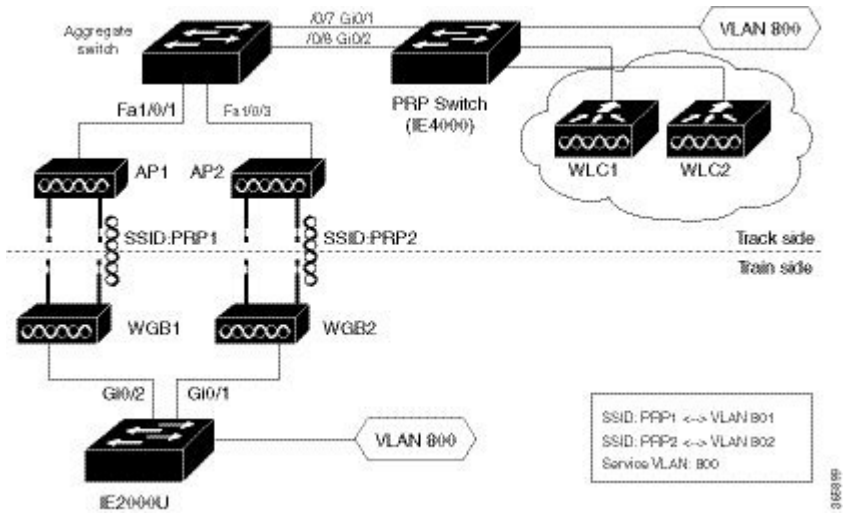
- Separation of expected redundancy in the network:
  - Traffic expecting redundancy mapped to two reserved SSID A and SSID B each with specified VLAN.
  - Each WGB is configured to connect either SSID A or SSID B.
  - Others traffic without expectation of redundancy is recommended to be mapped to other SSID.
- WGB supports unified VLAN function and it is recommended that wired clients not to use VLANs assigned to SSID A or SSID B.
- Wired clients connected to WGB are source and recipients of redundancy traffic.

The following figure shows a topology of concurrent wireless transmission via two WGBs paired with one PRP switch, commonly used in train transportation.

On the train side, the PRP switch (in this example, Cisco IE2000U) duplicates upstream packets and sends both packets simultaneously via two different ports, Gi0/1 and Gi0/2. The dual packets will pass from different WGBs or APs, to ensure that at least one packet reaches the destination. On the track side, one more PRP switch is added to each aggregating endpoint along the track. The PRP switch on the track side will remove the duplicating for upstream packets. The same redundancy for downstream packet is also available by the pair of PRP switches.

Note The throughput of this solution depends on the network elements depicted in the diagram. Each element along the wired and wireless transmission path should validate its throughput to avoid being the throughput bottleneck.

Figure 75: Concurrent Wireless Transmission via Two WGBs Paired With One PRP Switch



Controller Configuration (CLI Only)

To enable or disable PRP on a WLAN (new command):

```
(Cisco Controller)> config wlan wgb prp {enable|disable} <wlan id>
enable              Enable Parallel Redundancy Protocol (PRP) feature on a WLAN
disable             Disable Parallel Redundancy Protocol (PRP) feature on a WLAN
```

Note This feature is disabled by default.

This CLI will enable two WLANs to allow dual associations in flex-connect mode. It will also enable the AP to forward packets to or from WGB wired clients with double tags in flex-connect mode.

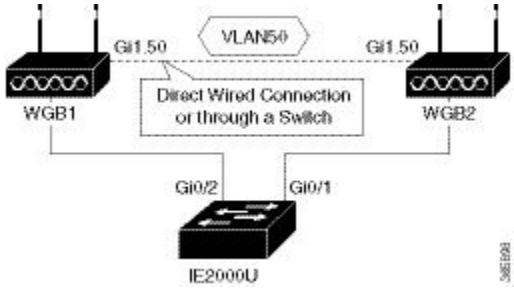
Note To enable unified VLANs in the WGB, the existing command config wgb vlan enable should also be executed. You should configure the inner VLAN (VLAN for wired client) on controller as well.

WGB Configuration for Roaming Coordination (CLI Only)

For Parallel Redundancy Protocol (PRP), wired client traffic will be duplicated to transmit in dual radio links in two WGBs. Dual radio links without any radio link coordination have the possibility to trigger roaming at the same time, so that the traffic will be broken in a short window time.

The following figure is a typical PRP scenario of train transportation. AP like IW3702 has two physical Ethernet ports. Gig0 will be exclusively used to bridge PRP traffic. Gig1 will be used for internal communication. Gig 1 will connect to a non-PRP port on the PRP switch or connect to a peer Gig1 port directly.

Figure 76: Peer Link Between Two WGBs



Configuration of Dual Radio Coordination on Two WGBs

Follow these steps to configure dual radio coordination on two WGBs:

1. Configure service VLAN.

   Use the following command to enable the service VLAN traffic that will be punted to local handling process for sub interface on Gig0 or Gig1.

   ```
   WGB(config)# workgroup-bridge service-vlan <vlan id>
   ```

2. Configure peer coordinator address.

   Use the following commands to set peer coordinator address and create the coordination communication process. For example, if you have configured the service VLAN to 50, you should configure the local/peer coordinator address under sub interface 50.

   ```
   WGB(config)# interface GigabitEthernet1.50
   WGB(config-subif)# encapsulation dot1q 50
   WGB(config-subif)# ip coordinator peer-addr <addr>
   ```

3. Configure dot11 radio coordinator on two WGBs.

   Use the following commands to create dot11 coordinator process, and enable dot11 roaming coordinator service on radio 0 or radio 1.

   ```
   WGB(config)# dot11 coordinator uplink single [radio 0|radio 1]
   ```

4. Configure dot11 coordination roaming waiting timer.

   Use the following command to set the dot11 coordination roaming waiting timer. The default is 100ms.

   ```
   WGB(config)# dot11 coordinator timeout roam-wait [value]
   ```

5. Configure Dot11 roaming coordination bypass.

   Use the following command to bypass roaming coordination decision on WGB. When configured, it is used to collect WGB's roaming conflict statistics, and will not affect the current roaming behavior.

   ```
   WGB(config)# dot11 coordinator bypass
   ```

6. Configure to avoid bridge loop.

   Wired network on WGB side can introduce a bridge loop if you connect the Gig1 port of WGBs directly or via a switch. The following sample configurations can avoid the bridge loop.

Note The coordination traffic is forwarded on service VLAN and will not be blocked.

- To avoid bridge loop when connecting the Gig1 port of WGBs directly, configure the following on both WGBs:

```
WGB(config)# access-list 700 deny 0000.0000.0000 ffff.ffff.ffff
WGB(config)# interface gigabitEthernet 1
WGB(config-if)# l2-filter bridge-group-acl
WGB(config-if)# bridge-group 1
WGB(config-if)# bridge-group 1 output-address-list 700
```

- To avoid traffic loop when connecting two WGBs via a switch, configure the following on the switch port:

```
interface GigabitEthernet0/3
switchport trunk allowed vlan 50
switchport mode trunk

interface GigabitEthernet0/4
switchport trunk allowed vlan 50
switchport mode trunk
```

Controller Configuration

Note For more information about Controller configuration for FlexConnect, see the FlexConnect Chapter in the *Cisco Wireless Controller Configuration Guide*.

Follow these steps to configure the wireless controller for FlexConnect:

1. Create two WLANs with the SSID PRP1 and PRP2.
2. Enable local switching for each WLAN.

Note For any wired client within the service VLAN, you need to create a corresponding dynamic interface with the same service VLAN on controller.

Configuration of AP

1. Configure AP to FlexConnect mode and join controller.
2. Enable VLAN support on each AP, and make sure PRP SSID is included.

Configuration of WGBs

- WGB1 Configuration

```
hostname WGB1
dot11 ssid PRP1
   vlan 801
   authentication open
interface Dot11Radio1
 no ip address
 ssid PRP1
 antenna gain 0
```

```
 stbc
 beamform ofdm
 station-role workgroup-bridge
!
interface Dot11Radio1.800
 encapsulation dot1Q 800
 bridge-group 2
 bridge-group 2 spanning-disabled
!
interface Dot11Radio1.801
 encapsulation dot1Q 801 native
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0.800
 encapsulation dot1Q 800
 bridge-group 2
!
interface GigabitEthernet0.801
 encapsulation dot1Q 801 native
 bridge-group 1
!
interface BVI1
 mac-address 4c00.821a.c0b0
 ip address dhcp
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 route ip
!
workgroup-bridge unified-vlan-client
```

- WGB2 Configuration

```
hostname WGB2
dot11 ssid PRP2
   vlan 802
   authentication open
interface Dot11Radio1
 no ip address
 !
 ssid PRP2
 !
 antenna gain 0
 stbc
 beamform ofdm
 station-role workgroup-bridge
!
interface Dot11Radio1.800
 encapsulation dot1Q 800
 bridge-group 2
 bridge-group 2 spanning-disabled
!
interface Dot11Radio1.802
 encapsulation dot1Q 802 native
 bridge-group 1
 bridge-group 1 spanning-disabled
!
```

```
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0.800
 encapsulation dot1Q 800
 bridge-group 2
!
interface GigabitEthernet0.802
 encapsulation dot1Q 802 native
 bridge-group 1
!
interface BVI1
 mac-address f872.eae4.a4d8
 ip address dhcp
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
bridge 1 route ip
workgroup-bridge unified-vlan-client
```

Aggregated Switch Configuration

```
Agg-SW# show run int fa 1/0/1
description ***AP1***
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 201
 switchport trunk allowed vlan 201,801,802
 switchport mode trunk
end


Agg-SW#show run int fa 1/0/3
Building configuration...


Current configuration : 196 bytes
!
interface FastEthernet1/0/3
 description ***AP2***
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 201
 switchport trunk allowed vlan 201,801,802
 switchport mode trunk
end

Agg-SW# show run int fa 1/0/7
Building configuration...


Current configuration : 178 bytes
!
interface FastEthernet1/0/7
 description ***PRP-Track-SW***
 switchport access vlan 801
 switchport trunk encapsulation dot1q
 switchport mode dot1q-tunnel
 no cdp enable
end
```

```
Agg-SW# show run int fa 1/0/8
Building configuration...


Current configuration : 178 bytes
!
interface FastEthernet1/0/8
 description ***PRP-Track-SW***
 switchport access vlan 802
 switchport trunk encapsulation dot1q
 switchport mode dot1q-tunnel
 no cdp enable
```

PRP Switch Configuration

```
interface PRP-channel1
 switchport mode trunk
interface GigabitEthernet0/1
 switchport mode trunk
 no ptp enable
 no cdp enable
 prp-channel-group 1
!
interface GigabitEthernet0/2
 switchport mode trunk
 no ptp enable
 no cdp enable
 prp-channel-group 1
```

Note For the PRP configurations on the Cisco IE switches, refer to Parallel Redundancy Protocol Software Configuration Guide for Industrial Ethernet 2000U Series Switches.

Verifying the PRP Configurations

Follow these steps to verify the PRP configurations:

Before you begin

- Create an SVI interface on the train side PRP switch with service vlan: 800.
- Configure the SVI interface on the track side PRP switch with service vlan: 800, and create the DHCP pool.

Procedure

Step 1 On the train side PRP switch, use the following command to check whether an IP address has been assigned to Vlan 800 from the DHCP pool on the track side.

Example:

```
PRP-Train-SW# show ip int bri
Interface              IP-Address      OK? Method Status                Protocol
```

```
Vlan1                  unassigned      YES NVRAM  administratively down down
Vlan800                10.10.80.67     YES DHCP   up                    up
```

Step 2 On the track side PRP switch, use the following command to display ingress packet statistics. In this example, LAN A and LAN B both have one packet.

Example:

```
PRP-Track-SW# show prp statistics ingressPacketStatistics
GE ports PRP INGRESS STATS:
   ingress pkt lan a: 1
   ingress pkt lan b: 1
   ingress crc lan a: 0
   ingress crc lan b: 0
   ingress danp pkt acpt: 0
   ingress danp pkt dscrd: 0
   ingress supfrm rcv a: 0
   ingress supfrm rcv b: 0
   ingress over pkt a: 0
   ingress over pkt b: 0
   ingress pri over pkt_a: 0
   ingress pri over pkt_b: 0
FE ports PRP INGRESS STATS:
   ingress pkt_lan a: 0
   ingress pkt_lan b: 0
   ingress crc lan a: 0
   ingress crc lan b: 0
   ingress danp pkt acpt: 0
   ingress danp pkt dscrd: 0
   ingress supfrm rcv a: 0
   ingress supfrm rcv b: 0
   ingress over pkt a: 0
   ingress over pkt b: 0
   ingress pri over pkt a: 0
   ingress pri over pkt b: 0
```

Step 3 On the train side PRP switch, ping the track side with the following command, to send 5 packets from the train to the track side:

Example:

```
PRP-Train-SW# ping 10.10.80.1
<= issue ping from train to track side, 5 pkts
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.80.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms
```

Step 4 On the track side PRP switch, use the following command to display the number of packets that LAN A and LAN B have received, and the number of duplicated packets that have been discarded. In this example, after receiving 5 packets, both LAN A and LAN B have 6 packets in total.

Example:

```
PRP-Track-SW# show prp statistics ingressPacketStatistics
GE ports PRP INGRESS STATS:
   ingress pkt lan a: 6   <= LAN A receives 5pkts
   ingress pkt lan b: 6   <= LAN B receives 5pkts
   ingress crc lan a: 0
   ingress crc lan b: 0
   ingress danp pkt acpt: 5
```

```
   ingress danp pkt dscrd: 5  <= discard 5 duplicate pkts
   ingress supfrm rcv a: 0
   ingress supfrm rcv b: 0
   ingress over pkt a: 0
   ingress over pkt b: 0
   ingress pri over pkt_a: 0
   ingress pri over pkt_b: 0
FE ports PRP INGRESS STATS:
   ingress pkt_lan a: 0
   ingress pkt_lan b: 0
   ingress crc lan a: 0
   ingress crc lan b: 0
   ingress danp pkt acpt: 0
   ingress danp pkt dscrd: 0
   ingress supfrm rcv a: 0
   ingress supfrm rcv b: 0
   ingress over pkt a: 0
   ingress over pkt b: 0
   ingress pri over pkt a: 0
   ingress pri over pkt b: 0
```

Dual Radio Parallel Redundancy Protocol Enhancement on WGB

Release 8.5 provides the Dual Radio Parallel Redundancy Protocol (PRP) enhancement as the second phase of the PRP feature.

This feature enables dual radio (2.4G and 5G) workgroup bridge mode on a WGB simultaneously. The WGB is wirelessly connected to the access points, with redundant packet transmissions over 2.4 GHz and 5 GHz subsystem.

Supported platforms and access point mode:

- Controller and AP on the infrastructure side—FlexConnect AP mode (central authentication, local switching), the following IOS-based platforms are supported: IW3702, 2700, 3700, and 1570 series.
- WGB on the client side—Only supported for IW3700 Series
- Roaming coordination—Only supported for IW3700 Series

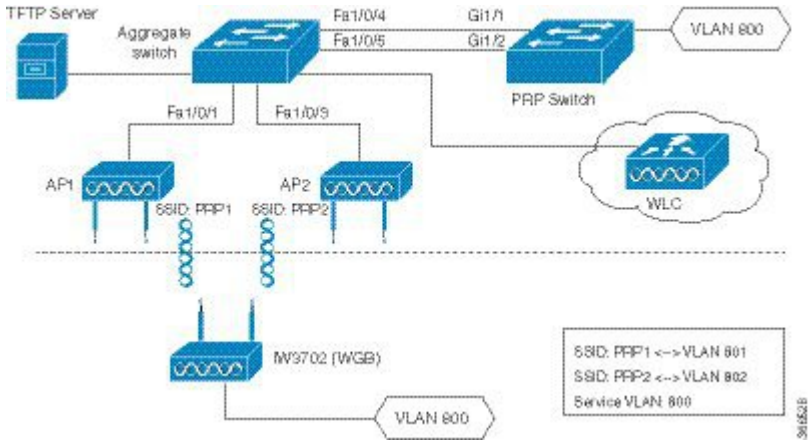
Sample Network Configuration

Figure 77: Concurrent Wireless Transmission Via One WGB With Dual Radio and Paired With One PRP Switch, on page 1102 shows a topology of concurrent wireless transmission via one WGB with dual radio and paired with one PRP switch.

The WGB (Cisco IW3702 Access Point) duplicates upstream packets and sends both packets simultaneously via 2.4 GHz and 5 GHz. The duplicated packets will pass to the access points, to ensure that at least one packet reaches the destination. On the infrastructure side, a PRP switch (for example, Cisco IE4000) is added to each aggregating endpoint. The PRP switch on the infrastructure side will remove the duplicating for upstream packets. The same redundancy for downstream packet is also implemented by the pair of PRP switch and WGB.

Note The throughput of this solution depends on the network elements depicted in the diagram. Each element along the wired and wireless transmission path should validate its throughput to avoid being the throughput bottleneck.

Figure 77: Concurrent Wireless Transmission Via One WGB With Dual Radio and Paired With One PRP Switch



Configuration of Roaming Coordination on a Single WGB

As the client traffic will be duplicated to transmit in dual radio links of one WGB, radio link coordination is necessary to avoid the possibility to trigger roaming at the same time, which will cause the traffic to be broken in a short window time.

- Configure dot11 dual radio coordinator on one WGB.

```
WGB(config)# dot11 coordinator uplink both
```

- Configure dot11 coordination roaming waiting timer. The value of the timer is from 50–150 ms. The default is 100 ms.

```
WGB(config)# dot11 coordinator timeout roam-wait [value]
```

Controller Configurations

This section contains the configurations on controller to enable PRP under WLAN and multiple VLAN support.

Note When you create WLAN, the BSSID of WLAN (mapping to 2.4G radio) and the BSSID of WLAN (mapping to 5G radio) must be different.

Note From release 8.5, you can configure the PRP settings via both CLI and GUI.

Enabling PRP Under WLAN (CLI)

- Use the following command to enable PRP under WLAN. The value of WLAN ID is between 1 and 512.

```
(WLC)> config wlan wgb prp enable <WLAN id>
```

- Use the following command to check the PRP status:

```
(WLC)> show wlan <WLAN id>
```

The output of this show command displays the PRP status as below:

```
Universal Ap Admin.............................. Disabled
Broadcast Tagging............................... Disabled
PRP............................................. Enabled
```

Enabling PRP Under WLAN (GUI)

To enable PRP under WLAN in GUI, choose **WLAN** -> **Advanced**. In the **WGB PRP** field, select the check box in front of **Enable**.

Enabling Multiple VLAN Support (CLI)

Use the following command to enable or disable the multiple VLAN support:

```
(WLC-PRP)> config wgb vlan {enable|disable}
enable Enable WGB Vlan Client Support
disable Disable WGB Vlan Client Support
```

Enabling Multiple VLAN Support (GUI)

To enable multiple VLAN support in GUI, choose **Controller** -> **General**. In the **WGB Vlan Client** field, choose **Enable** from the drop-down list.

WGB Configurations

This section contains the commands on WGB to configure the PRP settings.

Enabling PRP Mode on WGB

The following commands enable the PRP submode on WGB.

```
iw3702(config)# dot11 wgb prp
iw3702(config-prp)# no shutdown
```

Note PRP is disabled by default after the **dot11 wgb prp** command is executed. To enable the PRP feature, execute the **no shutdown** command.

Submode PRP Configuration Commands

- **bvi-vlanid**—Configure vlan id of the BVI interface.
- **dummy-ip**—Configure dummy ip for the radio interface.
- **shutdown**—Disable the PRP feature.
- **exit**—Exit from prp sub-mode.
- **no**—Negate a command or set its defaults.

Configuring Dummy IP Address for Radio Interface

Use the following command to configure the dummy ip address for the radio interface to associate to the access point. By default the IP address will be assigned as 1.1.X.Y and 1.1.X.(Y+1) to 2.4G and 5G, where X and Y are the last 2 bytes of the WGB's Ethernet MAC address.

```
iw3702(config-prp)# dummy-ip <IP_addr>
```

Configuring Vlan for BVI Under PRP Mode

Use the following command to configure Vlan for BVI under PRP mode. If not configured, the BVI interface cannot get IP address via DHCP under PRP mode.

```
iw3702(config-prp)# bvi-vlanid <Vlan_Id>
```

Note The vlan configured by the **bvi-vlanid** command is reserved for BVI only. Do not use it for any wired clients.

Configuration Example of WGB

This section provides an example of the WGB configuration. .

```
hostname Vehicle
!
dot11 wgb prp
  no shutdown
  bvi-vlanid 900
!
dot11 ssid PRP1
   vlan 801
   authentication open
   no ids mfp client
!
dot11 ssid PRP2
   vlan 802
   authentication open
   no ids mfp client
!
interface Dot11Radio0
 no ip address
 load-interval 30
 !
 ssid PRP1
```

```
 !
 antenna gain 0
 antenna a-antenna
 packet retries 32 drop-packet
 station-role workgroup-bridge
 rts retries 32
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.800
 encapsulation dot1Q 800
 bridge-group 50
 bridge-group 50 spanning-disabled
!
interface Dot11Radio0.801
 encapsulation dot1Q 801
 bridge-group 100
 bridge-group 100 spanning-disabled
!
interface Dot11Radio1
 no ip address
 load-interval 30
 !
 ssid PRP2
 !
 antenna gain 0
 antenna a-antenna
 peakdetect
 packet retries 32 drop-packet
 station-role workgroup-bridge
 rts retries 32
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1.800
 encapsulation dot1Q 800
 bridge-group 50
 bridge-group 50 spanning-disabled
!
interface Dot11Radio1.802
 encapsulation dot1Q 802
 bridge-group 200
 bridge-group 200 spanning-disabled
!
interface GigabitEthernet0
 no ip address
 load-interval 30
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface GigabitEthernet0.800
 encapsulation dot1Q 800
 bridge-group 50
 bridge-group 50 spanning-disabled
!
interface GigabitEthernet1
 no ip address
 shutdown
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
```

```
!
interface BVI1
 mac-address 0081.c408.c594
 ip address dhcp
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 route ip
!
workgroup-bridge unified-vlan-client
end
```

Aggregated Switch Configuration

```
interface FastEthernet1/0/1
 description ***AP1***
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 201
 switchport trunk allowed vlan 201,801,802
 switchport mode trunk
end

interface FastEthernet1/0/3
 description ***AP2***
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 201
 switchport trunk allowed vlan 201,801,802
 switchport mode trunk
end
interface FastEthernet1/0/4
 description ***PRP-Track-SW***
 switchport access vlan 801
 switchport trunk encapsulation dot1q
 switchport mode dot1q-tunnel
 no cdp enable
end

interface FastEthernet1/0/5
 description ***PRP-Track-SW***
 switchport access vlan 802
 switchport trunk encapsulation dot1q
 switchport mode dot1q-tunnel
 no cdp enable
```

PRP Switch Configuration

```
interface PRP-channel1
 switchport mode trunk
interface GigabitEthernet1/1
 switchport mode trunk
 no ptp enable
 no cdp enable
 prp-channel-group 1
interface GigabitEthernet1/2
 switchport mode trunk
 no ptp enable
 no cdp enable
```

```
prp-channel-group 1
```

Verifying the Configuration

- Verify the packet replication and discarding details.

```
Vehicle# show dot11 wgb prp
available uplink count: 0
Index: 0 Status: DOWN Name: Dot11Radio0 Virtual-Dot11Radio0 AP: cc46.d616.ad84
Index: 1 Status: DOWN Name: Dot11Radio1 Virtual-Dot11Radio1 AP: cc46.d616.ad8a
======== Statistic counters ==========================
cnt_total_sent_A_: 5481     <= RADIO 0 REPLICATION
cnt_total_sent_B_: 940       <= RADIO 1 REPLICATION
cnt_tx_difference: 4541
cnt_total_received_A_: 337   <= RADIO 0 DISCARDING
cnt_total_received_B_: 56     <= RADIO 1 DISCARDING
cnt_rx_difference: 281
cnt_total_errors_A_: 0
cnt_total_errors_B_: 0
cnt_total_discard: 1              <= DISCARDED PACKET COUNT
cnt_discard_table_used_items: 0
max_duplicate_delay_: 0
```

- Display the roaming coordination status.

```
WGB# show coordinator status
current coordinator role is: Master
```

- Display the roaming coordination statistics.

```
WGB# show dot11 coordinator statistics
Vehicle#show dot11 coordinator statistics
Dot11 Roaming Coordination CURRENT Statistics:
                        Total Roaming Count: 1034
-------------------------------------------------------------------------------
      Scheduled Roaming: 1034                  Forced Roaming: 0
--------------------------------------    --------------------------------------
RATESHIFT          RSSI                   MAXRETRY           BEACON_LOST
0                  1034                   0                  0
--------------------------------------
Backoff     Timeout       Immediate
3           1             1030
-------------------------
Master Conflict: 4          Slave Conflict: 0
-----------------------------------------------------
            Total Conflict Count: 4
Dot11 Roaming Coordination FULL Statistics:
                        Total Roaming Count: 1034
-------------------------------------------------------------------------------
      Scheduled Roaming: 1034                  Forced Roaming: 0
--------------------------------------    --------------------------------------
RATESHIFT          RSSI                   MAXRETRY           BEACON_LOST
0                  1034                   0                  0
--------------------------------------
Backoff     Timeout       Immediate
3           1             1030
-------------------------
```

```
Conflict: 4
Roaming Coordination Settings
-------------------------------------------------------------------------------
Current Roaming Wait Timeout: 100 ms
```

Debug Commands

- Clear roaming coordination statistics.

  clear dot11 coordinator {**all**|**current**} **statistics**

- Clear PRP statistics.

  clear dot11 wgb prp statistics

- Debug roaming coordination.
  - Use the following command to view the primary-subordinate role and communication related debug information:

    debug coordinator {**detail**|**error**|**event**|**packet**|**timers**

  - Use the following command to view dot11 radio roaming coordination related debug information:

    debug dot11 coordinator {**detail**|**error**|**event**|**timers**

- Disable PRP debug messages on CLI.

  no debug dot11 prp {**bvi**|**config**|**uplink**|**forward**|**event**|**trailer**|**bypass**

- Debug PRP configuration.

  debug dot11 prp {**bvi**|**config**|**uplink**|**forward**|**event**|**trailer**|**bypass**

DLEP Client Support on WGB

Radio Aware Routing (RAR) is a mechanism where radios can interact with routing protocols (such as OSPFv3 or EIGRP, but only EIGRP is supported in this feature) to signal the appearance, disappearance, and link conditions of one-hop routing neighbors. The Dynamic Link Exchange Protocol (DLEP) is a radio aware routing (RAR) protocol, which addresses the challenges faced when merging IP routing and radio frequency (RF) communications.

The DLEP client support feature allows the workgroup bridge (WGB) to report radio link metrics to a router, for example, the Cisco Embedded Services Router (ESR). The WGB acts as the DLEP client, and the ESR acts as the DLEP server. The uplink selection is based on radio link quality metrics. For example, when two WGBs are deployed in a truck, there are redundancy radio links. The link with better radio quality while the truck is moving can be selected before the radio link completely goes down.

There are two methods of DLEP peer discovery, auto discovery and manual configuration. In this release, only the manual configuration method is supported.

Note This feature applies to the IW3700 Series. Only DLEP version 7 is supported.

Configuring the Physical Interface

The DLEP session is established between ESR and WGB through wired Ethernet interface. Static IP address needs to be configured under BVI interface. Subinterface of Gigabit Ethernet is also supported. But the subinterface should be configured with the same VLAN as the wireless interface. Here is an example:

```
interface GigabitEthernet0.811
encapsulation dot1Q 811
ip address 8.1.1.50 255.255.255.0
ip dlep local-port 38682 server-addr 8.1.1.211 server-port 55556
```

Configuring DLEP Local TCP Port and Server Address

Use the following command to enable the WGB to work as a DLEP client and configure the DLEP local port and server address.

```
wgb(config-if)# ip dlep local-port x server-addr x.x.x.x server-port x
```

Once configured, the WGB will listen on the configured local port for incoming DLEP connections.

Configuring Optional DLEP Timers

Configuring Heartbeat Timer

Use the following command to set the interval for the DLEP client to wait before declaring a DLEP server peer failed.

```
wgb(config-if)# ip dlep set heartbeat-timer x
```

The value range of the heartbeat timer is from 1 to 60 seconds. The default value is 5 seconds. The new heartheat timer value will take effect in the next new dlep session.

Configuring Neighbor Update Interval

Use the following command to set the interval for DLEP client to send neighbor update event in millisecond.

```
wgb(config-if)# ip dlep set neighbor-update-interval x
```

The value range of the neighbor update interval is from 100 to 5000 milliseconds. If not specified, the default value is 4000 milliseconds. The new neighbor update timer will take effect in the next new DLEP session. The WGB will send neighbor update message which contains radio metrics to the DLEP server every x milliseconds. Neighbor update interval will impact ESR response speed when link state changes. It is

recommended to set a shorter neighbor-update-interval for high speed roaming. For example, you may set neighbor-update-interval to 500ms when WGB's moving speed is up to 80km/h.

Configuring DLEP Neighbors

The WGB uses the radio interface to detect neighbor and neighbor's metrics. Configure DLEP neighbor information under the radio interface.

Configuring Neighbor MAC Address

Use the following command to configure routing neighbor MAC address:

```
wgb(config-if)# dlep neighbor <mac address>
```

(Optional) Configuring RSSI Threshold and CDR Threshold

Use the following command to configure RSSI and CDR threshold:

```
wgb(config-if)# dlep neighbor <mac address> rssi-threshold x cdr-threshold x
```

Use the following command to configure RSSI threshold:

```
wgb(config-if)# dlep neighbor <mac address> rssi-threshold x
```

The value range of RSSI threshold is 1–100 dbm. The default value is 80 dbm. Once the RSSI value is above the configured RSSI threshold, the WGB will send neighbor update message including all the radio metrics to the DLEP server immediately.

Use the following command to configure CDR threshold:

```
wgb(config-if)# dlep neighbor <mac address> cdr-threshold x
```

The value range of CDR threshold is 7-6000 mbps. If not configured, no event will be triggered no matter what the current data rate is. Once configured, the neighbor update will be sent to the DLEP server when the current data rate is lower than the configured CDR threshold.

Note For roaming scenarios, the neighbor update will be sent out immediately after the roaming is completed.

Note There are two ways to trigger the metric update. One is the event trigger which is controlled by rssi-threshold or cdr-threshold. The other is the timer trigger which is controlled by the neighbor update interval.

Verifying DLEP Configuration

Displaying DLEP Configuration

The following command shows information about DLEP configurations, such as the server's IP address, port, heartbeat threshold, and peer-terminate-ack-timeout value.

```
WGB# show dlep config
 local tcp port=38682
 local ipv4=8.1.1.50
 router tcp port=55556
 router ipv4=8.1.1.211
 Type Description: no type description
 local ID=0
 peer offer tiemout=5 seconds
 peer heartbeat interval=5 seconds
 peer heartbeat missed threshold=3
 peer termination ack timeout=1000 milliseconds
 peer termination missed ack threshold=3
 neighbor up ack timeout=1000 milliseconds
 neighbor up missed ack threshold=3
 neighbor update interval timeout=4000 milliseconds
 neighbor activity timer=10 seconds
 neighbor down ack timeout=1000 milliseconds
 neighbor down missed ack threshold=3
```

Displaying DLEP Peer Information

The following command provides DLEP peer (DLEP server for WGB) information.

```
WGB# show dlep peers
DLEP Local Client 3
 Client ID=0
 Router ID=0
 Peer Description=
 Peer TCP port=55556
 Peer IPv4=8.1.1.211
 router offer timeout count=0
 peer heartbeat missed count=1
 peer term ack missed count=0
 peer term ack missed threshold=3
 neighbor up ack timeout=1000 milliseconds
 neighbor up missed ack threshold=3
 neighbor update interval timeout=4000 milliseconds
 neighbor activity timer=10 seconds
 neighbor down ack timeout=1000 milliseconds
 neighbor down missed ack threshold=3
 Metrics:
 RLQ TX=100 <0-100> RLQ RX=100 <0-100>
 Resources TX=100 <0-100> Resources RX=100 <0-100>
 Latency=0 milliseconds
 CDR TX=100000000 bps  CDR RX=100000000 bps
 MDR TX=100000000 bps  MDR RX=100000000 bps
```

Displaying DLEP Neighbors

The following command shows information of DLEP neighbors.

```
WGB# show dlep neighbors
DLEP Local Client 3
 Client ID=0
 Router ID=0
 Peer Description=
 Peer TCP port=55556
 Peer IPv4=8.1.1.211 Neighbor Local ID=5004
 Neighbor MAC= 00:50:56:8F:5F:FE
 activity timer=5 milliseconds
 Metrics:
 RLQ TX=100 <0-100> RLQ RX=100 <0-100>
 Resources TX=100 <0-100> Resources RX=100 <0-100>
 Latency=0 milliseconds
 CDR TX=144000000 bps  CDR RX=144000000 bps
 MDR TX=217000000 bps  MDR RX=217000000 bps
 Credits:
 MRW CREDITS=0 credits
 RRW CREDITS=0 credits
```

Displaying DLEP Client Counters

The following command shows packets counters of DLEP client.

```
WGB# show dlep counters
DLEP Client Counters
Last Clear Time = 13:13:51 UTC Mon Sep 15 2014
DLEP Server IP=8.1.1.111:55556
Peer Counters:
 RX Peer Discovery       0      TX Peer Offer             0
 RX Peer Offer           0      TX Peer Discovery         0
 RX Peer Init            0      TX Peer Init Ack          0
 RX Peer Init Ack        0      TX Peer Init              0
 RX Heartbeat            7449   TX Heartbeat              7278
 RX Peer Terminate       0      TX Peer Terminate Ack     0
 RX Peer Terminate Ack   0      TX Peer Terminate         0
 RX Peer Update Request  0      TX Peer Update Response   0
Neighbor Counters:
 RX Neighbor Up                0      TX Neighbor Up Ack                0
 RX Neighbor Up Ack            0      TX Neighbor Up                    0
 RX Neighbor Metric            0      TX Neighbor Metric                0
 RX Neighbor Down              0      TX Neighbor Down Ack              0
 RX Neighbor Down Ack          0      TX Neighbor Down                  0
 RX Neighbor Link Char Request 0      TX Neighbor Link Char Response    0
 RX Neighbor Link Char Response 0     TX Neighbor Link Char Request     0

Exception Counters:
 RX Invalid Message    0      RX Unknown Message        0
 Neighbor Not Found    0
Timer Counters:
 Peer Heartbeat Timer              7278
 Peer Terminate Ack Timer          0
 Neighbor Init Ack Timer           0
 Neighbor Update Ack Timer         0
 Neighbor Metrics Interval Timer   0
 Neighbor Terminate Ack Timer      0
```

Debug Commands

Note Contact your Cisco Support engineer for any troubleshooting support you may need.

The following command triggers the WGB to send peer terminate to the DLEP server to remove the specified peer:

```
wgb# clear dlep peer
```

The following command clears the DLEP client counters:

```
wgb# clear dlep counters
```

The following command displays the DLEP client process event information:

```
WGB# debug dlep client [detail]
```

The following command displays the DLEP neighbor transaction information:

```
WGB# debug dlep neighbor {<mac-address>|all|detail|error|metric|state}
  H.H.H    DLEP client neighbor MAC addr
  all      debugging information for all DLEP neighbors
  detail   DLEP neighbor detail information
  error    DLEP neighbor error information
  metrics  DLEP neighbor metrics information
  state    DLEP neighbor state machine information
```

The following commands display the DLEP peer transaction information:

```
WGB# debug dlep peer {detail|error|state|packet {detail|dump|incoming|outgoing}}
  detail  DLEP peer detail information
  error   DLEP peer error information
  packet  display DLEP peer packet information
  state   DLEP peer state machine information

WGB# debug dlep peer packet {detail|dump|incoming|outgoing}
  detail    display DLEP client packet details
  dump      display DLEP peer packet as a hex dump
  incoming  filter DLEP client incoming packets
  outgoing  filter DLEP client outgoing packets
```

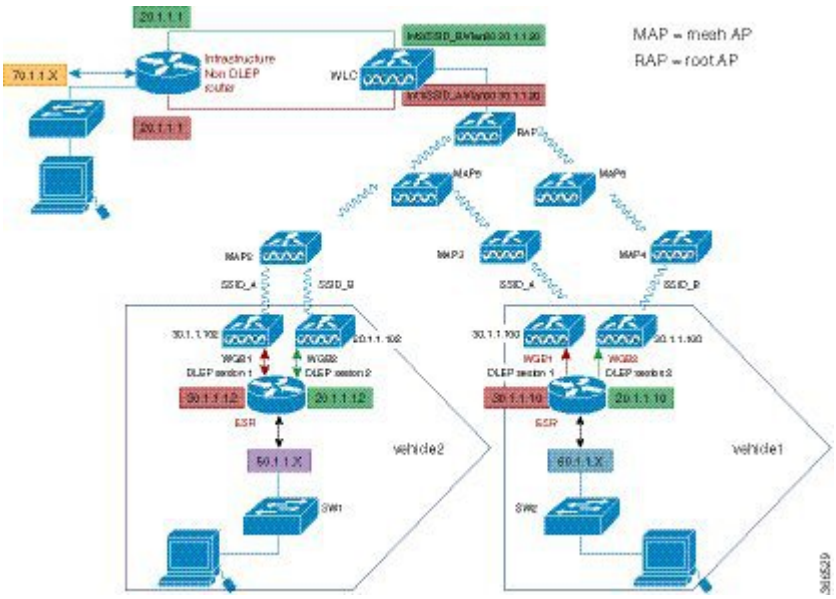
The following commands display the DLEP timer detail information:

```
WGB# debug dlep timer [detail
```

Configuration Example

This section contains a DLEP configuration example, including the configurations of WGB, controller, and ESR.

In this example, the DLEP server is implemented by ESR. Two WGBs act as DLEP clients. deployed in the same vehicle to provide redundant radio links. Each mesh AP (MAP) is configured with two SSIDs. Each WGB associates to a different SSID and establish a DLEP session with the ESR respectively. WGBs report radio link metrics to ESR through the DLEP sessions. Based on these radio link metrics, routing protocol of the ESR makes routing selection. The L2TPv3 tunnel is required to bridge the network behind ESR to be layer 2 adjacency across the IP networks.



Controller Configuration

Follow these steps to configure controller:

Procedure

Step 1 Configure AP to FlexConnect mode.

Step 2 Create two WLAN SSID for the redundant radio links.

Step 3 Configure CCKM.

WGB Configuration

For WGB fast secure roaming use case, it is recommended to configure CCKM and you need to configure CCKM on controller first. You are suggested to enable roaming coordinator when using DLEP.

Follow these steps to configure WGB:

Procedure

Step 1 Configure DLEP neighbor under radio interface.

Example:

```
dlep neighbor 000c.29da.a804 rssi-threshold 72 cdr-threshold 120
```

where the MAC address is the interface MAC of ISR-G2.

Step 2 Configure DLEP local port and server address under BVI1 or GigabitEthernet0 subinterface.

Example:

```
ip dlep local-port 38682 server-addr 100.100.1.2 server-port 55556
```

where the server address is the interface IP address of the ESR.

Step 3 Configure CCKM.

Example:

```
dot11 ssid k901
   vlan 901
   authentication open eap EAP-FAST
   authentication network-eap EAP-FAST
   authentication key-management wpa version 2 cckm
   dot1x credentials FAST
   dot1x eap profile FAST
eap profile FAST
 method fast
dot1x credentials FAST
 username cisco
 password 0 cisco
interface Dot11Radio1
 no ip address
 encryption mode ciphers aes-ccm
 encryption vlan 901 mode ciphers aes-ccm
```

Step 4 Enable coordinator.

Example:

```
dot11 coordinator uplink single Dot11Radio1
interface GigabitEthernet1.10
 encapsulation dot1Q 10
 ip address 192.168.0.1 255.255.255.0
 ip coordinator peer-addr 192.168.0.2
!
workgroup-bridge service-vlan 10
```

What to do next

The following examples show the configurations of WGB1 and WGB2:

WGB1 Configuration Example

```
dot11 ssid k901
   vlan 901
```

```
   authentication open eap EAP-FAST
   authentication network-eap EAP-FAST
   authentication key-management wpa version 2 cckm
   dot1x credentials FAST
   dot1x eap profile FAST
dot11 coordinator uplink single Dot11Radio1
eap profile FAST
 method fast
dot1x credentials FAST
 username cisco
 password 0 cisco
interface Dot11Radio0
 no ip address
 shutdown
 !
 encryption vlan 901 mode ciphers aes-ccm
 !
 ssid k901
 !
packet retries 32 drop-packet
 station-role root
 rts retries 32
 infrastructure-client
!
interface Dot11Radio1
 no ip address
 !
 encryption mode ciphers aes-ccm
 !
 encryption vlan 901 mode ciphers aes-ccm
 !
 ssid k901
 !
peakdetect
station-role workgroup-bridge
 dlep neighbor 286f.7f75.0810 rssi-threshold 72 cdr-threshold 120
 mobile station scan 5220 5280
 mobile station period 1 threshold 76
 infrastructure-client
!
interface Dot11Radio1.901
 encapsulation dot1Q 901 native
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0.901
 encapsulation dot1Q 901 native
 ip address 100.100.1.12 255.255.255.0
 ip dlep set neighbor-update-interval 500
 ip dlep local-port 38682 server-addr 100.100.1.2 server-port 55556
 bridge-group 1
 no bridge-group 1 spanning-disabled
!
interface GigabitEthernet1
 no ip address
 duplex auto
 speed auto
 l2-filter bridge-group-acl
 bridge-group 1
```

```
no bridge-group 1 spanning-disabled
!
interface GigabitEthernet1.10
 encapsulation dot1Q 10
 ip address 192.168.0.1 255.255.255.0
 ip coordinator peer-addr 192.168.0.2
!
interface BVI1
 mac-address 0081.c475.b73c
 ip address 100.100.1.11 255.255.255.0
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
workgroup-bridge unified-vlan-client
workgroup-bridge service-vlan 10
workgroup-bridge timeouts auth-response 300
workgroup-bridge timeouts assoc-response 300
```

WGB2 Configuration Example

```
dot11 ssid k902
   vlan 902
   authentication open eap EAP-Methods
   authentication network-eap EAP-Methods
   authentication key-management wpa version 2 cckm
   dot1x credentials FAST
   dot1x eap profile FAST
!
dot11 coordinator uplink single Dot11Radio1
!
power out-never
eap profile FAST
 method fast
!
no ipv6 cef
!
dot1x credentials FAST
 username cisco
 password 0 cisco
!
interface Dot11Radio0
 no ip address
 shutdown
 !
 encryption vlan 902 mode ciphers aes-ccm
 !
 ssid k902
 !
station-role root
 rts retries 32
 infrastructure-client
!
interface Dot11Radio1
 no ip address
 !
 encryption vlan 902 mode ciphers aes-ccm
 !
 ssid k902
 !
 antenna gain 0
 antenna a-antenna
 peakdetect
```

```
 ampdu transmit priority 6
 amsdu transmit priority 6
 packet retries 32 drop-packet
 station-role workgroup-bridge
 dlep neighbor 286f.7f75.0810 rssi-threshold 72 cdr-threshold 120
 mobile station scan 5220 5280
 mobile station period 1 threshold 76
 infrastructure-client
!
interface Dot11Radio1.902
 encapsulation dot1Q 902 native
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0.902
 encapsulation dot1Q 902 native
 ip address 100.100.2.12 255.255.255.0
 ip dlep set neighbor-update-interval 500
 ip dlep local-port 38682 server-addr 100.100.2.2 server-port 55555
 bridge-group 1
 no bridge-group 1 spanning-disabled
!
interface GigabitEthernet1
 no ip address
 duplex auto
 speed auto
 l2-filter bridge-group-acl
 bridge-group 1
no bridge-group 1 spanning-disabled
!
interface GigabitEthernet1.10
 encapsulation dot1Q 10
 ip address 192.168.0.2 255.255.255.0
 ip coordinator peer-addr 192.168.0.1
!
interface BVI1
 mac-address 002a.1001.3eb0
 ip address 100.100.2.11 255.255.255.0
 ipv6 address dhcp
 ipv6 address autoconfig
!
workgroup-bridge unified-vlan-client
workgroup-bridge service-vlan 10
workgroup-bridge timeouts auth-response 300
workgroup-bridge timeouts assoc-response 300
```

ESR Configuration

Follow these steps to configure ESR.

Note For more information of configuring DLEP on ESR, See the following chapter of the *Software Configuration Guide for the Cisco 5900 Embedded Services Routers* : https://www.cisco.com/c/en/us/td/docs/solutions/GGSG-Engineering/15-4-3M/config-guide/Configuration-Guide/DLEP.html

Procedure

Step 1 Configure DLEP under Ethernet interfaces.

Example:

```
interface Ethernet0/1
 description DLEP radio connection
 ip address 100.100.1.2 255.255.255.0
 ip dlep vtemplate 1 version v1.7 client ip 100.100.1.12 port 38682
 duplex auto
 speed auto
interface Ethernet0/2
 description DLEP radio connection
 ip address 100.100.2.2 255.255.255.0
 ip dlep vtemplate 2 version v1.7 client ip 100.100.2.12 port 38682
 duplex auto
 speed auto
```

Step 2 Configure the virtual template.

Example:

```
interface Virtual-Template 1
 ip unnumbered Ethernet0/1
 ipv6 enable
interface Virtual-Template 2
 ip unnumbered Ethernet0/2
```

Step 3 Configure the VMI interface.

Example:

```
interface vmi1
 ip unnumbered Ethernet0/1
 physical-interface Ethernet0/1
interface vmi2
 ip unnumbered Ethernet0/2
 physical-interface Ethernet0/2
```

Step 4 Configure EIGRP with static neighbor.

The link metrics of VMI interface map to the basic EIGRP interface parameters according to the following mapping table:

VMI	EIGRP
Current data rate	Bandwidth
Relative link quality resources	Reliability
Latency	Delay
Load	Load

For more information about this mapping, see Enhanced Interior Gateway Routing Protocol (EIGRP) Wide Metrics White Paper.

For the implementation of this feature, relative link quality (RLQ) is the main factor to be considered for link quality. So the default EIGRP metric weights should be updated using the **metric weights** command.

Note
When DLEP works between WGB and ESR, WGB reports CDR and RLQ. Default K values of EIGRP are: K1=K3=1, K2=K4=K5=0. Thus, by default, only CDR will impact ESR route selection. When calculating CDR, WGB will take negotiated data rate, RF status, retry counters, roaming event, and so on into consideration. For WGB low speed moving scenarios, CDR can guarantee the better link to be selected. But for WGB high speed moving scenario, or other cases where RF signal changes rapidly, the delay introduced by CDR calculation may cause large data interruption. To make ESR respond more quickly to link state change, you may change the K values of EIGRP case by case, for example, setting K5=<1-255>, to make RLQ impact more on route selection.

Example:

```
router eigrp 100
 metric weights 0 1 0 1 0 1
 traffic-share min across-interfaces
 network 2.2.2.2 0.0.0.0
 network 100.100.1.0 0.0.0.255
 network 100.100.2.0 0.0.0.255
 neighbor 100.100.1.1 vmi1
 neighbor 100.100.2.1 vmi2
 eigrp router-id 2.2.2.2
```

Step 5 (Optional) Configure L2TPv3 tunnel, which is required by this example, but optional for basic DLEP configurations.

Example:

```
pseudowire-class R1R2
 encapsulation l2tpv3
 protocol l2tpv3 l2tp-defaults
 ip local interface Loopback1
```

What to do next

ESR Configuration Example

```
hostname ESR-Vehicle
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$DecM$eQ2Pbh2rdVafrS9UngqnA0
enable password cisco123!
!
no aaa new-model
clock timezone CST 8 0
mmi polling-interval 60
no mmi auto-configure
```

```
no mmi pvc
mmi snmp-timeout 180
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email
 address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http
  no destination transport-method email
!
ip multicast-routing
!
no ip domain lookup
ip host ESR-Infra 209.165.200.10
ip cef
no ipv6 cef
l2tp-class l2tp-defaults
 retransmit initial retries 30
 cookie size 8
!
multilink bundle-name authenticated
!
no virtual-template subinterface
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
license udi pid CISCO5921-K9 sn 9W30339RC8G
license platform throughput level c5921-x86-level5
!
redundancy
!
```

```
pseudowire-class R1R2
 encapsulation l2tpv3
 protocol l2tpv3 l2tp-defaults
 ip local interface Loopback1
!
interface Loopback1
 ip address 2.2.2.2 255.255.255.255
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
 bfd interval 50 min_rx 50 multiplier 3
!
interface Ethernet0/1
 description DLEP radio connection
 ip address 100.100.1.2 255.255.255.0
 ip dlep vtemplate 1 version v1.7 client ip 100.100.1.12 port 38682
 duplex auto
 speed auto
!
interface Ethernet0/2
 description DLEP radio connection
 ip address 100.100.2.2 255.255.255.0
 ip dlep vtemplate 2 version v1.7 client ip 100.100.2.12 port 38682
 duplex auto
 speed auto
!
interface Ethernet0/3
 ip address 100.100.3.2 255.255.255.0
 shutdown
 duplex auto
 speed auto
 no keepalive
!
interface Ethernet1/0
 no ip address
 duplex auto
 speed auto
 xconnect 209.165.200.10 123 encapsulation l2tpv3 pw-class R1R2
!
interface Ethernet1/1
 ip address 10.124.22.237 255.255.255.0
!
interface Ethernet1/2
 no ip address
 shutdown
!
interface Ethernet1/3
 no ip address
 shutdown
!
interface Virtual-Template1
 ip unnumbered Ethernet0/1
 ipv6 enable
!
interface Virtual-Template2
 ip unnumbered Ethernet0/2
!
interface vmi1
 ip unnumbered Ethernet0/1
 ip dampening-change eigrp 100 5
 ipv6 address FE80::901 link-local
```

```
 physical-interface Ethernet0/1
!
interface vmi2
 ip unnumbered Ethernet0/2
 ip dampening-change eigrp 100 5
 ip hello-interval eigrp 100 60
 ip hold-time eigrp 100 180
 physical-interface Ethernet0/2
!
router eigrp 100
 metric weights 0 1 0 1 0 1
 traffic-share min across-interfaces
 network 2.2.2.2 0.0.0.0
 network 100.100.1.0 0.0.0.255
 network 100.100.2.0 0.0.0.255
 neighbor 100.100.1.1 vmi1
 neighbor 100.100.2.1 vmi2
 eigrp router-id 2.2.2.2
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 10.0.0.0 255.0.0.0 Ethernet1/1
!
dialer-list 1 protocol ip permit
ipv6 ioam timestamp
!
access-list 1 permit 2.2.2.2
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
 no domain-lookup
line aux 0
line vty 0 4
 password cisco
 login
 transport input all
!
ntp mindistance 0
!
end
```

ISR-G2 Configuration

The ISR-G2 in this example can be replaced by an ESR with no need to configure DLEP.

Use these commands to configure L2TPv3 on ISR-G2. It is required by this example, but optional for basic DLEP configuration.

```
pseudowire-class R2R1
 encapsulation l2tpv3
 protocol l2tpv3 l2tp-defaults
 ip local interface Loopback1
```

ISR-G2 Configuration Example

```
hostname ISR-G2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
!
ip dhcp excluded-address 100.100.0.1 100.100.0.10
ip dhcp excluded-address 100.100.1.1 100.100.1.10
ip dhcp excluded-address 100.100.2.1 100.100.2.10
!
ip dhcp pool vlan900
 network 100.100.0.0 255.255.255.0
 domain-name cisco.com
 default-router 100.100.0.1
 lease 0 0 30
!
ip dhcp pool vlan901
 network 100.100.1.0 255.255.255.0
 domain-name cisco.com
 default-router 100.100.1.1
 lease 0 0 30
!
ip dhcp pool vlan902
 network 100.100.2.0 255.255.255.0
 domain-name cisco.com
 default-router 100.100.2.1
 lease 0 0 30
!
no ip domain lookup
ip cef
l2tp-class l2tp-defaults
 retransmit initial retries 30
 cookie size 8
!
ipv6 source-route
ipv6 dhcp pool vlan900-v6
 address prefix 2016:1:0:900::/112 lifetime 120 90
 dns-server 2016:1:0:900::3
 domain-name cisco.com
!
ipv6 multicast-routing
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
!
voice-card 0
!
license udi pid CISCO2911/K9 sn FGL205010MR
license accept end user agreement
license boot suite FoundationSuiteK9
license boot suite AdvUCSuiteK9
!
username cisco privilege 15 secret 5 $1$MxQb$wNWP92nY5L3eFxnGHKs.60
!
redundancy
!
```

```
pseudowire-class R2R1
 encapsulation l2tpv3
 protocol l2tpv3 l2tp-defaults
 ip local interface Loopback1
!
interface Loopback1
 ip address 10.10.10.1 255.255.255.255
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.900
 encapsulation dot1Q 900
 ip address 100.100.0.1 255.255.255.0
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 1
 ipv6 address 2016:1:0:900::1/64
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 nd ra interval 30
 ipv6 dhcp server vlan900-v6
!
interface GigabitEthernet0/0.901
 encapsulation dot1Q 901
 ip address 100.100.1.1 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/0.902
 encapsulation dot1Q 902
 ip address 100.100.2.1 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 xconnect 2.2.2.2 123 encapsulation l2tpv3 pw-class R2R1
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
router eigrp 100
 metric weights 0 1 0 1 0 1
 traffic-share min across-interfaces
 network 10.10.10.1 0.0.0.0
 network 100.100.0.0 0.0.0.255
 network 100.100.1.0 0.0.0.255
 network 100.100.2.0 0.0.0.255
 neighbor 100.100.2.2 GigabitEthernet0/0.902
 neighbor 100.100.1.2 GigabitEthernet0/0.901
 eigrp router-id 10.10.10.1
!
ip forward-protocol nd
!
no ip http server
```

```
no ip http secure-server
!
access-list 1 permit 10.10.10.1
!
control-plane
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```

Viewing the Status of Workgroup Bridges (GUI)

Procedure

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)

Procedure

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**

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.

Cisco Wave 2 Access Points as Workgroup Bridges

Starting Release 8.8.120.0, Cisco Wave 2 Access Points can operate as Workgroup Bridges.

Universal WGB (UWGB) is a complementary mode of WGB feature that associates with any Root AP (Cisco or Non-Cisco RAP). When the WGB device is in UWGB mode this limits the association to one wired client.

Note Before changing the WGB to UWGB mode, ensure that the WGB has had a graceful exit from the Cisco controller.

This section contains the following subsections:

Guidelines and Restrictions on Cisco Wave 2 Access Points as Workgroup Bridges

- A maximum of 20 clients are supported behind a Cisco WGB device.
- The Workgroup Bridges mode is supported only on Cisco 2800, 3800, 4800, and 1560 Series Access Points.
- This feature functions only when you connect a power supply unit capable of providing minimum of 26W power to the Cisco Wave 2 AP.
- We recommend you to shut down the primary Ethernet port of the WGB before executing **clear wgb client all** command. If there is any traffic flowing in the WGB, then the above command might not clear all the WGB client entries.

Caution Before shutting down the primary Ethernet port of the WGB please make sure that the WGB is powered by an external power source and NOT Powered-Over-Ethernet.

- Access points in WGB mode do not support LAG.
- Access points in WGB mode do not support the Aux port.
- Before you change from WGB mode to UWGB mode, we recommend that you remove the client entry from the controller. This prevents association of the actual client instead of the client identity and getting added to the exclusion list.
- When associated with an SSID, the WGB MAC address is unique for each radio slot (0/1).
- IPv6 protocol is not supported.
- VLANs are not supported. For more information, see CSCvk32521.

Configuring Cisco Wave 2 Access Points Image (CLI)

Procedure

Step 1 Configure the boot path by entering this command:

(cisco-wave2-ap)#configure boot path {**1** | **2**}

Default value is *2*.

Step 2 Load the AP image from archives by entering one of the following commands:

To load the AP image, choose from one of the following CLIs:

- Reload after loading the image—**(cisco-wave2-ap)#archive download-sw /reload** *tftp://tftp-server-ip-address/tar-filename-along-with-path*
- No reload after loading the image—**(cisco-wave2-ap)#archive download-sw /no-reload** *tftp://tftp-server-ip-address/tar-filename-along-with-path*

Step 3 Configure the NTP server on the AP by entering this command:

(cisco-wave2-ap)#configure ntp server *ntp-server-ipv4-addr*

Step 4 View the current booth path by entering this command:

(cisco-wave2-ap)#show boot

Step 5 View the current NTP server settings by entering this command:

(cisco-wave2-ap)#show ntp

Configuring Cisco Wave 2 Access Points as Workgroup Bridge (CLI)

Before you begin

To prevent the connected wired client and switch behind the WGB using the same IP address which is observed in controller, we recommend you to disable the IGMP snooping using the command **no ip igmp snooping** on the WGB switch.

Procedure

Step 1 Enter the privileged mode in the AP by entering this command:

(cisco-wave2-ap)#enable

Step 2 Switch the AP to Workgroup Bridge mode by entering this command:

(cisco-wave2-ap)#ap-type workgroup-bridge

Step 3 Configure the IP address of the AP by entering this command:

- IPv4:
  - DHCP IP address—**(cisco-wave2-ap)#configure ap address ipv4 dhcp**
  - Static IP address—**(cisco-wave2-ap)#configure ap address ipv4 static** *ip-addr netmask gateway-ipaddr*

Step 4 Add a username for the AP management by entering this command:

(cisco-wave2-ap)#configure ap management add username *username* **password** *pwd* **secret** *secret-hint*

Step 5 Configure the AP hostname by entering this command:

(cisco-wave2-ap)#configure ap hostname *ap-name*

Configuring a Dot1X Credential (CLI)

Procedure

- Configure a dot1x credential by entering this command:

  (cisco-wave2-ap)#configure dot1x credential *profile-name* **username** *name* **password** *pwd*

- [Optional] Delete a dot1x profile by entering this command:

  (cisco-wave2-ap)#configure dot1x credential *profile-name* **delete**

- Deauthenticate WGB client by entering this command:

  (cisco-wave2-ap)#clear wgb client {**all** | **single** *mac-addr*}

Configuring an EAP Profile (CLI)

Procedure

Step 1 Configure the EAP profile method type by entering this command:

(cisco-wave2-ap)#configure eap-profile *profile-name* **method** {**fast** | **leap** | **peap** | **tls**}

Step 2 Attaching the CA Trustpoint by entering this command:

(cisco-wave2-ap)#configure eap-profile *profile-name* **trustpoint** {**default** | **name** *trustpoint-name*}

Note
With the default profile, WGB uses the internal MIC certificate for authentication.

Step 3 Configure the 802.1X credentials profile by entering this command:

(cisco-wave2-ap)#configure eap-profile *profile-name* **dot1x-credential** *profile-name*

Step 4 [Optional] Delete an EAP profile by entering this command:

(cisco-wave2-ap)#configure eap-profile *profile-name* **delete**

Step 5 View the WGB EAP dot1x profile summary by entering this command:

(cisco-wave2-ap)#show wgb eap dot1x credential profile

Step 6 View summary of EAP and dot1x profiles by entering this command:

(cisco-wave2-ap)#show wgb eap profile all

Configuring Manual-Enrollment of a Trustpoint for Workgroup Bridge (CLI)

Procedure

Step 1 Create a Trustpoint in WGB by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **enrollment terminal**

Step 2 Authenticate a Trustpoint manually by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **authenticate**

Enter the base 64 encoded CA certificate and end the certificate by entering **quit** in a new line.

Step 3 Configure a private key size by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **key-size** *key-length*

Step 4 Configure the subject-name by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email*

Step 5 Generate a private key and Certificate Signing Request (CSR) by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **enroll**

Create the digitally signed certificate using the CSR output in the CA server.

Step 6 Import the signed certificate in WGB by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **import certificate**

Enter the base 64 encoded CA certificate and end the certificate by entering **quit** in a new line.

Step 7 [Optional] Delete a Trustpoint by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *trustpoint-name* **delete**

Step 8 View the Trustpoint summary by entering this command:

(cisco-wave2-ap)#show crypto pki trustpoint

Step 9 View the content of the certificates that are created for a Trustpoint by entering this command:

(cisco-wave2-ap)#show crypto pki trustpoint *trustpoint-name* **certificate**

Configuring an SSID Profile (CLI)

Procedure

- Choose one of the following authentication protocols for the SSID profile.
  - Configure an SSID profile with Open Authentication—**(cisco-wave2-ap)#configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication open**
  - Configure an SSID profile with PSK Authentication—**(cisco-wave2-ap)#configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication psk** *preshared-key* **key-management** {**dot11r** | **wpa2** | **dot11w** {**optional | required**}}
  - Configure an SSID profile with EAP Authentication—**(cisco-wave2-ap)#configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication eap profile** *eap-profile-name* **key-management** {**dot11r** | **wpa2** | **dot11w** {**optional | required**}}
- Attach a SSID profile to a radio interface by entering this command:

  (cisco-wave2-ap)#configure dot11radio *radio-nterface* **mode wgb ssid-profile** *profle-name*
- [Optional] Delete an SSID profile by entering this command:

  (cisco-wave2-ap)#configure ssid-profile *ssid-profile-name* **delete**
- View the summary of configured and connected SSIDs by entering this command:

  (cisco-wave2-ap)#show wgb ssid
- View the management, control, and data packet statistics by entering this command:

  (cisco-wave2-ap)#show wgb packet statistics

Configuring Radio Interface for Workgroup Bridges (CLI)

Procedure

- From the available two radio interfaces, before configuring WGB or UWGB mode on one radio interface, configure the other radio interface to root-ap mode.

  Map a radio interface as root-ap by entering this command:

  (cisco-wave2-ap)#configure dot11Radio *radio-int* **mode root-ap**

Note When an active SSID or EAP profile is modified, you need to reassociate the profile to the radio interface for the updated profile to be active.

- Map a radio interface to a WGB SSID profile by entering this command:

  (cisco-wave2-ap)#configure dot11Radio *radio-int* **mode wgb ssid-profile** *ssid-profile-name*

- Map a radio interface to a Universal WGB SSID profile by entering this command:

  (cisco-wave2-ap)#configure dot11Radio *radio-int* **mode uwgb** *mac-addr* **ssid-profile** *ssid-profile-name*

- Configure a radio interface by entering this command:

  (cisco-wave2-ap)#configure dot11Radio *radio-int* { **enable** | **disable** }

Note After configuring the uplink to the SSID profile, we recommend you to disable and enable the radio for the changes to be active.

- Configure the radio antenna by entering this command:

  (cisco-wave2-ap)#configure dot11Radio *radio-int* **antenna** { **a-antenna** | **ab-antenna** | **abc-antenna** | **abcd-antenna** }

- Enable encryption on a radio interface by entering this command:

  (cisco-wave2-ap)#configure dot11Radio *radio-int* **encryption mode ciphers aes-ccm**

- Configure the device channel rate by entering this command:

  (cisco-wave2-ap)#configure wgb mobile rate { **basic 6 9 18 24 36 48 54** | **mcs** *mcs-rate* }

- Configure the threshold duration and signal strength to trigger scanning by entering this command:

  (cisco-wave2-ap)#configure wgb mobile period *seconds thres-signal*

- Configure the static roaming channel by entering this command:

  (cisco-wave2-ap)#configure wgb mobile station interface dot11Radio *radio-int* **scan** *channel-number* **add**

- [Optional] Delete the mobile channel by entering this command:

  (cisco-wave2-ap)#configure wgb mobile station interface dot11Radio *radio-int* **scan** *channel-number* **delete**

- [Optional] Disable the mobile channel scanning by entering this command:

  (cisco-wave2-ap)#configure wgb mobile station interface dot11Radio *radio-int* **scan disable**

- Configure the beacon miss-count by entering this command:

  (cisco-wave2-ap)#configure wgb beacon miss-count *value*

  Default setting is set to disabled.

Note When you set the beacon miss-count value to 10 or lower, then the beacon miss-count gets disabled. Set the value to 11 or higher to enable this function.

- View the Wi-Fi station statistics by entering this command:

  (cisco-wave2-ap)#show wgb wifi *wifi-interface* **stats**

- View the radio antenna settings by entering this command:

  (cisco-wave2-ap)#show controllers dot11Radio *radio-interface* **antenna**

- View the mobile station channels scan configuration by entering this command:

  (cisco-wave2-ap)#show wgb mobile scan channel

- View the configuration that is stored in the NV memory by entering this command:

  (cisco-wave2-ap)#show configuration

- View the running configuration in the device by entering this command:

  (cisco-wave2-ap)#show running-config

Note The output displays the configured parameters only.

- View the WGB forwarding details by entering this command:

  (cisco-wave2-ap)#show wgb forwarding all

Configuring Workgroup Bridge Timeouts (CLI)

Procedure

- Configure the WGB association response timeout by entering this command:

  (cisco-wave2-ap)#configure wgb association response timeout *response-millisecs*

  The default value is 5000 milliseconds. The valid range is between 300 and 5000 milliseconds.

- Configure the WGB authentication response timeout by entering this command:

  (cisco-wave2-ap)#configure wgb authentication response timeout *response-millisecs*

  The default value is 5000 milliseconds. The valid range is between 300 and 5000 milliseconds.

- Configure the Universal WGB client response timeout by entering this command:

  (cisco-wave2-ap)#configure wgb uclient timeout *timeout-secs*

  The default timeout value is 60 seconds. The valid range is between 1 and 65535 seconds.

- Configure the WGB EAP timeout by entering this command:

  (cisco-wave2-ap)#configure wgb eap timeout *timeout-secs*

  The default value is 3 seconds. The valid range is between 2 and 60 seconds.

- Configure the WGB channel scan timeout by entering this command:

  (cisco-wave2-ap)#configure wgb channel scan timeout {**fast** | **medium** | **slow** }

- Configure the WGB DHCP response timeout by entering this command:

  (cisco-wave2-ap)#configure wgb dhcp response timeout *timeout-millisecs*

  The default value is 60 seconds. The valid range is between 1000 and 60000 milliseconds.

- View the WGB association summary by entering this command:

  (cisco-wave2-ap)#show wgb dot11 association

Configuring Bridge Forwarding for Workgroup Bridge (CLI)

The Cisco Wave 2 AP as Workgroup Bridge recognizes the Ethernet clients only when the traffic has the bridging tag.

We recommend setting the WGB bridge client timeout value to default value of 300 seconds, or less in environment where change is expected, such as:

- Ethernet cable is unplugged and plugged back.
- Endpoint is changed.
- Endpoint IP is changed (static to DHCP and vice versa).

If you require to retain the client entry in the WGB table for a longer duration, we recommend you to increase the client WGB bridge timeout duration.

Procedure

Step 1 Add a WGB client using the MAC address by entering this command:

(cisco-wave2-ap)#configure wgb bridge client add *mac-addr*

Step 2 Configure the WGB bridge client timeout by entering this command:

(cisco-wave2-ap)#configure wgb bridge client timeout *timeout-secs*

Default timeout value is 300 seconds. The valid range is between 10 and 1000000 seconds.

Step 3 View the WGB wired clients over the bridge by entering this command:

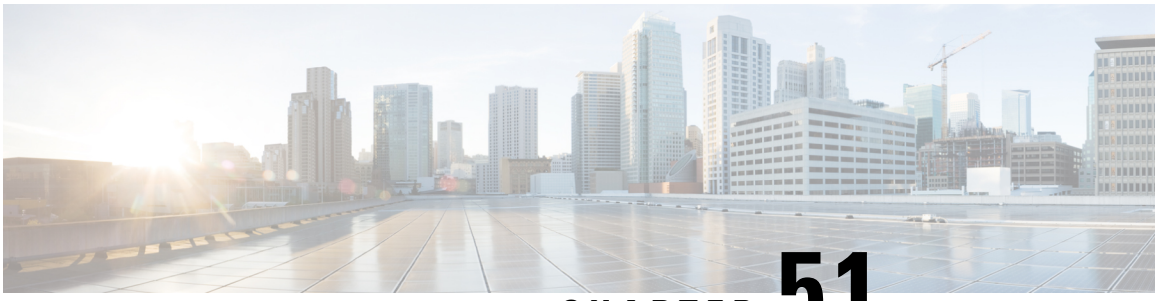
(cisco-wave2-ap)#show wgb bridge

Step 4 View the WGB Gigabit wired clients over the bridge by entering this command:

(cisco-wave2-ap)#show wgb bridge wired gigabitEthernet *giga-wire-interface*

Step 5 View the WGB bridge radio interface summary by entering this command:

(cisco-wave2-ap)#show wgb bridge dot11Radio *interface-number*



CHAPTER 51

Software-Defined Access Wireless

- Introduction to Software-Defined Access Wireless , on page 1139
- Configuring SD-Access Wireless (CLI), on page 1145
- Enabling SD-Access Wireless (GUI), on page 1146
- Configuring SD-Access Wireless VNID (GUI), on page 1147
- Configuring SD-Access Wireless WLAN (GUI), on page 1147
- Configuring DNS Access Control List on SD-Access (GUI), on page 1148

Introduction to Software-Defined Access Wireless

The Enterprise Fabric provides end-to-end enterprise-wide segmentation, flexible subnet addressing, and controller-based networking with uniform enterprise-wide policy and mobility. It moves the enterprise network from current VLAN-centric architecture to a user group-based enterprise architecture, with flexible Layer 2 extensions within and across sites.

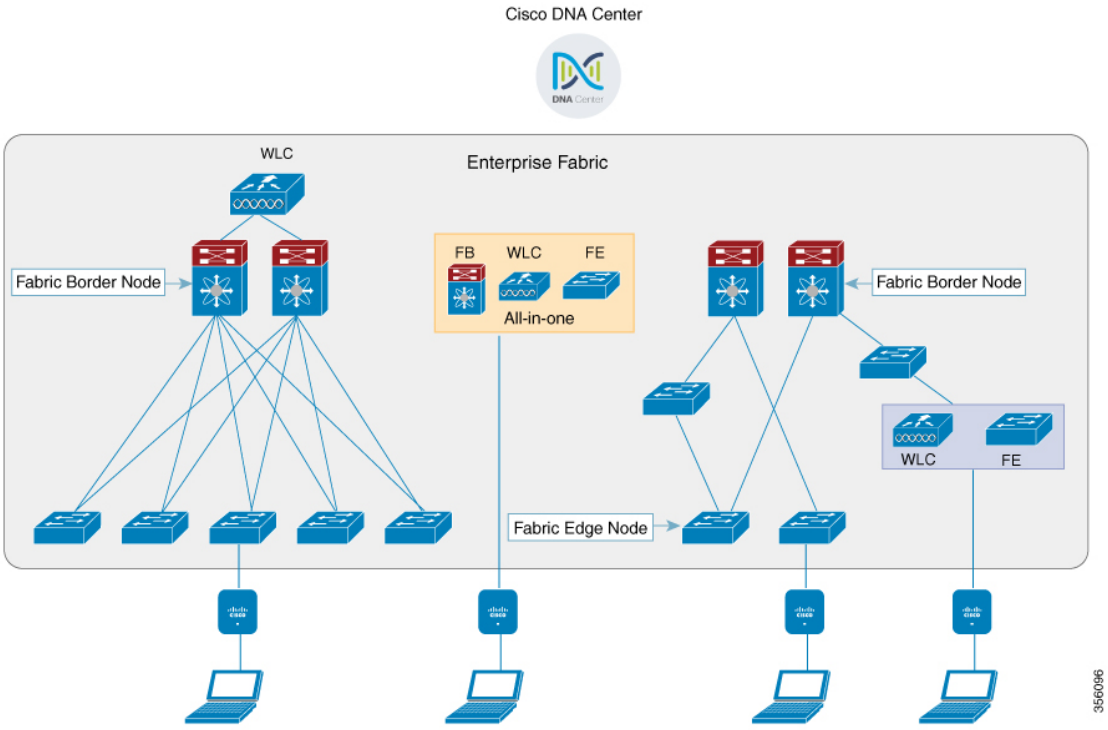
Enterprise fabric is a network topology where traffic is passed through inter-connected switches, while providing the abstraction of a single Layer 2 or Layer 3 device. This provides seamless connectivity, with policy application and enforcement at the edge of the fabric. Fabric uses IP overlay, which makes the network appear as a single virtual entity without using clustering technologies.

The following definitions are used for fabric nodes:

- **Enterprise Fabric**: A network topology where traffic is passed through inter-connected switches, while providing the abstraction of a single Layer 2 or Layer 3 device.
- **Fabric Domain**: An independent operation part of the network. It is administered independent of other fabric domains.
- **End Points**: Hosts or devices that connect to the fabric edge node are known as end points (EPs). They directly connect to the fabric edge node or through a Layer 2 network.

The following figure shows the components of a typical SD-Access Wireless. It consists of Fabric Border Nodes (BN), Fabric Edge Nodes (EN), Wireless Controller, Cisco DNA Center, and Host Tracking Database (HDB).

Figure 78: Software-Defined Access Wireless



The figure covers the following deployment topologies:

- All-in-one Fabric—When we have all Fabric Edge, Fabric Border, Control-Plane and controller functionality enabled on a Catalyst 4500E switch. This toplogy is depicted in the mid part of the figure.
- Split topology—When we have Fabric Border, or Control Plane, or controller on a Catalyst 4500E switch with separate Fabric Edge. This toplogy is depicted in the left-most part of the figure.
- Co-located Fabric Edge and Controller—When we have Fabric Edge and controller on a Catalyst 4500E switch. This toplogy is depicted in the right-most part of the figure.

Cisco DNA Center: Is an open, software-driven architecture built on a set of design principles with the objective of configuring and managing Catalyst 4500E Series switches.

Host ID Tracking Database(map-server and map-resolver in LISP): This database allows the network to determine the location of a device or user. When the EP ID of a host is learnt, other end points can query the database about the location of the host. The flexibility of tracking subnets helps in summarization across domains and improves the scalability of the database.

Fabric Border Node(Proxy Egress Tunnel Router [PxTR or PITR/PETR] in LISP): These nodes connect traditional Layer 3 networks or different fabric domains to the enterprise fabric domain. If there are multiple fabric domains, these nodes connect a fabric domain to one or more fabric domains, which could be of the same or different type. These nodes are responsible for translation of context from one fabric domain to another. When the encapsulation is the same across different fabric domains, the translation of fabric context is generally 1:1. The fabric control planes of two domains exchange reachability and policy information through this device.

Fabric Edge Nodes(Egress Tunnel Router [ETR] or Ingress Tunnel Router [ITR] in LISP): These nodes are responsible for admitting, encapsulating or decapsulating, and forwarding of traffic from the EPs. They lie at the perimeter of the fabric and are the first points of attachment of the policy. EPs could be directly or indirectly attached to a fabric edge node using an intermediate Layer 2 network that lies outside the fabric domain. Traditional Layer 2 networks, wireless access points, or end hosts are connected to fabric edge nodes.

Wireless Controller: The controller provides AP image and configuration management, client session management and mobility. Additionally, it registers the mac address of wireless clients in the host tracking database at the time of client join, as well as updates the location at the time of client roam.

Access Points: AP applies all the wireless media specific features. For example, radio and SSID policies, webauth punt, peer-to-peer blocking, and so on. It establishes CAPWAP control and data tunnel to controller. It converts 802.11 data traffic from wireless clients to 802.3 and sends it to the access switch with VXLAN encapsulation.

The SDA allows to simplify:

- Addressing in wireless networks
- Mobility in wireless networks
- Guest access and move towards multi-tenancy
- Leverage Sub-net extension (stretched subnet) in wireless network
- Provide consistent wireless policies

Related Topics

Software Defined Access and FlexConnect Post Authentication IPv6 ACL Support, on page 1234

AP Bring-up Process

The sequence of bringing up an AP is given below:

- Switch powers up the AP (POE or UPOE)
- AP gets an IP address from the DHCP server.
- Switch registers the IP address of the AP with the map server.
- AP discovers controller through CAPWAP discovery.
- After Datagram Transport Layer Security (DTLS) handshake, CAPWAP control tunnel is created between AP and controller for control packets. CAPWAP data tunnel is created for IEEE 802.11 management frames. The AP image is downloaded and the configuration is pushed on AP from controller.
- Controller queries the map server for the switch (RLOC IP) behind which the AP has been registered.
- Controller registers a dummy MAC address with the map server.
- Map server sends a dummy MAC address notification to the switch to create a VXLAN tunnel to AP.
- AP is ready to accept clients.

Onboarding the Wireless Clients

The sequence of onboarding the clients is given below:

- The wireless client associates itself with the AP.
- Client starts IEEE 802.1x authentication on Controller (if configured) using CAPWAP data tunnel.
- After Layer 2 authentication is complete, Controller registers MAC address of the client with map server.
- Map server sends a notify message to switch with the client details.
- Switch adds the client MAC to the Layer 2 forwarding table.
- Controller moves the client to RUN state and the client can start sending traffic.
- Switch registers the IP address of the client to the MAP server.
- The switch decapsulates the VXLAN packet.
- The switch forwards the DHCP packet to the DHCP server or relay.
- The switch receives the DHCP ack for the wireless client. Switch learns the IP address of the client and sends an update to the map server.
- Switch broadcasts the DHCP ack to all ports in the VLAN, including the AP facing VXLAN tunnels.
- DHCP acknowledgment reaches AP, which forwards it to the client.
- AP sends IP address of the client to controller.
- controller moves the client to the RUN state.

Platform Support

Table 46: Supported AireOS Controllers

Controller	Support
3504	Yes
5520	Supported only on the local mode AP
8540	Supported only on the local mode AP
vWLC	No

Table 47: AP Support

AP	Support
802.11n	No
802.11ac Wave 1	Yes
802.11ac Wave 2	Yes
Mesh	No

Table 48: Client Security

Security	Support
Open and Static WEP	No
WPA-PSK	Yes
802.1x (WPA/WPA2)	Yes
MAC Filtering	Yes
CCKM Fast Roaming	Yes
Local EAP	Yes. However, it is not recommended.
AAA Override	Supported for SGT, L2 VNID, ACL policy, and QoS policy.
Internal WebAuth	IPv4 clients
External Webauth	IPv4 clients
Pre Auth ACL	IPv4 clients
FQDN ACL	No

Table 49: IPv6 Support

IPv6	Support
IPv6 Infra Support	No
IPv6 Client Support	Yes (From Release 8.8 onwards)

Table 50: Polciy, QoS, and Feature Support

Features	Support
IPv4 ACL for Clients	Yes. Flex ACL for ACL at AP.
IPv6 ACL for Clients	Yes (From Release 8.8 onwards)
P2P Blocking	Supported through security group tag (SGT) and security group ACL (SGACL) on the switch for clients on the same AP.
IP Source Guard	Switches
AVC Visibility	AP
AVC QOS	AP
Downloadable Protocol Pack updates	No

Features	Support
Device profiling	No
mDNS Proxy	No
MS Lync Server QOS Integration	No
Netflow Exporter	No
QoS	Yes (Metal profiles and rate limiting)
Passive Client/Silent Host	No
Location tracking / Hyperlocation	Yes
Wireless Multicast	Yes **Note** Video streaming is supported from Release 8.8 onwards.
URL Filtering	No
HA	Controller to controller

Migration From Converged Access

The following list shows the migration process from converged access to fabric wireless:

1. Bring up the controller with image supporting fabric mode.
2. Configure the network with the fabric mode for the appropriate subnets, using an APIC-EM or CLIs. We recommed that you use APIC-EM for this purpose.
3. Configure the discovery mechanism such that the DHCP discovery on the new AP subnet should lead to the controller supporting fabric mode.
4. When the AP comes up, do a DHCP request and get the IP address in the AP VLAN.
5. The AP creates a control plane CAPWAP tunnel with the controller.
6. Based on the configuration, the controller programs the AP for the fabric mode.
7. AP follows the SDA for wireless flow.

Note

- Mobility between fabric and non-fabric SSIDs are not supported
- AP images and licenses are hosted on the controller and the AP fetches the images and licenses directly from it. APIC-EM is responsible for managing the AP licenses on the controller.
- After a TCP connection flap in the controller, it takes about five to six minutes to reestablish the connection. During this time, the access tunnels gets reset during client join.

Restrictions

- In a preauthentication scenario, IP addresses (either IPv4 or IPv6) learned via DNS resolution are lost after controller switchover.
- HA sync for Fabric related statistics is not supported.

Additional References

For more information about software-defined access wireless, see the *SD-Access Wireless Design and Deployment Guide* at https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf.

Configuring SD-Access Wireless (CLI)

Perform the following steps to configure fabric on a WLAN.

Before you begin

- Configure the AP in local mode to enable fabric on it.

Procedure

Step 1 **config wlan fabric enable** *wlanid*

Example:

```
config wlan fabric enable wlan1
```

Enables Fabric on the WLAN.

Step 2 **config wlan fabric vnid** *vnid wlanid*

Example:

```
config wlan fabric vnid 10 wlan1
```

Configures a Virtual Extensible LAN (VXLAN) network identifier (VNID) on fabric WLAN.

Step 3 **config wlan fabric encap vxlan** *wlanid*

Example:

```
config wlan fabric encap vxlan wlan1
```

Maps a VNID to the fabric WLAN.

Step 4 **config wlan fabric switch-ip** *ip-address wlanid*

Example:

```
config wlan fabric switch-ip 209.165.200.10 wlan1
```

Sets a VLAN peer ip to WLAN.

Step 5 **config wlan fabric** [**ipv6**] **acl** {*fabric-acl-name* | **none**} *wlan-id*

Example:

```
config wlan fabric acl fabric-acl wlan1
```

Configures a FlexConnect ACL on the controller and associates it with the Fabric WLAN. To dissociate a FlexConnect ACL from the Fabric WLAN, use the **none** option.

Step 6 **config fabric flex-acl-template template-entry** *template-name* {**add** | **delete**} *acl-name*

Example:

```
config fabric flex-acl-template template-entry myflextemplate add myflexacl
```

Pushes the ACL to AP and applies it to client via AAA.

Step 7 **config wlan fabric avc-policy** *fabric-avc-policy wlanid*

Example:

```
config wlan fabric fabric-avc-policy wlan1
```

Configures an AVC profile name associates it with the fabric WLAN.

Step 8 **config wlan fabric controlplane guest-fabric enable** *wlanid*

Example:

```
config wlan fabric controlplane guest-fabric enable wlan1
```

(Optional) Enables guest fabric for this WLAN .

Step 9 **show fabric summary**

Example:

```
show fabric summary
```

(Optional) Displays the fabric configuration summary.

Enabling SD-Access Wireless (GUI)

Use the following procedure to enable fabric and configure parameters on the enterprise and guest controllers.

Procedure

Step 1 Choose **Controller > Fabric Configuration > Control Plane**.

The Fabric Control Configuration page is displayed.

Step 2 Move the Fabric slider to enable or disable Fabric.

You can enable fabric and configure parameters on the enterprise and guest controllers, using the Fabric Enable/Disable option at the top of the screen.

Step 3 Select the check box in the Primary IP Address field to enable the fields.

Step 4 Enter an IP address in the **Primary IP Address** field.

Step 5 Enter a shared key in the **Pre Shared Key** field.

Step 6 The **Connection Status** field shows the connection status of the Fabric.

Step 7 Repeat the procedure described in steps 3 to 6 for **Secondary IP Address** and in the **Guest Controllers** section.

Step 8 Click **Apply**.

Configuring SD-Access Wireless VNID (GUI)

Use the following procedure to enable fabric and configure parameters on the enterprise and guest controllers.

Procedure

Step 1 Choose **Controller > Fabric Configuration > Interface**.

The **Fabric Interface > Edit** page is displayed.

Step 2 Enter an interface name in the **Fabric Interface Name** field.

Step 3 Enter an instance ID in the **L2 Instance ID** field.

Step 4 Enter the network IP adddress in the **Network IP** field.

Step 5 Enter the subnet mask at the **Subnet Massk** field.

Step 6 Enter an instance ID in the **L3 Instance ID** field.

Step 7 Click **Apply**.

Configuring SD-Access Wireless WLAN (GUI)

Use the following procedure to configure Fabric WLAN parameters.

Procedure

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 Select the Enabled check box under the Fabric Configuration section.

Step 5 Use the drop down to select the **Fabric Interface Name**.

Step 6 Enter an instance ID in the **L2 Instance ID** field.

Step 7 Enter the IP adddress in the **Peer IP** field.

Step 8 Use the drop down to select the **Fabric ACL** name.

Step 9 Use the drop down to select the **Fabric AVC** name.

Step 10 Click **Apply**.

Configuring DNS Access Control List on SD-Access (GUI)

Use the following procedure to configure Fabric DNS ACL parameters.

Procedure

Step 1 Configure the Control Place parameters.

See the Enabling SD-Access Wireless procedure.

Step 2 Configure the Fabric Interface parameters.

See the Configuring Fabric Interface procedure.

Step 3 Choose **WLANs** > **WLAN ID** > **Security** to open the WLANs Edit page.

Step 4 In the Security tab, set the Layer 3 Security to **Web Policy** from the drop-down list on the Layer 3 tab.

Step 5 From the **Preauthentication ACL** > **WebAuth FlexAcl** drop-down list choose the ACL option that you want to apply to the WLAN.

Step 6 Click **Apply**.

Configuring Access Control List Templates (GUI)

Procedure

Step 1 Choose **Controller** > **Fabric Configuration** > **Templates**.

The page displays the list of Fabric ACLs.

Step 2 To create a template:

You can create a new template (a) or copy an existing template (b) to create a new template.

- To create a new template—Choose **Fabric ACL Template** > **New** and enter the name of the template. Click **Apply**.
- To create a new template based on an existing template—Click **Copy**, enter the name of the template, and choose a template from the **Existing Fabric Templates** drop-down list. Click **Copy**.

Step 3 Click **Apply**.

Step 4 To link a FlexConnect ACL to this template, click the template name on the **Fabric ACL Template List** page.

The **Fabric ACL Template** > **Edit** page is displayed.

Step 5 From the **IPv4 ACL / IPv6 ACL** drop-down list, choose the post authentication ACL that you want to add to the Fabric ACL template.

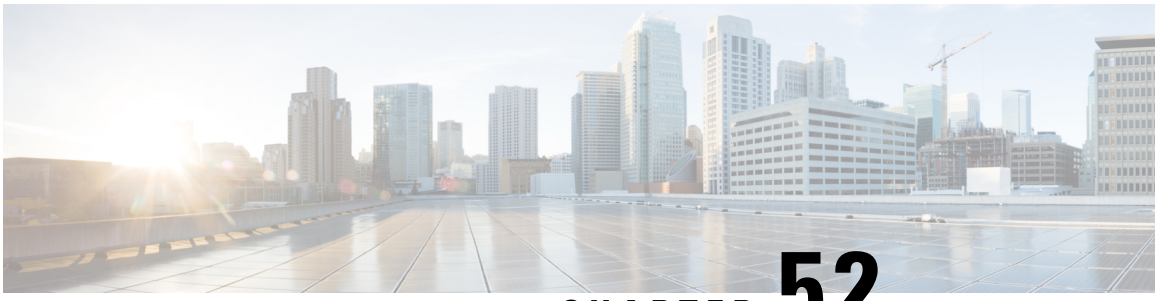
Step 6 Click **Add**.

Step 7 Save the configuration.

PART VIII

FlexConnect

- FlexConnect, on page 1153
- FlexConnect Groups, on page 1183
- FlexConnect Security, on page 1223
- OfficeExtend Access Points, on page 1239
- FlexConnect AP Image Upgrades, on page 1253
- FlexConnect AP Easy Admin, on page 1257
- WeChat Authentication Based Internet Access , on page 1259
- Lawful Interception of Traffic, on page 1265



CHAPTER 52

FlexConnect

- FlexConnect Overview, on page 1153
- FlexConnect Switching Modes, on page 1158
- FlexConnect Operation Modes, on page 1158
- FlexConnect VLANs and ACLs, on page 1159
- Central DHCP Server for FlexConnect, on page 1159
- Guidelines and Restrictions on FlexConnect, on page 1159
- Configuring FlexConnect, on page 1161

FlexConnect Overview

FlexConnect 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.

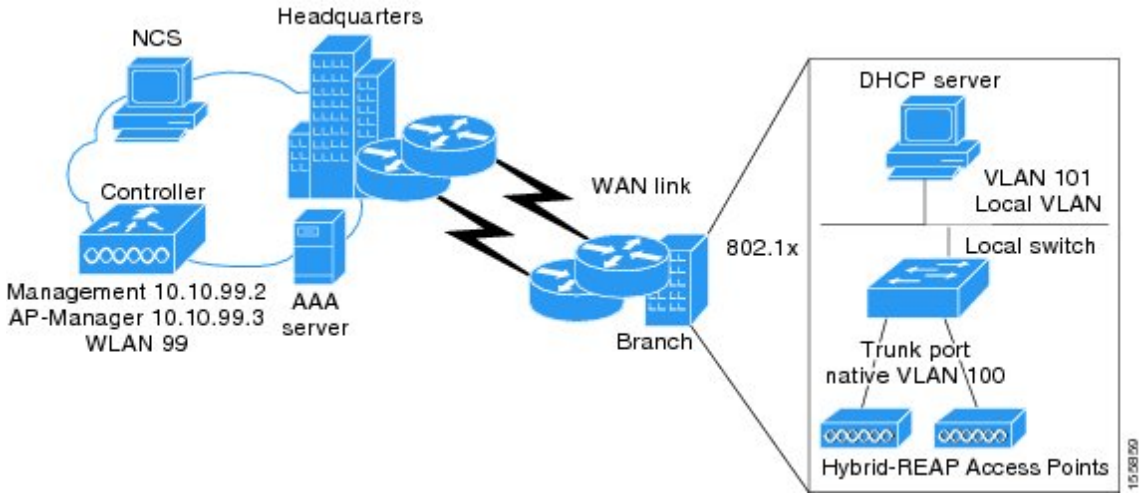
A FlexConnect AP can, on a per-WLAN basis, either tunnel client data in CAPWAP to the controller (called Central Switching), or have client data egress at the AP's LAN port (called Local Switching). With Locally Switched WLANs, the AP can tag client traffic in separate VLANs, to segregate the traffic from its management interface.

For a Locally Switched WLAN, the client authentication can either be handled by the controller (Central Authentication) or by the AP (Local Authentication).

If a FlexConnect AP should lose its CAPWAP connection to its controller, it goes into Standalone mode. In Standalone mode, any Centrally Switched WLANs are down, but Locally Switched WLANs remain operational. If the Locally Switched WLAN is configured for Central Authentication, the associated clients remain connected when the AP goes into Standalone mode, but will be unable to form new associations. A Locally Switched WLAN that uses Local Authentication remains operational whether the AP is in Standalone or Connected mode.

Figure 79: 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.

When AP is changed from local mode to FlexConnect mode, the AP does not reboot. However, when the AP is changed from FlexConnect mode to local mode, the AP reboots and displays the following error message:

```
Warning: Changing AP Mode will reboot the AP and will rejoin the controller
after a few minutes. Are you sure you want to continue?
```

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.
- 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.
  - 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.

- 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. his configuration is also correct for WLANs that are configured for 802.1X, WPA-802.1X, WPA2-802.1X, or Cisco Centralized Key Management, 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.

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.

FlexConnect Switching Modes

FlexConnect APs are capable of supporting the following switching modes concurrently, on a per-WLAN basis:

- **Local Switched**: Locally-switched WLANs map wireless user traffic to discrete VLANs via 802.1Q trunking, either to an adjacent router or switch. If so desired, one or more WLANs can be mapped to the same local 802.1Q VLAN.

  A branch user, who is associated to a local switched WLAN, has their traffic forwarded by the on-site router. Traffic destined off-site (to the central site) is forwarded as standard IP packets by the branch router. All AP control/management-related traffic is sent to the centralized controller separately via Control and Provisioning of Wireless Access Points protocol (CAPWAP).

- **Central Switched**: Central switched WLANs tunnel both the wireless user traffic and all control traffic via CAPWAP to the centralized controller where the user traffic is mapped to a dynamic interface/VLAN on the controller. This is the normal CAPWAP mode of operation.

  The traffic of a branch user, who is associated to a central switched WLAN, is tunneled directly to the centralized controller. If that user needs to communicate with computing resources within the branch (where that client is associated), their data is forwarded as standard IP packets back across the WAN link to the branch location. Depending on the WAN link bandwidth, this might not be desirable behavior.

IP Learning in FlexConnect Local Mode

In FlexConnext local switching scenarios, clients from the same sites may share the same address range, there is a possibility of multiple clients being allocated or registered with the same IP address. The controller receives IP address information from the AP, and if more than one client attempts to use the same IP address, the controller discards the last device trying to register an already-used address as an IP theft event, potentially resulting in client exclusion.

We recommend disabling IP learning in FlexConnect mode using the **config network ip-mac-binding disabled** command to ensure that no device tracking is done for clients, thus preventing the IP theft error.

Note This feature is applicable only for IPv4 addresses.

FlexConnect Operation Modes

FlexConnect APs can operate in the following modes:

- **Connected Mode**: The controller is reachable. In this mode, the FlexConnect AP has CAPWAP connectivity with its controller.
- **Standalone Mode**: The controller is unreachable. The FlexConnect AP has lost or failed to establish CAPWAP connectivity with its controller; for example, when there is a WAN link outage between a branch and its central site.

FlexConnect VLANs and ACLs

You can configure the LAN uplink interface of a FlexConnect AP as either an access port or as a trunk. If you configure the interface \as an access port, then the AP's management traffic and all client traffic, whether centrally or locally switched, will be in the same VLAN. For security and reliability reasons, we recommend that you segregate the client traffic from the management VLAN, and so to configure the AP's switchport as a trunk, with separately tagged VLANs for locally switched client traffic.

Note Do not confuse VLAN tagging for FlexConnect client VLANs with the management interface VLAN tagging feature, which is enabled under the **Advanced** tab for the AP configuration. Management interface VLAN tagging is configured independently of the AP's mode, and is not needed in order to tag client VLANs.

Central DHCP Server for FlexConnect

Ordinarily, a FlexConnect local switched WLAN will bridge client DHCP to the local VLAN. If a DHCP server or relay is not available on local VLANs, the Central DHCP Server feature can be used. For more information about configuring this feature, see https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/211325-FlexConnect-Central-DHCP-Configuration-E.html

Restrictions for Central DHCP Server for FlexConnect

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.

Guidelines and 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.

- Cisco FlexConnect mode requires that the client send traffic before learning the client's IPv6 address. Compared to in local mode where the controller learns the IPv6 address by snooping the packets during Neighbor Discovery to update the IPv6 address of the client.
- 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.
- 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.
- Cisco AP in FlexConnect mode loses the VLAN mapping after every reboot.
- 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 on locally switched WLANs is supported on Second-Generation APs.
- 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 controller 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 controller, 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.
- The Cisco Wave 2 APs in FlexConnect mode attempt discovery of the controller 18 times before renewing the DHCP on the Ethernet interface to get a new DHCP IP address. In a non-FlexConnect mode, the Cisco Wave 2 APs attempt discovery five times before renewing the IP address.

Configuring FlexConnect

Note The configuration tasks must be performed in the order in which they are listed.

Configuring the Switch at a Remote Site

Procedure

Step 1 Attach the AP 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 AP 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 AP.

In this sample configuration, the FlexConnect AP is connected to trunk interface FastEthernet 1/0/2 with native VLAN 100. The AP 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 AP, 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 192.168.200.224 255.255.255.224
   default-router 192.168.200.225
   dns-server 192.168.100.167
!
ip dhcp pool LOCAL-SWITCH
   network 192.168.201.224 255.255.255.224
   default-router 192.168.201.225
   dns-server 192.168.100.167
!
interface GigabitEthernet1/0/2
 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 192.168.200.225 255.255.255.224
!
interface Vlan101
 ip address 192.168.201.226 255.255.255.229
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 51: 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)

WLAN	Security	Authentication	Switching	Interface Mapping (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*.

Procedure

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)

Procedure

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** field, enter a unique profile name for the WLAN.

Step 5 In the **WLAN SSID** field, 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 controller, you will see ip-theft false positives. If ip-theft exclusion is enabled on the controller, 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).
  - 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.

- Check or uncheck the **FlexConnect Local Auth** check box to enable or disable local authentication for the WLAN.
- Check or uncheck the **Learn Client IP Address** check box to enable or disable the IP address of the client to be learned.

- Check or uncheck the **VLAN based Central Switching** check box to enable or disable central switching on a locally switched WLAN based on AAA overridden VLAN. For more information see https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/FlexConnect_DG.html#pgfId-43615.

  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.

- Check or uncheck 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.
- Check or uncheck 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.
- Check or uncheck 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.
- Check or uncheck the **Central Assoc** check box to enable or disable client reassociation and security key caching on the controller. The PMIPv6 MAG on AP feature requires that the client reassociation be handled centrally at the controller in large-scale deployments of Cisco APs, to support fast roaming.

  Configuration of central association with local authentication is not supported for the WLAN. After the PMIPv6 tunnel is set up, all data traffic from the PMIPv6 clients are forwarded from the Cisco AP to the local mobility anchor (LMA) in the Generic Routing Encapsulation (GRE) tunnel. If the connectivity between the Cisco AP and the controller is lost, the data traffic for the existing PMIPv6 clients continues to flow until the connectivity between the Cisco AP and the client is lost. When the AP is in stand-alone mode, no new client associations are accepted on the PMIPv6-enabled WLAN.

Step 9 Save the configuration.

Related Topics

Configuring IP-MAC Context Distribution For FlexConnect Local Switching Clients (GUI), on page 1185

Configuring the Controller for FlexConnect (CLI)

Procedure

Step 1 **config wlan flexconnect local-switching** *wlan_id* **enable**—Configures the WLAN for local switching.

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.

Additional Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/FlexConnect_DG.html#pgfId-43615

Step 4 **config wlan flexconnect central-assoc** *wlan-id* {**enable** | **disable**}— Informs the Cisco AP in FlexConnect mode to handle client association and reassociation and security key caching for the clients on the WLAN by the controller. The PMIPv6 MAG on AP feature requires that the client reassociation be handled centrally at the controller in large-scale deployments of Cisco APs, to support fast roaming.

By default, the client association and reassociation and security key caching are handled by the Cisco AP in FlexConnect mode.

Configuration of central association with local authentication is not supported for the WLAN. After the PMIPv6 tunnel is set up, all data traffic from the PMIPv6 clients are forwarded from the Cisco AP to the local mobility anchor (LMA) in the Generic Routing Encapsulation (GRE) tunnel. If the connectivity between the Cisco AP and the controller is lost, the data traffic for the existing PMIPv6 clients continue to flow until the connectivity between the Cisco AP and the client is lost. When the AP is in stand-alone mode, no new client associations are accepted on the PMIPv6 enabled WLAN.

Step 5 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 6 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.

Procedure

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.

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.

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 Web Policy ACL on an AP in FlexConnect mode by entering this command:

  config ap flexconnect web-policy policy acl {**add** | **delete**} *acl_name cisco_ap*

Note You can configure up to 16 Web 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.
- **show flexconnect client exclusion-list**—Displays the list of clients which are in the exclusion list of the Wave 2 AP's locally.

Use these commands on the FlexConnect access point to get the mac addresses of the client:

- **show flexconnect client counter vlan-central-switching**—Shows the mac addresses of the vlan centrally switched client and its corresponding centrally and locally switched counters of the packets.

- **show flexconnect client local-switching**—Shows the mac addresses of the locally switched client and its corresponding centrally and locally switched counters of the packets.

Note These commands can be entered on the AP console only. If you enter these commands on the AP console, the commands are not communicated to the controller.

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.
- **debug flexconnect wlan-vlan** {**enable** | **disable**}—Enables or disables debugging of FlexConnect wlan-vlan.

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

Procedure

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.
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.
- **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
. . .
. . .
```

Configuring FlexConnect Ethernet Fallback

Information About FlexConnect Ethernet Fallback

You can configure an AP to shut down its radio when the Ethernet link is not operational. When the Ethernet link comes back to operational state, you can configure the AP to set its radio back to operational state. This feature is independent of the AP being in connected or standalone mode. When the radios are shut down, the AP does not broadcast the WLANs, and therefore, the clients cannot connect to the AP, either through first association or through roaming.

To prevent radios from flapping when there is flapping of the Ethernet interface, a delay timer, which you can configure, is provided.

Restrictions for FlexConnect Ethernet Fallback

- The carrier delay that you configure on the Ethernet interface shuts down and reloads the interface based on hysteresis. Therefore, the delay that you configure might not be the exact delay before the Ethernet and 802.11 interfaces are shut down and reloaded.

Configuring FlexConnect Ethernet Fallback (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration**.

The **Global Configuration** page is displayed.

Step 2 In the **FlexConnect Ethernet Fallback** area, select or unselect the **Radio Interface Shutdown** check box.

Step 3 If you select the **Radio Interface Shutdown** check box, enter the delay or the Ethernet interface downtime, in seconds, after which the AP radio interface must be shut down. The default delay is 0 seconds.

Note
You can enter the delay only if you select the **Radio Interface Shutdown** check box.

Step 4 In the **FlexConnect Ethernet Fallback** area, select the **FlexConnect Arp-Cache** check box to add ARP entry for a client with locally switched WLAN on FlexConnect APs.

Note
This step enables the broadcast of ARP requests and the APs respond on behalf of the client.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuring FlexConnect Ethernet Fallback (CLI)

Procedure

Step 1 Configure the radio interface by entering this command:
config flexconnect fallback-radio-shut {**disable** | **enable delay** *time-in-seconds*}

Step 2 See the status of the FlexConnect Ethernet Fallback feature configuration by entering this command:
show flexconnect summary

Step 3 Add proxy ARP with locally switched WLAN on FlexConnect APs by entering this command:
config flexconnect arp-cache.

VideoStream for FlexConnect

Information About VideoStream for FlexConnect

For FlexConnect Access Points, the controller configures both centrally switched WLANs and locally switched WLANs. FlexConnect APs support multicast-to-unicast video traffic in the Local switching mode. In this mode, the WLANs are configured to bridge the data from the client to the wired interface of the FlexConnect APs.

A wireless client subscribes to an IP multicast stream by sending an Internet Group Management Protocol (IGMP) packet or JOIN message. The AP eBridge module receives the IGMP packets.

The IGMP packets are forwarded to the IGMP snooping module for processing.

The IGMP snooping module searches the VideoStream configuration table. If the destination group address is configured as a multicast-to-unicast stream, the module adds a record to the multicast-to-unicast list in the group-tracking table. Otherwise, it adds the record to the multicast-only list. The module tracks the hosts, groups, and group memberships for each radio in the database.

When downstream multicast packets arrive at the AP from the locally switched WLANs, the packet handler searches the mgroup table.

If the VideoStream exists on an AP and the locally switched WLAN has the Multicast Direct feature enabled, and streams are provided for the IP addresses, all the clients on the WLAN for the stream have the Multicast-to-Unicast feature enabled. In all scenarios, only the Multicast Direct feature is enabled.

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

Configuring VideoStream for FlexConnect (GUI)

The Internet Group Management Protocol (IGMP) module analyzes the multicast packets and places packet information into the host and group-tracking databases. On the basis of the controller configuration, the IGMP module admits the video multicast-to-unicast stream.

IGMP snooping and multicast forwarding is enabled on the local switch. The VideoStream group IP address is configured on controller and the index is less than 100. controller has an On/Off switch for the Multicast-to-Unicast feature at the global level, and per WLAN.

Each WLAN maps to a VLAN for a FlexConnect access point (AP). Therefore, a WLAN is equal to the On/Off switch. When the feature is turned on for a VLAN, it is only applied to provisioned media stream groups.

Before you begin

Before you configure VideoStream for FlexConnect, enable the multicast mode and the IGMP snooping as follows:

1. Choose **Controller** > **Multicast** to open the Multicast page.
2. Check the **Enable Global Multicast Mode** check box to configure the sending multicast packets task. (The check box is disabled by default.)
3. Click **Save Configuration** to save your changes.

Note VideoStream for FlexConnect configuration does not support IPv6 and the Multicast Listener Discovery (MLD) snooping.

Note See the section Configuring the Controller for FlexConnect for information about configuring the controller for FlexConnect in a locally switched WLAN.

Procedure

Step 1 Choose **Wireless** > **Media Stream** > **Streams** to open the Media Stream page.

Step 2 Click **Add New** to configure a new media stream. The **Media Streams** page is displayed.

Step 3 In the **Stream Name** text box, enter the media stream name. The stream name can be up to 64 characters.

Step 4 In the **Multicast Destination Start IP Address** text box, enter the start IPv4 address of the multicast media stream.

Step 5 In the **Multicast Destination End IP Address** text box, enter the end IPv4 address of the multicast media stream.

Note
For the resource reservation control, only the start and end IP addresses are important.

Step 6 Click **Apply**.

Because of the CAPWAP payload length limit, only the first 100 media streams are pushed from the controller to the corresponding AP.

The media stream configurations are pushed to the AP, after the AP joins the controller.

Note
Roaming is not supported in the standalone mode of the FlexConnect AP feature.

What to do next

Verify that the clients are associated by performing these steps:

1. Choose **Monitor** > **Multicast**.

   The Multicast Groups page is displayed.

2. View the details in the FlexConnect Multicast Media Stream Clients table.

Configuring VideoStream for FlexConnect (CLI)

Procedure

Step 1 Configure the Multicast feature on the WLANs media stream by entering the **config wlan media-stream multicast-direct** {**wlan_id** | **all**} {**enable** | **disable**} command.

Step 2 Enable or disable the Multicast feature by entering the **config media-stream multicast-direct** {**enable** | **disable**} command.

Step 3 Configure the various message-configuration parameters by entering the **config media-stream message** {**state** [**enable** | **disable**] | **url** *url* | **email** *email* | **phone** *phone _number* | **note** *note*} command.

Step 4 Save your changes by entering the **save config** command.

Step 5 Configure various global media-stream configurations by entering the **config media-stream add multicast-direct** *media_stream_name start_IP end_IP* [**template** {**very-coarse** | **coarse** | **ordinary** | **low-resolution** | **med-resolution** | **high-resolution**} | **detail** {*max_bandwidth avg-packet-size* | {**periodic** | **initial**}} *qos usage-priority* {**drop** | **fallback**} command.

The Resource Reservation Control (RRC) parameters are assigned with the predefined values based on the values assigned to the template.

The following templates can be 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 the **config media-stream delete** *media_stream_name* command.

Step 7 Save your changes by entering the **save config** command.

What to do next

To view the FlexConnect summary, use the following commands:

- **show capwap mcast flexconnect clients**
- **show running b | i mcuc**
- **show capwap mcast flexconnect groups**
- **show media-stream client flexconnect summary**

The following is the output **show media-stream client flexconnect summary** of command:

```
Client Mac    Stream-Name  Multicast-IP AP-Name   VLAN
----------     -----------  -----------  ----    ------
media-stream client FlexConnect <Media Stream Name>

Media Stream Name.............................. test
IP Multicast Destination Address (start)......... 224.0.0.1
IP Multicast Destination Address (end)........... 224.0.0.50
```

Viewing and Debugging Media Streams

Use these commands on a FlexConnect AP to get debug information:

Procedure

Step 1 **debug capwap mcast**
Shows general multicast activities.

Step 2 **debug ip igmp snooping group**
Shows the IGMP snooping group.

Step 3 **debug ip igmp snooping timer**
Shows IGMP snooping timer.

Step 4 **debug ip igmp snooping host**
Shows IGMP snooping host.

What to do next

- View a summary of the media stream and client information by entering the **show media-stream group summary** command.
- View details about a particular media stream group by entering **show media-stream group detail media_stream_name** command.
- Enable debugging of the media stream history by entering **debug media-stream history {enable | disable}** command.

FlexConnect+Bridge Mode

Information about Flex+Bridge Mode

A Control and Provisioning of Wireless Access Points protocol (CAPWAP) Access Point (AP) can be configured to operate in two different modes:

- FlexConnect mode
- Bridge/Mesh mode

The following are the bridging features for Flex+Bridge mode:

- The Flex+Bridge mode supports the centrally switched 802.11 WLAN. Traffic for this tunneled WLAN is forwarded to and from a CAPWAP controller over an IP tunnel.
- The Flex+Bridge mode supports the Root Ethernet VLAN Bridging. A root AP bridges the traffic for bridged 802.11 WLANs and secondary Ethernet LANs to a local Ethernet LAN over its root Ethernet port.
- The Flex+Bridge mode bridging is supported on Secondary Ethernet Access Ports and Secondary Ethernet VLAN Trunk Ports.
- Fault Tolerant Resilient Mode enables an AP to continue bridging traffic when the connection to the CAPWAP controller is lost. Both mesh and non-mesh root APs continue to bridge traffic. A child mesh AP (MAP) maintains its link to a parent AP and continues to bridge traffic till the parent link is lost. A child mesh AP cannot establish a new parent or child link till it reconnects to the CAPWAP controller. Existing wireless clients on the locally switching WLAN can stay connected with their AP in this mode. Their traffic will continue to flow through the Mesh and wired network. No new or disconnected wireless client can associate to the Mesh AP in this mode.
- You can configure a separate set of security ACLs for each VLAN that is configured for an Ethernet root port. In a mesh network, only root APs (RAPs) have an Ethernet root port.
- VLAN transparent bridging is not supported on Flex+Bridge mode. You must enter a set of allowed VLAN IDs for each secondary Ethernet trunk port.
- Path Control Protocol to create or delete path instances is supported on the Flex+Bridge mode.
- In a mesh network, a child mesh AP (MAP) inherits local WLAN/VLAN ID bindings, for bridged WLANs, and local secondary Ethernet access port/VLAN ID bindings. The bindings are inherited from the root AP (RAP) via path control messages. Bindings are required in a multi-hop mesh links to support FlexConnect capabilities in Mesh APs.

Note 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.

Restrictions on Flex+Bridge Mode

- An AP needs to be restarted, with a different bridging sub system, after bridge mode is changed.
- The FlexConnect and mesh modes are incompatible. A child mesh AP can only attach to another mesh AP; a child mesh AP cannot attach to a FlexConnect AP.
- A FlexConnect WLAN cannot be configured on a mesh AP.
- From 8.0 release onwards, Flex+Bridge mode allows the FlexConnect functionality across mesh APs. Flex+Bridge mode is used to enable FlexConnect capabilities on Mesh (Bridge mode) APs. Mesh APs inherit VLANs from the root AP that it is connected to it.
- You can enable or disable the VLAN trunking and configure a native VLAN ID, on each AP, for any of the following modes:
  - FlexConnect
  - Flex+Bridge (FlexConnect+Mesh)
- For the Flex+Bridge mode, control plane supports:
  - Connected (CAPWAP connected, controller is reachable.)
  - Standalone (CAPWAP disconnected, controller is not reachable.)
- For the Flex+Bridge mode, data plane supports:
  - Centralized (split MAC) - Data traffic via controller
  - Local (local MAC) - Data traffic by local switching from Root AP
- Starting in Release 8.8, ARP caching is not supported in APs operating in Flex+Bridge mode. For more information, see https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvm83632.
- A maximum of eight mesh hops are supported when operating in Flex+Bridge mode. The maximum number of Mesh APs per Root AP is 32.
- IRCM is not supported in FlexConnect+Bridge mode.
- Cisco TrustSec is not supported in Cisco Wave 2 APs that are in Flex+Bridge mode.
- Starting in Release 8.8, ARP caching is not supported in APs operating in Flex+Bridge mode. For more information, see https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvm83632.

For more information about Flex+Bridge, see the *Mesh Deployment Modes* chapter in the Mesh Deployment Guide.

Configuring Flex+Bridge Mode (GUI)

Procedure

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

Step 2 Click an AP name from the list of AP names and then click the **General** tab.

Step 3 From the AP mode drop-down list, choose **Flex+Bridge** mode.

Step 4 From the AP Sub mode drop-down list, choose none.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Step 7 Resilient mode is enabled by default. To disable the resilient mode, click the **FlexConnect** tab and uncheck the **Resilient Mode (Standalone mode support)** check-box.

Step 8 To push the root AP or FlexConnect WLAN to VLAN mapping to the other mesh APs, check the **Install mapping on radio backhaul** check box.

In a Flex+Bridge deployment, after you enable Backhaul Client Access globally, for the 5-GHz radios to beacon as expected, you must enable the **Install mapping on radio backhaul** option for the root APs operating in Flex+Bridge mode.

To enable Backhaul Client Access globally on the controller GUI, choose **Wireless** > **Mesh** to navigate to the **Mesh** page and then check the **Backhaul Client Access** check box.

Related Topics

Configuring Backhaul Client Access (GUI), on page 734

Configuring Flex+Bridge Mode (CLI)

Procedure

Step 1 Configure the Flex+Bridge mode by entering this command:

config ap mode flex+bridge

Step 2 Configure the Flex+Bridge sub mode by entering this command:

config ap mode flex+bridge submode

Step 3 Configure no sub mode by entering this command:

config ap mode flex+bridge submode none

Step 4 Enable or disable resilient Flex + Bridge mode by entering this command:

config ap flexconnect bridge resilient *ap-name* {**enable** | **disable**}

Step 5 Enable WLAN to VLAN mapping between the root APs and mesh APs by entering this command:

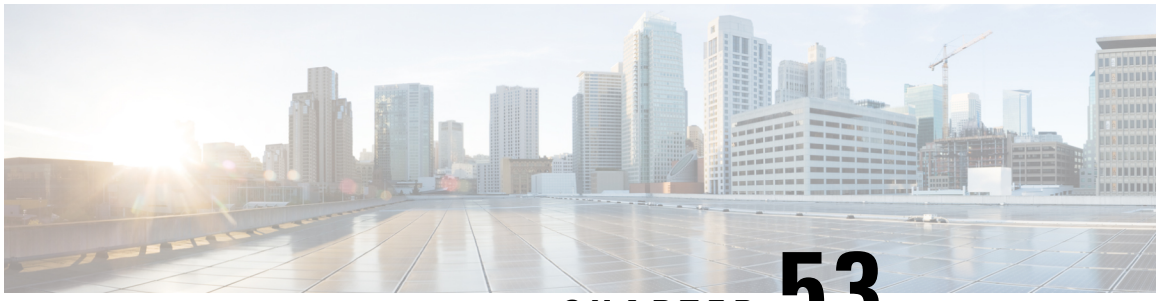
config ap flexconnect bridge backhaul-wlan *ap-name* {**enable** | **disable**}

Note
In a Flex+Bridge deployment, after you enable Backhaul Client Access globally, for the 5-GHz radios to beacon as expected, you must enable the **config ap flexconnect bridge backhaul-wlan** option for the root AP.

To enable Backhaul Client Access globally, enter this command: **config mesh client-access enable**

Related Topics

Configuring Backhaul Client Access (CLI), on page 734



CHAPTER 53

FlexConnect Groups

- Information About FlexConnect Groups, on page 1183
- Restrictions for FlexConnect Groups, on page 1189
- Configuring FlexConnect Groups (GUI), on page 1189
- Configuring FlexConnect Groups (CLI), on page 1193
- Moving APs from a Default FlexConnect Group to Another FlexConnect Group (GUI), on page 1195
- Viewing APs in a Default FlexGroup (GUI), on page 1196
- Viewing Default FlexGroup Details (CLI), on page 1196
- VLAN-ACL Mapping, on page 1199
- WLAN-VLAN Mapping, on page 1200
- OfficeExtend Access Points, on page 1202
- FlexConnect AP Image Upgrades, on page 1213
- FlexConnect AP Easy Admin, on page 1215
- WeChat Client Authentication, on page 1216
- Lawful Interception of Traffic, on page 1220

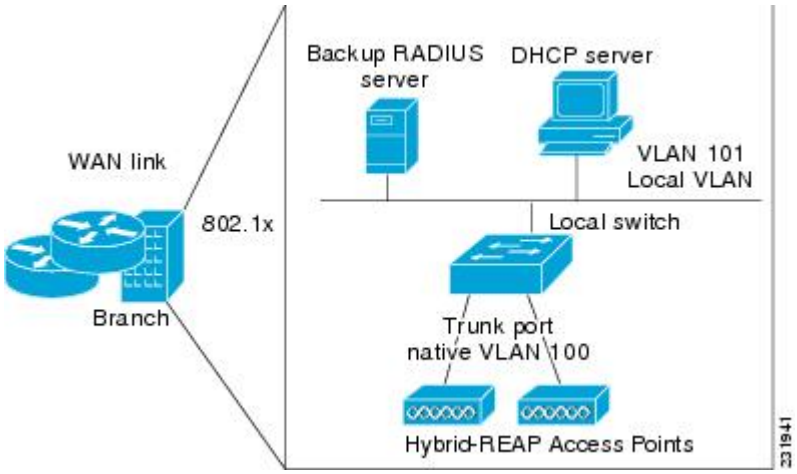
Information About FlexConnect Groups

To organize and manage your FlexConnect access points, you can create FlexConnect Groups and assign specific access points to them.

All of the FlexConnect APs in a group can share the same backup RADIUS server, fast secure roaming, local authentication configuration, and WLAN-VLAN mapping information. We recommend this feature if you have multiple FlexConnect APs 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 group rather than having to configure the same server on each AP. A maximum of 100 APs is supported per FlexConnect group (other than the default FlexConnect group, which is limited only by the maximum APs supported by the controller).

Figure 80: FlexConnect Group Deployment

The following figure shows a typical FlexConnect deployment with a backup RADIUS server in the branch office.



FlexConnect Groups and VLAN Support

You can configure VLAN Support and VLAN ID on a per FlexConnect group basis. This allows all APs in a FlexConnect group to inherit the VLAN configuration from the FlexConnect group including VLAN support, Native VLAN, and WLAN-VLAN mappings.

Deployment Considerations

- When the override flag is set at the FlexConnect Group, modification of VLAN Support, Native VLAN ID, WLAN-VLAN mappings, and Inheritance-Level at the AP is not allowed.
- An Inheritance-Level configuration is available at the FlexConnect AP. You have to set this to “Make VLAN AP Specific” to configure any AP-Specific VLAN Support, Native VLAN ID and VLAN-WLAN mappings on the AP. Note that you can modify this only when the override flag at the group is disabled.

  To achieve this on the controller GUI, choose **Wireless** > **All APs**, click on the AP name. In the FlexConnect tab, select **Make VLAN AP Specific** from the drop-down list.

IP-MAC Context Distribution for FlexConnect Local Switching Clients

Using this feature, you can prevent IP theft and ARP spoofing within the same FlexConnect group. The controller distributes the client IP:MAC context to all the APs in the same FlexConnect group. When the client roams to a new AP in the same FlexConnect group, the AP uses the IP:MAC context to validate the client data.

The Client IP-MAC context consists of the following parameter values:

- Source AP MAC Address to which a client is associated with
- Client’s MAC Address
- Client’s IPv4 Address
- Client’s IPv6 address count

- List of IPv6 addresses based on count

This section contains the following subsections:

Guidelines and Restrictions for IP-MAC Context Distribution for FlexConnect Local Switching Clients

- A maximum of 2000 client IP-MAC entries are supported in an AP.
- IP-MAC entries are deleted when the AP is rebooted.
- Clients behind NAT/PAT-enabled WLANs cannot use this IP:MAC binding as the controller reports and de-authenticates clients with duplicated IP address.
- AP evaluates IP-MAC context only for clients with IPv4 addresses, although distribution is done for both IPv4 and IPv6 addresses.
- This feature is not applicable to the default Flex Group.
- This feature does not support centrally switched clients as IP-Source guard is done at the controller data path.

Configuring IP-MAC Context Distribution For FlexConnect Local Switching Clients (GUI)

Procedure

Step 1 Choose **WLANs** > **WLANs** to open the **WLANs** page.
Step 2 Click the WLAN id you want to configure.
Step 3 Click the **Advanced** tab
Step 4 Under the **DHCP** section, check the **DHCP Addr. Assignment** check box.
Step 5 Under the **FlexConnect** section, check the **FlexConnect Local Switching** check box.
Step 6 Save the configuration.

Related Topics

Configuring the Controller for FlexConnect (GUI), on page 1163

Configuring IP-MAC Context Distribution For FlexConnect Local Switching Clients (CLI)

Procedure

- Configure the DHCP server on a WLAN by entering this command:

  config wlan dhcp_server *wlan-id ip_addr* **required**

- Configure the FlexConnect local switching on a WLAN by entering this command:

  config wlan flexconnect local-switching *wlan-id* **enable**

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 Fast Secure Roaming

Fast secure roaming among FlexConnect APs is supported only if the APs are in non-default FlexConnect groups. For OKC, fast roaming is supported between APs in different FlexConnect groups (because key caching is handled by the controller). For 802.11r and CCKM, fast roaming is supported only among APs in the same FlexConnect group. Sticky key caching is not supported with FlexConnect APs.

Note Fast roaming among FlexConnect and non-FlexConnect APs is not supported.

Note FlexConnect Groups is needed for fast roaming to work. Flex group needs to be created for fast roaming, 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/fast roaming. The group can be different for OKC as final check is done at the controller.

FlexConnect Groups and Local Authentication Server

You can configure the controller to allow a Cisco Wave 1 (IOS-based) FlexConnect AP 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.

Note This feature is not supported on Wave 2 and 802.11ax APs.

Note If you want to enable FlexConnect local authentication, you have to enable **FlexConnect AP Local Authentication** in the **Local Authentication** tab.

If the FlexConnect APs act as an 802.11X authenticator (RADIUS client), then configure the RADIUS servers in the **General** tab.

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 controller model, see the data sheet of the respective controller model.

Default FlexGroup

Default FlexGroup is a container where FlexConnect access points (APs), which are not a part of an administrator-configured FlexConnect group, are added automatically when they join the Cisco Wireless Controller. The Default FlexGroup is created and stored when the controller comes up (after upgrading from an earlier release. Note that a reload of the 8.3 will not create the group again. It will only restore the existing Default FlexGroup configuration.) This group cannot be deleted or added manually. Also, you cannot manually add or delete APs to the Default FlexGroup. The APs in the Default FlexGroup inherit the common configuration of the group. Any change in the group configuration is propagated to all the APs in the group.

When a group created by an admin is deleted, all the APs from that group are moved to the Default FlexGroup and inherit the configuration of this group. Similarly, APs that are removed manually from other groups are also added to the Default FlexGroup.

When an AP from the Default FlexGroup is added to a customized group, the existing configuration (from the Default FlexGroup) is deleted and the configuration from the customized group is pushed to the AP. If there is a standby controller, the Default FlexGroup and its configuration are also synchronized to it.

The AP provides FlexConnect group name during the join process. The AP could have received this group name either through cloud provisioning or through controller configuration. There are various scenarios involved in deciding the final FlexConnect group, when an AP joins and they are listed in the table below:

FlexConnect Group Received from AP	Status in Controller	Final Group Information/Configuration Setn to AP	Type of Entry (Based on Priority)
Group1	Group1 not present; AP entry not present in any group	Default FlexGroup	Admin
Group1	Group1 present but maximum entries reached; AP entry not present in any group	Default FlexGroup	Admin
Group1	Group1 present, but AP entry not present in any group	Group1	Cloud
Group1	Group1 present, but AP entry present as part of a different group, Group2 (added by admin)	Group2	Admin
Group1	Group1 present, but AP entry exists in a different group, Group2 learnt earlier through cloud	Group1	Cloud
No Group/Default Group	AP entry exists as part of Group2 (either through admin configuration or learnt via cloud)	Group2	Admin/Cloud

Whenever the final type of entry is cloud, the AP entry gets added to the corresponding FlexConnect group. Also, when the FlexConnect group received from AP is different from the resultant group, a trap is raised to inform the admin about the conflict. The **show flexconnect group detail** *group-name* **aps** command displays the conflict value.

The following features are not supported in default Flex Group:

- Efficient image upgrade
- PMK cache distribution
- Fast Roaming

The following features are supported in default Flex Group:

- VLAN support (native VLAN, WLAN-VLAN mapping)
- VLAN ACL mapping
- WebAuth, web policy, local split mapping
- Local authentication users
- RADIUS authentication

- Central DHCP or NAT-PAT
- Flex AVC
- VLAN name ID mapping
- Multicast override

Restrictions

- You cannot use the following CLIs to add or delete a Defaut FlexGroup or AP to a group:
  - **config flexconnect group default-flexgroup** {**add** | **delete**}
  - **config flexconnect group default-flexgroup ap** {**add** | **delete**}
- The Defaut FlexGroup does not have a default configuration.
- When you delete an AP from the customized flex group, the VLAN support is also deleted from that AP.

Restrictions for FlexConnect Groups

- When an AP moves from one FlexConnect group to another, it retains the pmk-cache and the iPSK P2P Blocking Flex feature behavior. It will end only after the session times-out for the clients that are associated to the AP.
- 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.

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.

Procedure

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 (Optional) To configure the FlexConnect APs as local authentication (RADIUS) servers, configure the 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 (Optional) To configure the FlexConnect APs as local 802.1X authenticators (RADIUS clients), configure the FlexConnect Group as follows:

a) Under the **General** tab, check the **Enable AP Local Authentication** check box to enable local authentication for this FlexConnect Group. By default, it is unchecked.

b) Click **Apply**.

c) In the **AAA** section, enter the server IP address, server type primary, shared secret, and optionally port number.

d) Click **Add**.

e) (Optional) If you are using secondary RADIUS server, repeat these steps.

f) Click **Apply**.

Step 15 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 16 In the **Policies** tab, choose the appropriate IPv4 or IPv6 policy ACL and click **Add**.

Step 17 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 18 Click **Save Configuration**.

Step 19 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.

Related Topics

Applying FlexConnect Access Control Lists (GUI), on page 1234

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.

Procedure

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 (Optional) To configure the FlexConnect APs as local authentication (RADIUS) servers, configure the FlexConnect Group 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 (Optional) To configure the FlexConnect APs as local 802.1X authenticators (RADIUS clients), configure the FlexConnect Group as follows:

a) To enable or disable local authentication for this FlexConnect group, enter this command:

config flexconnect group *group_name* **radius ap** {**enable** | **disable**}

Step 6 Configure a Web Policy ACL on a FlexConnect group by entering this command:

config flexconnect group *group-name* **web-policy policy acl** {**add** | **delete**} *acl-name*

Step 7 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 8 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 9 Configure central DHCP per WLAN by entering this command:

config flexconnect group *group-name* **central-dhcp** *wlan-id* {**enable override dns** | **disable** | **delete**}

Step 10 Configure the DHCP overridden interface for FlexConnect group, use the **config flexconnect group flexgroup dhcp overridden-interface enable**command.

Step 11 Configure policy acl on FlexConnect group by entering this command:

config flexconnect group *group_name* **policy** [**ipv6**] **acl** {**add** | **delete**} *acl-name*

Step 12 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 13 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 14 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 15 Save your changes by entering this command:

save config

Step 16 See the current list of flexconnect groups by entering this command:

show flexconnect group summary

Step 17 See the details for a specific FlexConnect Groups by entering this command:

show flexconnect group detail *group_name*

Related Topics

Applying FlexConnect Access Control Lists (CLI), on page 1236

Moving APs from a Default FlexConnect Group to Another FlexConnect Group (GUI)

Procedure

Step 1 Choose **Wireless** > **FlexConnect Groups**. The **FlexConnect Groups** window is displayed.

Step 2 Click the **Group Name** link of a FlexConnect Group. The **FlexConnect Groups > Edit** window is displayed.

Step 3 Click **FlexConnect AP** link. The **FlexConnect Group AP List** window is displayed.

Step 4 To move an AP that is currently in Default FlexGroup, select the corresponding Group Name from the **New Group Name** drop-down list, after selecting the APs from the **FlexConnect APs** list.

Step 5 To add an AP to the new group, click **Move**.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Viewing APs in a Default FlexGroup (GUI)

Procedure

Step 1 Choose **Wireless > FlexConnect Groups**. The **FlexConnect Groups** window, which contains the following details, is displayed:

- **Group Name**—Number of FlexConnect groups that are configured.
- **Number of APs**—Number of APs in each FlexConnect group.

Step 2 Click a **Group Name**. The **FlexConnect Groups > Edit** window, which displays the FlexConnect Group details, is displayed.

Viewing Default FlexGroup Details (CLI)

Procedure

Step 1 **show flexconnect group detail default-flexgroup**

Displays the configuration of the Default FlexGroup and the APs that are a part of it.

Example:

```
(Cisco Controller) >show flexconnect group detail default-flex-group

Number of APs in Group: 1
AP Ethernet MAC Name Status Mode
-------------------- -------------------- --------------- ----------------
a8:9d:21:b2:26:88 APa89d.21b2.2688 Joined Flexconnect
Efficient AP Image Upgrade ..... Disabled
Master-AP-Mac Master-AP-Name Model Manual
Group Radius Servers Settings:
Type Server Address Port
------------ ---------------- -------
Primary Unconfigured Unconfigured
```

```
Secondary Unconfigured Unconfigured
Group Radius AP Settings:
AP RADIUS server..... Disabled
EAP-FAST Auth..... Disabled
LEAP Auth..... Disabled
EAP-TLS Auth..... Disabled
--More-- or (q)uit
EAP-TLS CERT Download..... Disabled
PEAP Auth..... Disabled
Server Key Auto Generated... No
Server Key..... <hidden>
Authority ID..... 436973636f00000000000000000000000
Authority Info..... Cisco A_ID
PAC Timeout..... 0
HTTP-Proxy Ip Address..... 0.0.0.0
HTTP-Proxy Port..... 0
Multicast on Overridden interface config: Disabled
DHCP Broadcast Overridden interface config: Disabled
Number of User's in Group: 0
FlexConnect Vlan-name to Id Template name: none
Group-Specific Vlan Config:
Vlan Mode..... Disabled
Override AP Config..... Disabled
Group-Specific FlexConnect Wlan-Vlan Mapping:
WLAN ID Vlan ID
-------- --------------------
WLAN ID SSID Central-Dhcp Dns-Override Nat-Pat
```

Step 2 **show ap config general** *ap-name*

Shows a FlexConnect AP's FlexConnect group membership.

Example:

```
(Cisco Controller) >show ap config general APa89d.21b2.2688

Cisco AP Identifier..... 0
Cisco AP Name..... APa89d.21b2.2688
Universal AP..... Yes
Universal AP Prime Status..... NDP
Country code..... US - United States
Regulatory Domain allowed by Country..... 802.11bg:-A 802.11a:-AB
AP Country code..... US - United States
AP Regulatory Domain..... 802.11bg:-A 802.11a:-A
Switch Port Number ..... 2
MAC Address..... a8:9d:21:b2:26:88
IP Address Configuration..... DHCP
IP Address..... 8.1.2.186
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 8.1.2.1
NAT External IP Address..... None
CAPWAP Path MTU..... 1485
DHCP Release Override..... Disabled
Telnet State..... Globally Disabled
Ssh State..... Globally Disabled
Cisco AP Location..... default location
Cisco AP Floor Label..... 0
Cisco AP Group Name..... default-group
Primary Cisco Switch Name.....
Primary Cisco Switch IP Address..... 8.1.2.2
Secondary Cisco Switch Name.....
Secondary Cisco Switch IP Address..... Not Configured
Tertiary Cisco Switch Name.....
Tertiary Cisco Switch IP Address..... Not Configured
Administrative State ..... ADMIN_ENABLED
```

```
Operation State ................................ REGISTERED
Mirroring Mode ................................. Disabled
AP Mode ........................................ FlexConnect
Public Safety .................................. Disabled
ATF Mode ....................................... Disable
AP SubMode ..................................... Not Configured
Rogue Detection ................................ Enabled
AP Vlan Trunking ............................... Disabled
Remote AP Debug ................................ Disabled
Logging trap severity level ..................... informational
Logging syslog facility ......................... kern
S/W Version ..................................... 8.3.15.64
Boot Version ................................... 15.2.4.0
Mini IOS Version ............................... 8.0.115.0
Stats Reporting Period ......................... 180
Stats Collection Mode .......................... normal
LED State....................................... Enabled
PoE Pre-Standard Switch......................... Disabled
PoE Power Injector MAC Addr..................... Disabled
Power Type/Mode................................. PoE/Full Power
Number Of Slots................................. 2

AP Model........................................ AIR-AP3702E-UXK9
AP Image........................................ C3700-K9W8-M
IOS Version..................................... 15.3(20160217:163330)$
Reset Button.................................... Enabled
AP Serial Number................................ FCW1905N1CX
AP Certificate Type............................. Manufacture Installed
AP LAG Configuration Status ..................... Disabled
LAG Support for AP ............................. No
Native Vlan Inheritance: ....................... AP
FlexConnect Vlan mode :......................... Disabled
FlexConnect Group............................... default-flex-group
Group VLAN ACL Mappings
Group VLAN Name to Id Mappings
AP-Specific FlexConnect Policy ACLs :
L2Acl Configuration ............................ Not Available
FlexConnect Local-Split ACLs :
WLAN ID PROFILE NAME ACL TYPE
------- ------------------------------ -------------------------------- -------
Flexconnect Central-Dhcp Values :
WLAN ID PROFILE NAME Central-Dhcp DNS Override Nat-Pat
Type
------- -------------------------------- -------------- -------------- ---------
------
FlexConnect Backup Auth Radius Servers :
Primary Radius Server........................... Disabled
Secondary Radius Server......................... Disabled
AP User Mode.................................... AUTOMATIC
AP User Name.................................... Cisco
AP Dot1x User Mode.............................. Not Configured
AP Dot1x User Name.............................. Not Configured
Cisco AP system logging host.................... 255.255.255.255
AP Up Time...................................... 0 days, 19 h 26 m 09 s
AP LWAPP Up Time................................ 0 days, 15 h 28 m 46 s
Join Date and Time.............................. Thu Feb 18 18:58:54 2016
Join Taken Time................................. 0 days, 00 h 07 m 02 s
GPS Present..................................... NO
Ethernet Vlan Tag............................... Disabled
Ethernet Port Duplex............................ Auto
Ethernet Port Speed............................. Auto
AP Link Latency................................. Disabled
Rogue Detection................................. Enabled
AP TCP MSS Adjust............................... Disabled
```

```
Hotspot Venue Group.............................. Unspecified
Hotspot Venue Type............................... Unspecified
DNS server IP ..................................... 255.255.255.255
```

Step 3 **show flexconnect group detail** *groupname* **aps**

Displays the APs that are part of a specific group.

Example:

```
(Cisco Controller) >show flexconnect group detail default-flex-group aps

Number of APs in Group: 1
AP Ethernet MAC Name Status Mode
------------------- -------------------- --------------- ----------------
a8:9d:21:b2:26:88 APa89d.21b2.2688 Joined Flexconnect
```

VLAN-ACL Mapping

Configuring VLAN-ACL Mapping on FlexConnect Groups (GUI)

Procedure

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.

WLAN-VLAN Mapping

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.

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

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 Select the **VLAN Support** check box and specify the **Native VLAN ID**.

Step 6 Select the **Override Native VLAN on AP** check box.

- Overrides the VLAN Support and Native VLAN ID previously configured on the access points
- Changes the inheritance level at the AP to "Group Specific"
- Removes AP-specific WLAN-VLAN VLAN-ACL mappings
- Pushes the group-specific configuration including WLAN-VLAN mapping configured on the group to all the APs in the group.

Step 7 To verify that the inheritance level is Group Specific:

a) Choose **Wireless** > **Access Points** > **All APs** and click the name of the AP.
b) In the FlexConnect tab, view the **Inheritance Level** field.
c) Click **VLAN Mappings** to view the details of WLAN-VLAN mappings.

Step 8 Click **Apply**.

Step 9 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.

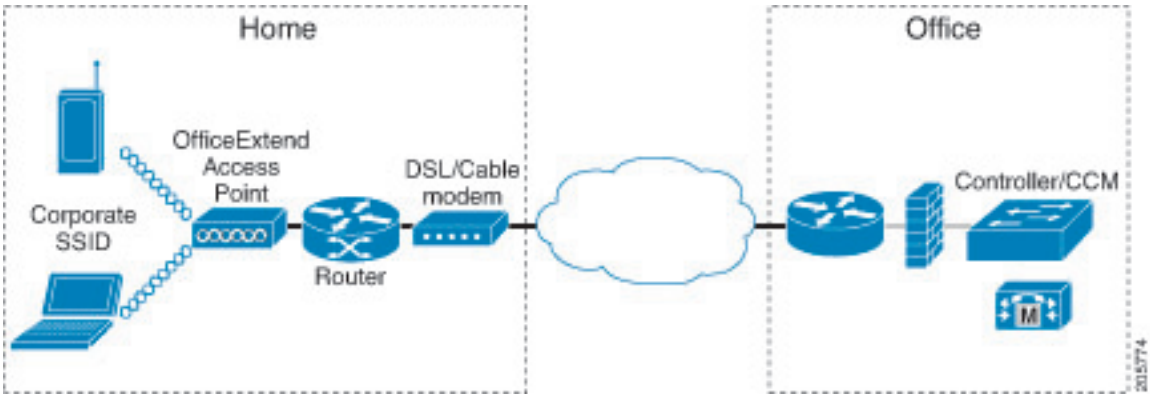
OfficeExtend Access Points

A Cisco OfficeExtend access point (Cisco OEAP) provides secure communications from a controller 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 81: 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. In Release 8.5, only one OEAP is supported behind a NAT device, but in Release 8.10, multiple OEAPs are supported 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.

Additional References

- See the Release Notes for information about supported Cisco OEAPs.

- https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/215928-flexconnect-oeap-with-split-tunneling-co.html

Implementing Security

Note The LSC configuration is optional.

1. (Optional) Use local significant certificates (LSCs) to authorize your OfficeExtend access points, by following the instructions in the "Authorizing Access Points Using LSCs" sectionn.
2. (Optional) 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

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)

Procedure

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 feature is supported on all internal antenna AP models.

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 controller 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.

- Enable split tunneling without gateway override by entering this command:

  config wlan split-tunnel *wlan-id* **enabled apply-acl** *acl name*

- Enable split tunneling with gateway override by entering this command:

  config wlan split-tunnel *wlan-id* **enabled override gateway** *gateway ip* **mask** *subnet mask* **apply-acl** *acl name*

- 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 a Personal SSID on an OfficeExtend Access Point

Procedure

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.

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. For more information, see https://www.cisco.com/c/dam/m/zh_cn/solutions/enterprise-networks/mobility-express/office-extend/office-extend-deployment-guide.pdf.

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.

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*}

Viewing Voice Metrics on OfficeExtend Access Points

Use this command to view information about voice metrics on the OfficeExtend access points in your network:

show ap stats 802.11{a | b} *Cisco_AP*

Information similar to the following appears:

```
OEAP WMM Stats :
  Best Effort:
    Tx Frame Count.............................. 0
    Tx Failed Frame Count....................... 0
    Tx Expired Count............................ 0
    Tx Overflow Count........................... 0
    Tx Queue Count.............................. 0
    Tx Queue Max Count.......................... 0
    Rx Frame Count.............................. 0
    Rx Failed Frame Count....................... 0
  Background:
    Tx Frame Count.............................. 0
    Tx Failed Frame Count....................... 0
    Tx Expired Count............................ 0
    Tx Overflow Count........................... 0
    Tx Queue Count.............................. 0
    Tx Queue Max Count.......................... 0
    Rx Frame Count.............................. 0
    Rx Failed Frame Count....................... 0
  Video:
    Tx Frame Count.............................. 0
    Tx Failed Frame Count....................... 0
    Tx Expired Count............................ 0
    Tx Overflow Count........................... 0
    Tx Queue Count.............................. 0
    Tx Queue Max Count.......................... 0
    Rx Frame Count.............................. 0
    Rx Failed Frame Count....................... 0
  Voice:
    Tx Frame Count.............................. 0
    Tx Failed Frame Count....................... 0
    Tx Expired Count............................ 0
    Tx Overflow Count........................... 0
    Tx Queue Count.............................. 0
    Tx Queue Max Count.......................... 0
    Rx Frame Count.............................. 0
    Rx Failed Frame Count....................... 0
```

View the voice metrics on the OfficeExtend access points in your network using the controller GUI as follows:

- 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.
- Hover your cursor over the blue drop-down arrow for the desired access point and click the **Detail** link for the desired client to open the Radio > Statistics page.

  This page shows the **OEAP WMM counters** for this access point.

Network Diagnostics

Network Diagnostics determines the non-DTLS throughput of the system by running a speed test on demand. Network Diagnostics allows troubleshooting of root causes leading to failures. It also determines the link latency and jitter by running a test on demand or periodically.

This section contains the following subsections:

Running Network Diagnostics (GUI)

Procedure

Step 1 Choose **WAN** > **Network Diagnostics**.
The Network Diagnostics page is displayed.

Step 2 Click **Start Diagnostics**.
The diagnostics page is displayed.

Running Network Diagnostics on the Controller

Procedure

Step 1 Choose **Wireless** > **All APs** > **Details**.

Step 2 Choose the **Network Diagnostics** tab.
The Network Diagnostics page is displayed.

Step 3 Click **Start Network Diagnostics**.
The diagnostics page is displayed.

Running Network Diagnostics (CLI)

Procedure

- To run network diagnostics, enter this command on the controller:
  show ap network-diagnostics *ap-name*

Remote LANs

This section describes how to configure remote LANs.

Prerequisites

Guidelines and Restrictions

- It is not possible to configure 802.1X on remote LANs through the controller GUI; configuration only through CLI is supported.
- Starting in Release 8.8, remote LAN clients can pass traffic in CPU switching and hardware switching mode. Prior to Release 8.8, remote LAN clients could pass traffic only in CPU switching mode and local switched remote LAN.

This section contains the following subsections:

Configuring a Remote LAN (GUI)

Procedure

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*

- Configure the local switching of client data associated to flexconnect by entering this command:
  config remote-lan flexconnect local-switching *remote-lan-id* **vlan** *vlan-id*

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.

Related Topics

Predownloading an Image to an Access Point, on page 85
Access Point Predownload Process, on page 86

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 reachable between these access points and firewall must not be deployed.

- 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 CAPWAP over IPv6.
- 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)

Procedure

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.

FlexConnect AP Easy Admin

The FlexConnect AP Easy Admin enables unified AP GUI access and configure the following parameters to connect to the controller:

- AP IP address: Static or DHCP IP address.
- Controller IP address priming: Ablity to configure the primary, secondary, and tertiary controller, and their IP addresses.
- CAPWAP preferred DNS configuration.
- PPPoE: Enabling of FlexConnect submode and configuring the username and password for PPPoE server authentication.
- TFTP: AP image upgrade through TFTP.

Configuring FlexConnect AP Easy Admin on the Controller (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration**.

The **Global Configuration** page is displayed.

Step 2 In the **AP Easy Configuration** section, check the **Enable Global AP Easy Configuration** check box.

Note

Easy Configuration is only applicable to the following Cisco Wave 1 (IOS-based) APs: 702, 1530, 1700, 2700, and 3700.

Step 3 Click **Apply**.

Configuring FlexConnect AP Easy Admin on the Controller (CLI)

Procedure

Step 1 Enable or disable AP Easy Admin on the controller by entering this command:

config network ap-easyadmin {**enable** | **disable**}

Step 2 View the network summary and to verify the status of AP easy admin feature by entering this command:

show network summary

WeChat Client Authentication

The WeChat messaging service is a cross platform communication software which supports text messages, audio calls, video calls, games. WeChat also offers full fledged m-commerce capabilities in their app using which you can do purchases, make bill payments within the WeChat app. This app has a large customer base in China and is gaining popularity in rest of the world. This feature gives WeChat users access to wireless internet service using their smartphones or PC. The authentication of the account is done by the WeChat servers. This is a simple process and requires little user inputs.

This platform benefits both, the customer and the merchant. The customer gets access to the Internet and the merchant gets a customer engaging platform to advertise merchandise and services.

Restrictions on WeChat Client Authentication

- This feature is supported on Cisco Wave 1 APs in FlexConnect mode only.
- Downgrading a controller running a release with QR-Scan or WeChat specific configuration to an older release which does not support this feature leads to XML validation errors for the Layer 3 security type during the downgrade process.

  The errors do not have any impact on the functioning of the controller.

Configuring WeChat Client Authentication on Controller (GUI)

Before you begin

The AP SSID and the controller MAC address needs be configured in the Baitone server database.

Procedure

Step 1 Log in to the controller GUI interface.

Step 2 Choose **WLANs** > **WLAN ID** > **Security** to open the WLANs Edit page.

Step 3 In the **Security** tab, configure the following parameters:

a) Set the Layer 2 Security to **None** from the drop-down list on the Layer 2 tab.
b) Set the Layer 3 Security to **Web Policy** from the drop-down list on the Layer 3 tab.
c) Choose **Passthrough**
d) Select the **Qr Code Scanning** check box.
e) Enter the portal web page address in the **`Redirect URL`** text box and **`Shared Key`** (Preconfigured on the external authentication server).
f) From the **Preauthentication ACL** > **WebAuth FlexAcl** drop-down list, choose the Acl option that you want to apply to the WLAN.

   Before the client is authenticated, this Acl allows the authentication traffic to pass through to the WeChat authentication servers.

Step 4 In the **Advanced** tab, select the **FlexConnect Local Switching** check box.

Step 5 (Optional) Enable local authentication by configuring the following parameters:

a) Under the **Security** tab, select the **Web policy done locally on AP** check box.

   This enables local authentication at the AP and the central authentication at the controller is disabled.

b) In the **Advanced** tab, select the **FlexConnect Local Auth** check box.

   Set this option to enable if **Web policy done locally on AP** is enabled

Step 6 On the **Wireless** tab, follow the steps:

a) Select the **FlexConnect ACLs**.

   Choose an existing Acl or create a new Acl

b) Add the **`portal page IP address`** and the **`WeChat authentication server IP address`** with permit action as new rules.

Step 7 In the **Wireless** > **Global Configuration** page, configure the following parameter:

a) Enter the virtual IP address in the **AP Virtual IP address** text box.

   The default Virtual AP IP address is: 10.1.0.6. The controller and the client interact with the AP using this AP virtual IP address.

Step 8 Choose **Security** > **Web Auth** > **Web Login Page**. Enter the values for:

a) **QrCode Scanning Bypass Timer**. The valid range is between 5 and 60 seconds to allow traffic temporary.
b) **QrCode Scanning Bypass Count**. The valid range is between 1 to 9 retries to bypass for authentication.

Configuring WeChat Client Authentication on Controller (CLI)

Before you begin

The AP SSID and the controller MAC address needs be configured in the external authentication server database.

Procedure

Step 1 Configure the WLAN:

a) Create a WLAN, by entering this command:

config wlan create *wlan-id profile-name ssid-name*

b) Disable L2 security by entering this command:

config wlan security wpa disable *wlan-id*

c) Enable WLAN L3 passthrough by entering this command:

config wlan security web-passthroughenable *wlan-id*

Step 2 Enable FlexConnect mode in a Cisco AP by entering this command:

config ap mode flexconnect *Cisco-AP*

Step 3 Enable or disable QR code scanning support for clients on the controller by entering this command:

config wlan security web-passthrough qr-scan {**enable | disable**} *wlan-id*

Step 4 Configure the QR-scan DES key for the WLAN by entering this command:

config wlan security web-auth *des key string wlan-id*

Step 5 Configure the QR scan authentication options - timer, and count by entering this command:

config custom-web qrscan-bypass-opt *timer count*

Step 6 Configure the external Web Authentication URL by entering this command:

config custom-web ext-webauth-url *ext-webauth-url*

Step 7 Configure flex-acl and attach to WLAN in L3 security

Step 8 Configure virtual IP of Controller with the same IP which is configured on Baitone

Step 9 Enable or disable QR code scanning support for clients on the controller:

- Enable or disable central authentication QR code scanning support for clients on the controller by entering this command:

  config wlan security web-passthrough qr-scan{**enable | disable**} *wlan-id*

- Enable or disable local authentication QR code scanning support for clients on the controller by entering this command:

  config wlan security web-passthrough qr-scan local{**enable | disable**} *wlan-id*

Step 10 Configure virtual IP for an AP by entering this command:

config ap virtual_ip {**enable | disable**} *ip address*

Step 11 See the state of WeChat QR scan feature for specific WLAN by entering this command:

show wlan *wlan-id*

Step 12 See the QR scan bypass options by entering this command:

show custom-web all

Authenticating Client Using WeChat App for Mobile Internet Access (GUI)

Before you begin

The WeChat App must be installed in the smartphone.

Procedure

Step 1 Connect the smartphone to the WeChat enabled SSID.

a) IPhone—Opens the portal page automatically.
b) Android—Open a URL using a browser which will redirect to the portal page.

Once connected to the SSID, you have 60 seconds to validate the WeChat account.

Step 2 Click the green button displayed to validate the WeChat account.

Step 3 Click the green connect button to connect to WeChat over Wi-Fi.

The merchant page is displayed which confirms the user is connected to the Internet.

Authenticating Client Using WeChat App for PC Internet Access (GUI)

Before you begin

The customer's mobile must have the WeChat app installed and have access to the Internet to authenticate the WeChat account.

Procedure

Step 1 Connect the PC to the WeChat enabled SSID.

The server identifies the client and displays the portal web page with a QR code.

Step 2 Scan the QR code using the WeChat app on the mobile.
The WeChat account authentication success is displayed.

Step 3 The PC browser displays the merchant page and is able to access the Internet.

Lawful Interception of Traffic

Using the Cisco wireless solution, it is possible to lawfully intercept traffic for monitoring purposes.

Cisco APs create syslog records for traffic and send the records to the controller. Traffic from both IPv4 and IPv6 protocols is recorded. The controller at configured intervals sends these syslog records to the syslog server.

Note The Cisco controller does not store any traffic interception related records.

Restrictions on Lawful Interception of Traffic

- To support IPv6 protocol, enable IPv6 on the controller
- This feature is supported only in Cisco Wave 2 APs operating in Flex + Bridge mode.

Configuring Lawful Interception of Traffic on a Cisco Controller (CLI)

Procedure

- Configure lawful interception by entering this command:

  config flexconnect lawful-intercept {**enable | disable**}
- Configure the syslog for IPv4 and IPv6 host by entering this command:

  config flexconnect lawful-intercept syslog host global {*ipv4 addr* | *ipv6 addr*}
- Configure the time interval for the syslog to be sent to the syslog server by entering this command:

  config flexconnect lawful-intercept timer *timer-value*
- See the lawful interception summary by entering this command:

  show flexconnect lawful-interception summary

Viewing and Debugging Lawful Interception of Traffic on a Cisco Access Point (CLI)

Procedure

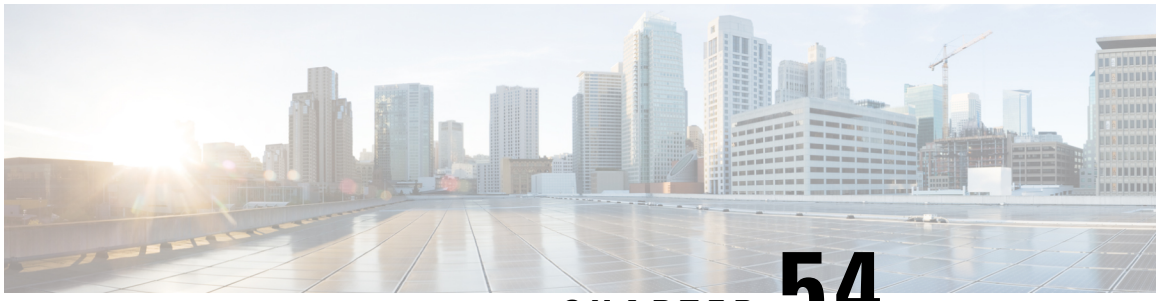
- See the lawful interception summary by entering this command:

  show flexconnect lawful-interception summary
- Debug lawful intercept by entering this command:

debug lawful-intercept flows {all | mac-addr {**all** | *mac-addr*}}

- Debug lawful-intercept syslog by entering this command:

  debug lawful-intercept syslog



CHAPTER 54

FlexConnect Security

- FlexConnect Access Control Lists, on page 1223
- Authentication, Authorization, Accounting Overrides, on page 1230
- Software Defined Access and FlexConnect Post Authentication IPv6 ACL Support, on page 1234

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.
  - You can define up to 20 URL domain based rules (or filters).
- 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.
- 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.
- Cisco Wave 2 and 802.11ax APs: When FlexConnect ACLs are applied to both wired and 802.11 interfaces, the client traffic honors only the ACL that is mapped to the 802.11 interface and not the ACL that is mapped to the wired interface.

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)

Procedure

Step 1 Choose **Security** > **Access Control Lists** > **FlexConnect Access Control Lists** > **IPv4 ACL/IPv6 ACL**.

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, hover over **Add Rule**, and select one of the two options:

- **IP Rule**—IP address based rule. A controller supports 512 ACLs with 64 rules in each ACL.
- **URL Rule**—Domain name-based rule. A controller supports 512 ACLs with 20 rules in each ACL.

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.

Step 7 Configure a URL domain-based rule for a given FlexConnect ACL:

a) Choose **URL Rule** to create a URL domain-based rule.

The **Access Control Lists** > **URL Rules** > **New** page is displayed.

b) The controller supports up to 20 rules for each ACL. These rules are listed in order from 1 to 20. In the **Sequence** field, enter a value (between 1 and 20) 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 19, 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) In the **URL** field, enter the Fully Qualified Domain Name (FQDN).

The URL domain name should be given in a valid format, for example, Cisco.com.

d) 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**.

e) Click **Apply**.

The **Access Control Lists > Edit** page is displayed on which the rules for this ACL are shown.

f) Repeat this procedure to add more rules, if required, for this ACL.

Step 8 Configure Local Web Authentication for FlexConnect:

a) Choose **WLANs** > **WLAN ID** > **Security**, select **Layer 3**.

b) From the **Preauthentication ACL** > **WebAuth FlexAcl** drop-down list, choose the ACL option that you want to apply to the WLAN.

Step 9 Configure Central Web Authentication for FlexConnect:

a) Choose **Wireless** > **FlexConnect Groups**.

The **FlexConnect Groups** page appears.

b) Click the **Group Name** link of the FlexConnect Group for which you want to configure Central Web Authentication.

c) Click the **ACL Mapping** > **Policies** tab.

d) Select the policy from the **Policy ACL** from the drop-down list.

e) Click **Add**.

f) Choose **WLANs** > **WLAN ID** > **Security**, to open the WLANs Edit page.

g) In the **Security** tab, configure the following parameters:

- Check the **MAC Filtering** check box in the **Layer 2 Security** tab.
- Set Layer 3 Security to **None** from the drop-down list in the **Layer 3** tab.

h) In the **Advanced** tab, configure the following parameters.

- Check the **Allow AAA Override** check box to enable AAA override.
- Choose **ISE NAC** from the **NAC State** drop-down list.

i) Save the configuration.

Related Topics

Configuring Access Control Lists (GUI), on page 249

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 [**ipv6**] **acl** {**create | delete** } *name*

  The IPv4 ACL name of up to 32 characters is supported.

  The [**ipv6**] option is introduced in Release 8.8. Post-authentication IPv6 ACL is supported for both central and local authentication of FlexConnect WLANs. This ACL will be applied to client when the client moves to *Run* state.

- 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 [**ipv6**] **acl rule add** *acl-name rule-index*

  b) Configure a rule's source IP address and netmask by entering this command:

     config flexconnect [**ipv6**] **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 [**ipv6**] **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*

     IPv6—**config flexconnect ipv6 acl rule destination address** *acl-name rule-index ipv6-addr prefix-len*

  e) Configure a rule's destination port range by entering this command:

     config flexconnect [**ipv6**] **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 [**ipv6**] **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 flexconnect [**ipv6**]**acl 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 [**ipv6**] **acl rule actionacl-name** *rule-index* **{permit |deny}**

i) Change the index value for an ACL rule by entering this command:

config flexconnect [**ipv6**]**acl rule change index** *acl-name old-index new-index*

j) Swap the index values between two rules by entering this command:

config flexconnect [**ipv6**] **acl rule swap** *acl-name index-1 index-2*

k) Delete a rule from the FlexConnect ACL by entering this command:

config flexconnect [**ipv6**] **acl rule delete** *name*

l) Apply an ACL to the FlexConnect access point by entering this command:

config flexconnect [**ipv6**] **acl apply** *acl-name*

- Configure a URL domain-based rule for an ACL.
  a) Add or delete a URL domain to an ACL by entering this command:

  config flexconnect [**ipv6**] **acl url-domain** { **add | delete** } *acl-name index*

  b) Add or edit the URL in a rule of a FlexConnect ACL by entering this command:

  config flexconnect [**ipv6**] **acl url-domain url** *acl-name index url-name*

  Enter the Fully Qualified Domain Name (FQDN).

  c) Set the permit or deny action to all the URLs in the FlexConnect ACL by entering this command:

  config flexconnect [**ipv6**] **acl url-domain action** *acl-name index* {**permit | deny** }

  Default action is to **deny**.

- [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*

Related Topics

Configuring Access Control List Rules (CLI), on page 277

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.

Configuring CAPWAP Message Aggregation (CLI)

Deployments with large number of FlexConnect APs should have CAPWAP message aggregation enabled. In such deployments, if CAPWAP message aggregation is disabled, the ACL and AVC settings on APs are found missing. At the time when the AP settings are missing, messages similar to the following are displayed in the controller message log:

```
Capwap Retransmission Queue Full for AP 38:ed:18:cd:f0:60
```

With the **debug capwap errors enable** in effect, errors similar to the following might be observed:

```
*spamReceiveTask: Aug 22 22:21:09.342: [PA] 00:11:0a:04:60:4d Unable to
get RadId. Sending of PMK cache entry to all APs in flexconnect group
failed :: bssid 00:00:00:00:00:00

*spamApTask1: Aug 22 22:21:43.809: [PA] 38:ed:18:cd:f0:60 Queue already
full

*spamApTask1: Aug 22 22:21:43.809: [PA] 38:ed:18:cd:f0:60 Failed to send
[XXX] payload
```

This issue is observed especially in the following conditions:

- FlexConnect ACLs and/or AVC in use
- A large number of WLANs in use

Workaround is to enter the command described below.

Procedure

- Enable CAPWAP message aggregation by entering this command:

  config advanced capwap-message-aggregation enable

Note In Release 8.5 and earlier releases, the default setting for this command is disabled. In Release 8.6 and later releases, the default setting is enabled.

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.

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 52: 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.
- On virtual controller platforms, per-client downstream rate limiting is not supported in FlexConnect central switching.
- 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 and later releases, in anchor-foreign scenarios with Cisco Wave 2 and 802.11ax APs, all of 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.
- The AAA ACLs and VLAN ACLs are applied on the client in the following order of precedence:
  - Wave 1 APs: Both the ACLs are active simultaneously on the client.
  - Wave 2 APs: AAA ACLs override the VLAN ACLs on the client.
- 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)

Procedure

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*

Software Defined Access and FlexConnect Post Authentication IPv6 ACL Support

This feature enables support for IPv6 ACLs in Fabric mode, central and local FlexConnect authentication on controllers. These ACLs support clients when they are in run or forwarding state.

If you have a WLAN that has Fabric mode in enabled state and configured for post-authentication IPv6 ACLs and AAA override is not enabled, the IPv6 ACL is applied to clients that associate with the WLAN. The clients that are served by APs within the same FlexConnect group remain governed by the applicable ACL. The allowed traffic is locally switched, denied traffic is dropped at the AP.

Restrictions on Software Defined Access and FlexConnect Post Authentication IPv6 ACL Support

Post-authentication DNS ACL for both IPv4 and IPv6 is not supported. However pre-authentication ACL is supported with 20 domain names per ACL.

Related Topics

Introduction to Software-Defined Access Wireless, on page 1139

Applying FlexConnect Access Control Lists (GUI)

Related Topics

Configuring FlexConnect Groups (GUI), on page 1189

Configuring Local Web Authentication for a WLAN with SDA and FlexConnect (GUI)

Configuring Local Web Authentication for FlexConnect for a WLAN.

Procedure

Step 1 Choose **WLANs** > **WLAN ID** > **Security** > **Layer 3** tab.

Step 2 From the **Preauthentication ACL** > **WebAuth Flex IPv4 / WebAuth Flex IPv6** drop-down list, choose the ACL that you want to apply to the WLAN.

Step 3 Save the configuration.

Configuring Local Web Authentication from FlexConnect Groups for FlexConnect APs (GUI)

Procedure

Step 1 Choose **Wireless** > **FlexConnect Groups**.

The FlexConnect Groups page appears.

Step 2 Click the Group Name link of the FlexConnect Group for which you want to configure the ACL.

Step 3 Click the **ACL Mapping** > **WLAN-ACL mapping** tab.

Step 4 From the **WebAuth IPv4 ACL/ WebAuth IPv6 ACL**, choose the ACL you want to apply from the drop-down list.

Step 5 Click **Add**.

Step 6 Save the configuration.

Configuring Central Web Authentication and Post Authentication ACL from FlexConnect Groups for FlexConnect APs (GUI)

Procedure

Step 1 Choose **Wireless** > **FlexConnect Groups**

The **FlexConnect Groups** page appears.

Step 2 Click the FlexConnect group name for which you want to configure the ACL.

Step 3 Click the **ACL Mapping** > **Policies** tab.

Step 4 From the **WebAuth IPv4 ACL/ WebAuth IPv6 ACL**, choose the ACL you want to apply from the drop-down list.

Step 5 Click **Add**

Step 6 Save the configuration.

Step 7 Choose **WLANs** > **WLAN ID** > **Security** to open the **WLANs > Edit** page.

Step 8 In the **Security** tab, configure the following parameters:

- Check the **MAC Filtering** check box in the **Layer 2 > Security** tab.

- Set **Layer 3 > Security** to **None** from the drop-down list in the **Layer 3** tab.

Step 9 In the **Advanced** tab, configure the following parameters.

- Check the **Allow AAA Override** check box to enable AAA override.
- Choose **ISE NAC** from the **NAC State** drop-down list.

Step 10 Save the configuration.

Configuring Post-Authentication Fabric ACL for a WLAN (GUI)

Procedure

Step 1 Choose **WLANs** > **WLAN ID** > **Advanced** tab.

Step 2 Check the **Fabric** Enabled check box under the Fabric Configuration section to enable Fabric for this WAN.

Step 3 From the **Fabric IPv4 ACL / Fabric IPv6 ACL** drop-down list, choose the post authentication ACL that you want to add to the Fabric enabled WLAN.

Step 4 Save the configuration.

Applying FlexConnect Access Control Lists (CLI)

Procedure

- Configure the Local Web Authentication for a WLAN by entering this command:

  config wlan security web-auth ipv6 flexacl *wlan-id* {*acl name* | none}

  Remove the applied ACL by using the none.

- Configure Local Web Authentication from FlexConnect Groups for FlexConnect APs by entering this command:

  config flexconnect group *group-name* **web-auth wlan** *wlan-id* **acl** *acl-name* {**enable | disable**}

- Configure the Central Web Authentication and Post Authentication ACL from FlexConnect Groups for FlexConnect APs by entering this command:

  config flexconnect group *group-name* **policy ipv6 acl add** *acl-name*

- Configuring Post-Authentication Fabric ACL for a WLAN by entering this command:

  config wlan fabric ipv6 acl {*acl-name* | **none**} *wlan-id*

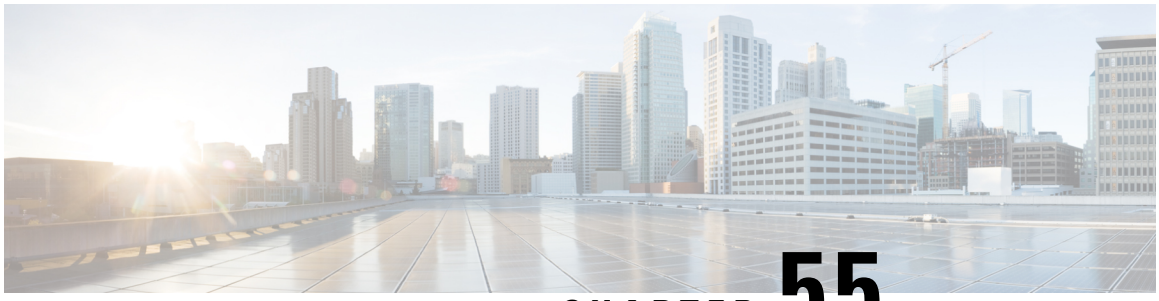
- Configuring Fabric ACL Template for Central Web Authentication and Post Authentication by entering this command:

  config fabric flex-acl-template template-entry *template-name* {**add | delete**} *acl-name*

  Pushes the ACL to AP and applies it to client through the AAA server.

Related Topics

Configuring FlexConnect Groups (CLI), on page 1193



CHAPTER 55

OfficeExtend Access Points

- OfficeExtend Access Points, on page 1239
- Implementing Security, on page 1240
- Configuring OfficeExtend Access Points, on page 1241
- Configuring a Personal SSID on an OfficeExtend Access Point, on page 1246
- Viewing OfficeExtend Access Point Statistics, on page 1247
- Viewing Voice Metrics on OfficeExtend Access Points, on page 1247
- Network Diagnostics, on page 1248
- Remote LANs, on page 1249

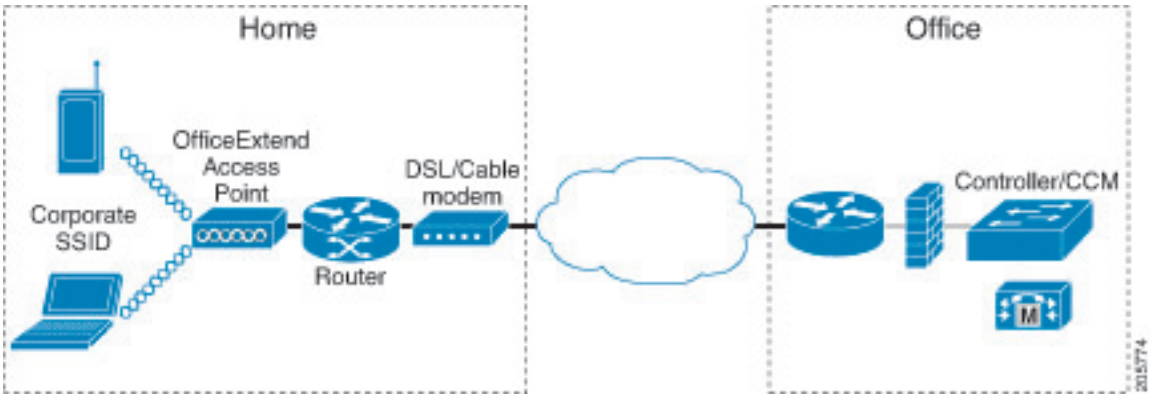
OfficeExtend Access Points

A Cisco OfficeExtend access point (Cisco OEAP) provides secure communications from a controller 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 82: 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. In Release 8.5, only one OEAP is supported behind a NAT device, but in Release 8.10, multiple OEAPs are supported 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.

Additional References

- See the Release Notes for information about supported Cisco OEAPs.
- https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/215928-flexconnect-oeap-with-split-tunneling-co.html

Implementing Security

Note The LSC configuration is optional.

1. (Optional) Use local significant certificates (LSCs) to authorize your OfficeExtend access points, by following the instructions in the "Authorizing Access Points Using LSCs" sectionn.
2. (Optional) 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

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)

Procedure

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 feature is supported on all internal antenna AP models.

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 controller 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.

- Enable split tunneling without gateway override by entering this command:

  config wlan split-tunnel *wlan-id* **enabled apply-acl** *acl name*

- Enable split tunneling with gateway override by entering this command:

  config wlan split-tunnel *wlan-id* **enabled override gateway** *gateway ip* **mask** *subnet mask* **apply-acl** *acl name*

- 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 a Personal SSID on an OfficeExtend Access Point

Procedure

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.

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. For more information, see https://www.cisco.com/c/dam/m/zh_cn/solutions/enterprise-networks/mobility-express/office-extend/office-extend-deployment-guide.pdf.

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.

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*}

Viewing Voice Metrics on OfficeExtend Access Points

Use this command to view information about voice metrics on the OfficeExtend access points in your network:

show ap stats 802.11{a | b} *Cisco_AP*

Information similar to the following appears:

```
OEAP WMM Stats :
  Best Effort:
    Tx Frame Count.............................. 0
    Tx Failed Frame Count....................... 0
    Tx Expired Count............................ 0
    Tx Overflow Count........................... 0
    Tx Queue Count.............................. 0
    Tx Queue Max Count.......................... 0
    Rx Frame Count.............................. 0
    Rx Failed Frame Count....................... 0
  Background:
    Tx Frame Count.............................. 0
    Tx Failed Frame Count....................... 0
```

```
    Tx Expired Count.............................. 0
    Tx Overflow Count............................. 0
    Tx Queue Count................................ 0
    Tx Queue Max Count............................ 0
    Rx Frame Count................................ 0
    Rx Failed Frame Count......................... 0
  Video:
    Tx Frame Count................................ 0
    Tx Failed Frame Count......................... 0
    Tx Expired Count.............................. 0
    Tx Overflow Count............................. 0
    Tx Queue Count................................ 0
    Tx Queue Max Count............................ 0
    Rx Frame Count................................ 0
    Rx Failed Frame Count......................... 0
  Voice:
    Tx Frame Count................................ 0
    Tx Failed Frame Count......................... 0
    Tx Expired Count.............................. 0
    Tx Overflow Count............................. 0
    Tx Queue Count................................ 0
    Tx Queue Max Count............................ 0
    Rx Frame Count................................ 0
    Rx Failed Frame Count......................... 0
```

View the voice metrics on the OfficeExtend access points in your network using the controller GUI as follows:

- 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.
- Hover your cursor over the blue drop-down arrow for the desired access point and click the **Detail** link for the desired client to open the Radio > Statistics page.

  This page shows the **OEAP WMM counters** for this access point.

Network Diagnostics

Network Diagnostics determines the non-DTLS throughput of the system by running a speed test on demand. Network Diagnostics allows troubleshooting of root causes leading to failures. It also determines the link latency and jitter by running a test on demand or periodically.

This section contains the following subsections:

Running Network Diagnostics (GUI)

Procedure

Step 1 Choose **WAN** > **Network Diagnostics**.
The Network Diagnostics page is displayed.

Step 2 Click **Start Diagnostics**.
The diagnostics page is displayed.

Running Network Diagnostics on the Controller

Procedure

Step 1 Choose **Wireless** > **All APs** > **Details**.

Step 2 Choose the **Network Diagnostics** tab.
The Network Diagnostics page is displayed.

Step 3 Click **Start Network Diagnostics**.
The diagnostics page is displayed.

Running Network Diagnostics (CLI)

Procedure

- To run network diagnostics, enter this command on the controller:
  show ap network-diagnostics *ap-name*

Remote LANs

This section describes how to configure remote LANs.

Prerequisites

Guidelines and Restrictions

- It is not possible to configure 802.1X on remote LANs through the controller GUI; configuration only through CLI is supported.
- Starting in Release 8.8, remote LAN clients can pass traffic in CPU switching and hardware switching mode. Prior to Release 8.8, remote LAN clients could pass traffic only in CPU switching mode and local switched remote LAN.

This section contains the following subsections:

Configuring a Remote LAN (GUI)

Procedure

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:

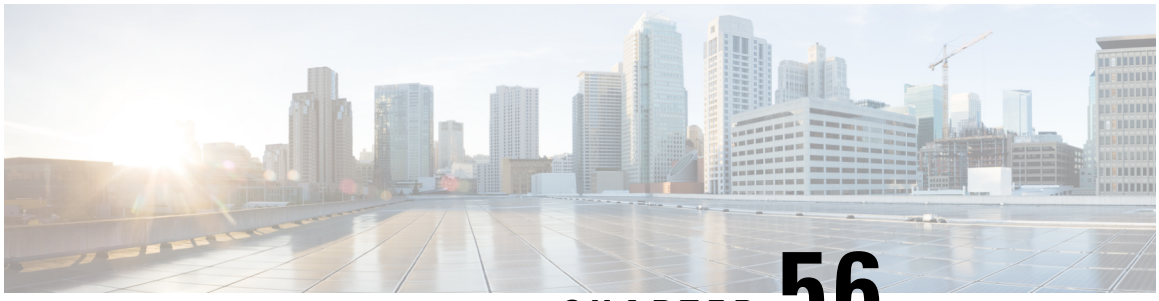
  config remote-lan {**enable** | **disable**} *remote-lan-id*

- 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*
- Configure the local switching of client data associated to flexconnect by entering this command:
  config remote-lan flexconnect local-switching *remote-lan-id* **vlan** *vlan-id*



CHAPTER 56

FlexConnect AP Image Upgrades

- FlexConnect AP Image Upgrades, on page 1253
- Restrictions on FlexConnect AP Image Upgrades, on page 1253
- Configuring FlexConnect AP Upgrades (GUI), on page 1254
- Configuring FlexConnect AP Upgrades (CLI), on page 1255

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.

Related Topics

Predownloading an Image to an Access Point, on page 85

Access Point Predownload Process, on page 86

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 reachable between these access points and firewall must not be deployed.
- 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 CAPWAP over IPv6.
- 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)

Procedure

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.

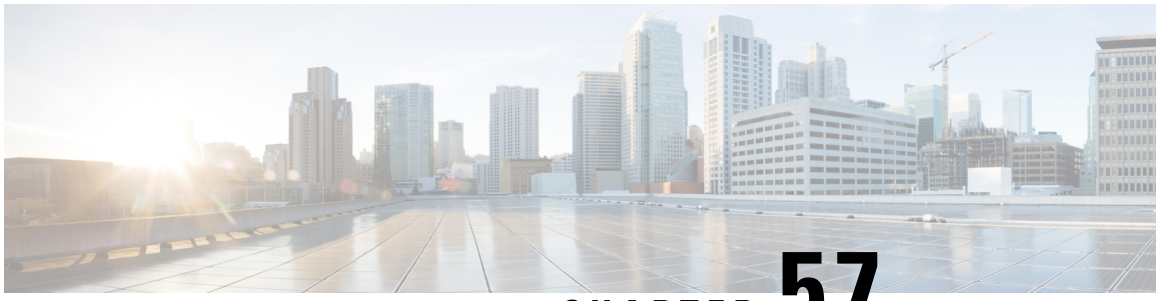
You can manually assign primary access points in the FlexConnect group by selecting the access points.

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.



CHAPTER 57

FlexConnect AP Easy Admin

- FlexConnect AP Easy Admin, on page 1257
- Configuring FlexConnect AP Easy Admin on the Controller (GUI), on page 1257
- Configuring FlexConnect AP Easy Admin on the Controller (CLI), on page 1258

FlexConnect AP Easy Admin

The FlexConnect AP Easy Admin enables unified AP GUI access and configure the following parameters to connect to the controller:

- AP IP address: Static or DHCP IP address.
- Controller IP address priming: Ablity to configure the primary, secondary, and tertiary controller, and their IP addresses.
- CAPWAP preferred DNS configuration.
- PPPoE: Enabling of FlexConnect submode and configuring the username and password for PPPoE server authentication.
- TFTP: AP image upgrade through TFTP.

Configuring FlexConnect AP Easy Admin on the Controller (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration**.

The **Global Configuration** page is displayed.

Step 2 In the **AP Easy Configuration** section, check the **Enable Global AP Easy Configuration** check box.

Note
Easy Configuration is only applicable to the following Cisco Wave 1 (IOS-based) APs: 702, 1530, 1700, 2700, and 3700.

Step 3 Click **Apply**.

Configuring FlexConnect AP Easy Admin on the Controller (CLI)

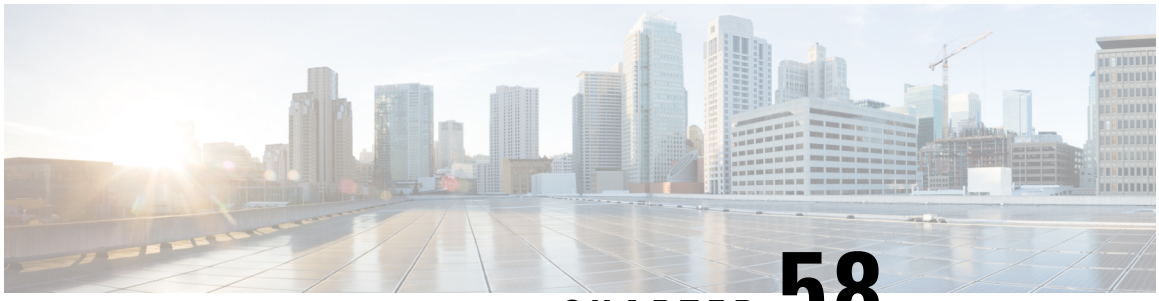
Procedure

Step 1 Enable or disable AP Easy Admin on the controller by entering this command:

config network ap-easyadmin {**enable** | **disable**}

Step 2 View the network summary and to verify the status of AP easy admin feature by entering this command:

show network summary



CHAPTER 58

WeChat Authentication Based Internet Access

- WeChat Client Authentication, on page 1259
- Configuring WeChat Client Authentication on Controller (GUI), on page 1259
- Configuring WeChat Client Authentication on Controller (CLI), on page 1261
- Authenticating Client Using WeChat App for Mobile Internet Access (GUI), on page 1262
- Authenticating Client Using WeChat App for PC Internet Access (GUI), on page 1262

WeChat Client Authentication

The WeChat messaging service is a cross platform communication software which supports text messages, audio calls, video calls, games. WeChat also offers full fledged m-commerce capabilities in their app using which you can do purchases, make bill payments within the WeChat app. This app has a large customer base in China and is gaining popularity in rest of the world. This feature gives WeChat users access to wireless internet service using their smartphones or PC. The authentication of the account is done by the WeChat servers. This is a simple process and requires little user inputs.

This platform benefits both, the customer and the merchant. The customer gets access to the Internet and the merchant gets a customer engaging platform to advertise merchandise and services.

Restrictions on WeChat Client Authentication

- This feature is supported on Cisco Wave 1 APs in FlexConnect mode only.
- Downgrading a controller running a release with QR-Scan or WeChat specific configuration to an older release which does not support this feature leads to XML validation errors for the Layer 3 security type during the downgrade process.

  The errors do not have any impact on the functioning of the controller.

Configuring WeChat Client Authentication on Controller (GUI)

Before you begin

The AP SSID and the controller MAC address needs be configured in the Baitone server database.

Procedure

Step 1 Log in to the controller GUI interface.

Step 2 Choose **WLANs** > **WLAN ID** > **Security** to open the WLANs Edit page.

Step 3 In the **Security** tab, configure the following parameters:

a) Set the Layer 2 Security to **None** from the drop-down list on the Layer 2 tab.

b) Set the Layer 3 Security to **Web Policy** from the drop-down list on the Layer 3 tab.

c) Choose **Passthrough**

d) Select the **Qr Code Scanning** check box.

e) Enter the portal web page address in the **`Redirect URL`** text box and **`Shared Key`** (Preconfigured on the external authentication server).

f) From the **Preauthentication ACL** > **WebAuth FlexAcl** drop-down list, choose the Acl option that you want to apply to the WLAN.

Before the client is authenticated, this Acl allows the authentication traffic to pass through to the WeChat authentication servers.

Step 4 In the **Advanced** tab, select the **FlexConnect Local Switching** check box.

Step 5 (Optional) Enable local authentication by configuring the following parameters:

a) Under the **Security** tab, select the **Web policy done locally on AP** check box.

This enables local authentication at the AP and the central authentication at the controller is disabled.

b) In the **Advanced** tab, select the **FlexConnect Local Auth** check box.

Set this option to enable if **Web policy done locally on AP** is enabled

Step 6 On the **Wireless** tab, follow the steps:

a) Select the **FlexConnect ACLs**.

Choose an existing Acl or create a new Acl

b) Add the **`portal page IP address`** and the **`WeChat authentication server IP address`** with permit action as new rules.

Step 7 In the **Wireless** > **Global Configuration** page, configure the following parameter:

a) Enter the virtual IP address in the **AP Virtual IP address** text box.

The default Virtual AP IP address is: 10.1.0.6. The controller and the client interact with the AP using this AP virtual IP address.

Step 8 Choose **Security** > **Web Auth** > **Web Login Page**. Enter the values for:

a) **QrCode Scanning Bypass Timer**. The valid range is between 5 and 60 seconds to allow traffic temporary.

b) **QrCode Scanning Bypass Count**. The valid range is between 1 to 9 retries to bypass for authentication.

Configuring WeChat Client Authentication on Controller (CLI)

Before you begin

The AP SSID and the controller MAC address needs be configured in the external authentication server database.

Procedure

Step 1 Configure the WLAN:

a) Create a WLAN, by entering this command:

config wlan create *wlan-id profile-name ssid-name*

b) Disable L2 security by entering this command:

config wlan security wpa disable *wlan-id*

c) Enable WLAN L3 passthrough by entering this command:

config wlan security web-passthroughenable *wlan-id*

Step 2 Enable FlexConnect mode in a Cisco AP by entering this command:

config ap mode flexconnect *Cisco-AP*

Step 3 Enable or disable QR code scanning support for clients on the controller by entering this command:

config wlan security web-passthrough qr-scan {**enable | disable**}*wlan-id*

Step 4 Configure the QR-scan DES key for the WLAN by entering this command:

config wlan security web-auth *des key string wlan-id*

Step 5 Configure the QR scan authentication options - timer, and count by entering this command:

config custom-web qrscan-bypass-opt *timer count*

Step 6 Configure the external Web Authentication URL by entering this command:

config custom-web ext-webauth-url *ext-webauth-url*

Step 7 Configure flex-acl and attach to WLAN in L3 security

Step 8 Configure virtual IP of Controller with the same IP which is configured on Baitone

Step 9 Enable or disable QR code scanning support for clients on the controller:

- Enable or disable central authentication QR code scanning support for clients on the controller by entering this command:

  config wlan security web-passthrough qr-scan{**enable | disable**} *wlan-id*

- Enable or disable local authentication QR code scanning support for clients on the controller by entering this command:

  config wlan security web-passthrough qr-scan local{**enable | disable**} *wlan-id*

Step 10 Configure virtual IP for an AP by entering this command:

config ap virtual_ip {**enable** | **disable**} *ip address*

Step 11 See the state of WeChat QR scan feature for specific WLAN by entering this command:

show wlan *wlan-id*

Step 12 See the QR scan bypass options by entering this command:

show custom-web all

Authenticating Client Using WeChat App for Mobile Internet Access (GUI)

Before you begin

The WeChat App must be installed in the smartphone.

Procedure

Step 1 Connect the smartphone to the WeChat enabled SSID.

a) IPhone—Opens the portal page automatically.
b) Android—Open a URL using a browser which will redirect to the portal page.

Once connected to the SSID, you have 60 seconds to validate the WeChat account.

Step 2 Click the green button displayed to validate the WeChat account.

Step 3 Click the green connect button to connect to WeChat over Wi-Fi.

The merchant page is displayed which confirms the user is connected to the Internet.

Authenticating Client Using WeChat App for PC Internet Access (GUI)

Before you begin

The customer's mobile must have the WeChat app installed and have access to the Internet to authenticate the WeChat account.

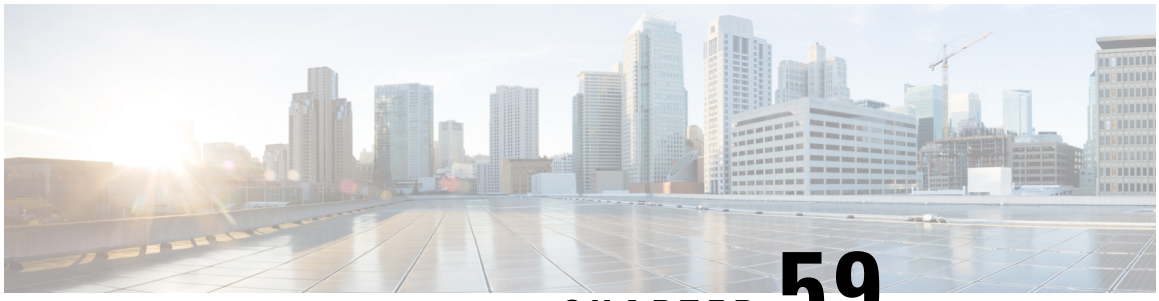
Procedure

Step 1 Connect the PC to the WeChat enabled SSID.

The server identifies the client and displays the portal web page with a QR code.

Step 2 Scan the QR code using the WeChat app on the mobile.
The WeChat account authentication success is displayed.

Step 3 The PC browser displays the merchant page and is able to access the Internet.



CHAPTER 59

Lawful Interception of Traffic

- Lawful Interception of Traffic, on page 1265
- Configuring Lawful Interception of Traffic on a Cisco Controller (CLI), on page 1265
- Viewing and Debugging Lawful Interception of Traffic on a Cisco Access Point (CLI), on page 1266

Lawful Interception of Traffic

Using the Cisco wireless solution, it is possible to lawfully intercept traffic for monitoring purposes.

Cisco APs create syslog records for traffic and send the records to the controller. Traffic from both IPv4 and IPv6 protocols is recorded. The controller at configured intervals sends these syslog records to the syslog server.

Note The Cisco controller does not store any traffic interception related records.

Restrictions on Lawful Interception of Traffic

- To support IPv6 protocol, enable IPv6 on the controller
- This feature is supported only in Cisco Wave 2 APs operating in Flex + Bridge mode.

Configuring Lawful Interception of Traffic on a Cisco Controller (CLI)

Procedure

- Configure lawful interception by entering this command:

  config flexconnect lawful-intercept {**enable** | **disable**}

- Configure the syslog for IPv4 and IPv6 host by entering this command:

  config flexconnect lawful-intercept syslog host global {*ipv4 addr* | *ipv6 addr*}

- Configure the time interval for the syslog to be sent to the syslog server by entering this command:
  config flexconnect lawful-intercept timer *timer-value*
- See the lawful interception summary by entering this command:
  show flexconnect lawful-interception summary

Viewing and Debugging Lawful Interception of Traffic on a Cisco Access Point (CLI)

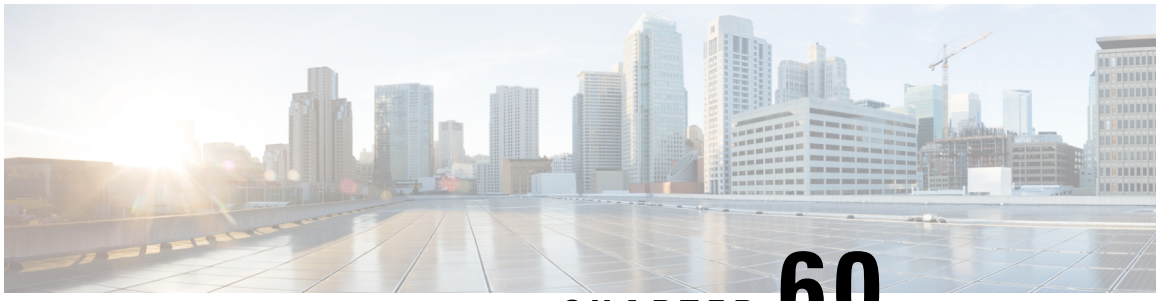
Procedure

- See the lawful interception summary by entering this command:
  show flexconnect lawful-interception summary
- Debug lawful intercept by entering this command:
  debug lawful-intercept flows {all | mac-addr {**all** | *mac-addr*}}
- Debug lawful-intercept syslog by entering this command:
  debug lawful-intercept syslog

PART IX

Monitoring the Network

- Monitoring the Controller, on page 1269
- System and Message Logging, on page 1273



CHAPTER 60

Monitoring the Controller

- Viewing System Resources, on page 1269
- Viewing System Resources (GUI), on page 1269
- Viewing System Resources (CLI), on page 1270

Viewing System Resources

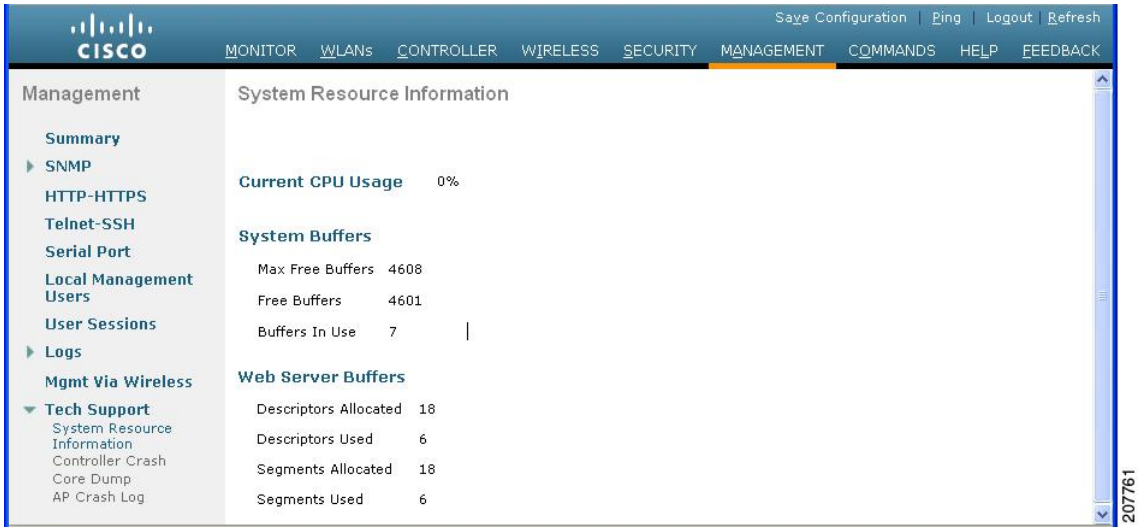
You can determine the amount of system resources being used by the controller. Specifically, you can view the current controller CPU usage, system buffers, and web server buffers.

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 83: System Resource Information Page



The following system information is displayed:

- **System Resource Information**: Displays current and individual CPU usage, system buffers, and web server buffers.
- **Controller Crash Information**: Displays information present in the controller crash log file.
- **Core Dump**: Configures the core dump transfer through FTP. You must enter the server details to where the core dump has to be transferred.
- **AP Crash Logs**: Displays AP crash log information.
- **System Statistics**:
  - **IO Stats**: Displays CPU and input/output statistics for the controller.
  - **Top**: Displays the CPU usage.
- **Dx LCache Summary**: Displays database and local cache statistics.

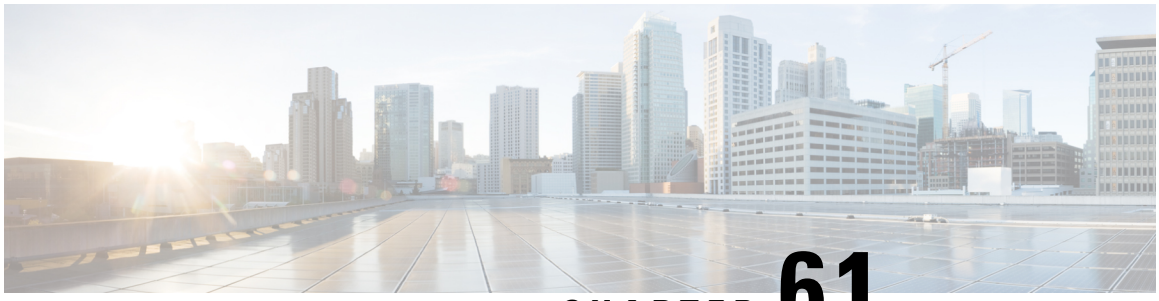
Viewing System Resources (CLI)

On the controller CLI, enter these commands:

- **show cpu**: Displays current CPU usage information.

  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**: Displays system resource information.
- **show system dmesg clear**: Clears the dmesg logs after first printing its contents. The dmesg file contains the kernel log-messages.
- **show system interfaces**: Displays information about the configured network interfaces.

- **show system interrupts**: Displays the number of interrupts.
- **show system iostat** {**summary** | **detail**}: Displays CPU and input/output statistics.
- **show system ipv6**:
  - **show system ipv6 neighbours**: Displays the IPv6 neighbor cache.
  - **show system ipv6 netstat**: Displays system network IPv6 stats.
  - **show system ipv6 route**: Displays the IPv6 route information.
- **show system meminfo**: Displays system memory information.
- **show system neighbours**: Displays the IPv6 neighbor cache.
- **show system netstat**: Displays system network stats.
- **show system portstat**:
  - **show system portstat all verbose**: Displays all system active service or port statistics.
  - **show system portstat tcp verbose**: Displays system active service or port statistics related to TCP.
  - **show system portstat udp verbose**: Displays system active service or port statistics related to UDP.
- **show system process**:
  - **show system process maps** *pid*: Displays region of contiguous virtual memory in the PID.
  - **show system process stat** {**all** | *pid*}: Displays statistics for all or a particular process.
  - **show system process summary** : Displays a summary of processes.
- **show system route**: Displays system routing table.
- **show system slabs**: Displays memory usage on slab level.
- **show system slabtop**: Displays the slab usage.
- **show system timer ticks**: Displays the number of ticks and seconds since the timer lib started.
- **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 usb**: Displays configuration of USB.
- **show system vmstat**: Displays system virtual memory statistics.



CHAPTER 61

System and Message Logging

• System and Message Logging, on page 1273

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.

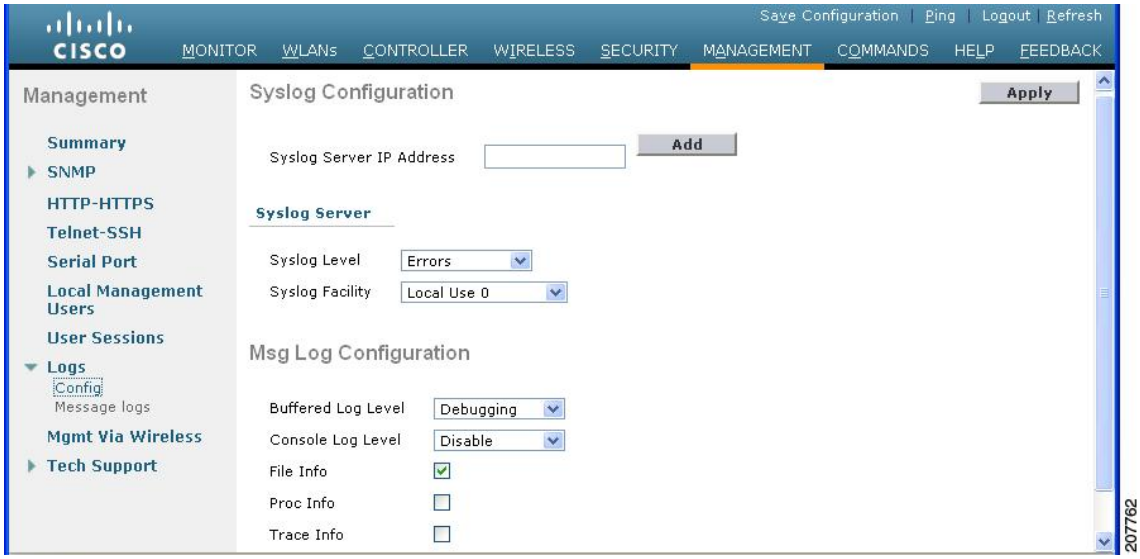
This section contains the following subsections:

Configuring System and Message Logging (GUI)

Procedure

Step 1 Choose **Management** > **Logs** > **Config**. The Syslog Configuration page appears.

Figure 84: Syslog Configuration Page



Step 2 In the **Syslog Server IP Address (IPv4/IPv6)** field, 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 field.

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)

Procedure

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 {**assocfail** | **associate** | **authentication** | **authfail** | **deauthenticate** | **disassociate** | **excluded**} {**enable** | **disable**}

where:

- **assocfail**: 802.11 association fail syslog for clients.
- **authentication**: Authentication success syslog for clients
- **authfail**: 802.11 authentication fail syslog for clients
- **deauthenticate**: 802.11 deauthentication syslog for clients
- **disassociate**: 802.11 disassociation syslog for clients
- **excluded**: Excluded syslog for clients

Step 8 Configure transmission of syslog messages over IPSec by entering this command:

config logging syslog ipsec {**enable** | **disable**}

Step 9 Configure transmission of syslog messages over transport layer security (TLS) by entering this command:

config logging syslog tls {**enable** | **disable**}

Enabling syslog over TLS on the controller enables the feature for all syslog hosts defined in the controller. You can define up to three syslog hosts per controller. The controller transmits messages concurrently to all the configured syslog hosts.

Check if the controller has an active TLS connection to the syslog server by entering the **show logging** command. The following is a sample output:

```
- syslog over tls.............................. Enabled
  - Host 0..................................... 209.165.200.224
    - TLS auth status.......................... connected
    - packets sent............................. 3879
    - packets dropped.......................... 2
  - Host 1.....................................
  - Host 2.....................................
```

Caution
Issue: Some messages are not transmitted to the syslog server even though it is reachable.

Analysis: This issue occurs because syslog over TLS is enabled in the controller, multiple syslog hosts are defined in the controller, the number of syslog messages generated are high, and one of the syslog hosts is not reachable over TLS.

Step 10 Set the severity level for logging messages to the controller buffer and console by entering 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 11 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 12 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 13 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 14 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 15 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 16 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 *ap-name*

  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 all access points or for a specific access point joined to the controller, enter this command:

  clear ap eventlog {**all** | *ap-name*}

PART X

Troubleshooting

- Debugging on Cisco Wireless Controllers, on page 1285
- Controller Unresponsiveness, on page 1299
- Debugging on Cisco Access Points, on page 1311
- Packet Capture, on page 1325

CHAPTER 62

Debugging on Cisco Wireless Controllers

- Troubleshooting AAA RADIUS Interactions for WLAN Authentication, on page 1285
- Understanding Debug Client on Wireless Controllers, on page 1293
- Deauthenticating Clients, on page 1293
- Using the CLI to Troubleshoot Problems, on page 1294
- Potential Reasons for Controller Reset, on page 1296

Troubleshooting AAA RADIUS Interactions for WLAN Authentication

- Test AAA RADIUS interactions for WLAN authentication by entering this command:

  test aaa radius username *username* **password** *password* **wlan-id** *wlan-id* [**apgroup** *apgroupname* **server-index** *server-index*]

  The command parameters include the following:

  - username and password (both in plain text)
  - WLAN ID
  - AP group name (optional)
  - AAA server index (optional)

  This test command sends to the RADIUS server an access request for client authentication. Access request exchange takes place between controller and AAA server, and the registered RADIUS callback handles the response.

  The response includes authentication status, number of retries, and RADIUS attributes.

- View the RADIUS response to test RADIUS request by entering this command:

  test aaa show radius

Guidelines

- Both username and password must be plain text, similar to MAC authentication
- If AP group is entered, the WLAN entered must belong to that AP group

- If server index is entered, the request to test RADIUS is sent only to that RADIUS server
- If the RADIUS request does not get a response, the request is not sent to any other RADIUS server
- RADIUS server at the server index must be in enabled state
- This test command can be used to verify configuration and communication related to AAA RADIUS server and should not be used for actual user authentication
- It is assumed that the AAA server credentials are set up as required

Restrictions

- No GUI support
- No TACACS+ support

Example: Access Accepted

```
(Cisco Controller) > test aaa radius username user1 password Cisco123 wlan-id 7 apgroup
default-group server-index 2

Radius Test Request

  Wlan-id..................................... 7
  ApGroup Name................................ default-group

  Attributes                      Values
  ----------                      ------
  User-Name                       user1
  Called-Station-Id               00:00:00:00:00:00:EngineeringV81
  Calling-Station-Id              00:11:22:33:44:55
  Nas-Port                        0x0000000d (13)
  Nas-Ip-Address                  172.20.227.39
  NAS-Identifier                  WLC5520
  Airespace / WLAN-Identifier     0x00000007 (7)
  User-Password                   Cisco123
  Service-Type                    0x00000008 (8)
  Framed-MTU                      0x00000514 (1300)
  Nas-Port-Type                   0x00000013 (19)
  Tunnel-Type                     0x0000000d (13)
  Tunnel-Medium-Type              0x00000006 (6)
  Tunnel-Group-Id                 0x00000051 (81)
  Cisco / Audit-Session-Id        ac14e327000000c456131b33
  Acct-Session-Id                 56131b33/00:11:22:33:44:55/210

test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) > test aaa show radius

Radius Test Request
  Wlan-id..................................... 7
  ApGroup Name................................ default-group
  Server Index................................ 2
Radius Test Response
Radius Server            Retry Status
-------------            ----- ------
172.20.227.52            1     Success
Authentication Response:
  Result Code: Success
  Attributes                      Values
```

```
  ----------                    ------
  User-Name                     user1
  Class                         CACS:rs-acs5-6-0-22/230677882/20313
  Session-Timeout               0x0000001e (30)
  Termination-Action            0x00000000 (0)
  Tunnel-Type                   0x0000000d (13)
  Tunnel-Medium-Type            0x00000006 (6)
  Tunnel-Group-Id               0x00000051 (81)

(Cisco Controller) > debug aaa all enable

*emWeb: Oct 06 09:48:12.931: 00:11:22:33:44:55 Sending Accounting request (2) for station
00:11:22:33:44:55
*emWeb: Oct 06 09:48:12.932: 00:11:22:33:44:55 Created Cisco-Audit-Session-ID for the mobile:

ac14e327000000c85613fb4c
*aaaQueueReader: Oct 06 09:48:12.932: User user1 password lengths don't match
*aaaQueueReader: Oct 06 09:48:12.932: ReProcessAuthentication previous proto 8, next proto
 40000001
*aaaQueueReader: Oct 06 09:48:12.932: AuthenticationRequest: 0x2b6d5ab8
*aaaQueueReader: Oct 06 09:48:12.932:  Callback.....................................0x101cd740
*aaaQueueReader: Oct 06 09:48:12.932:  protocolType.................................0x40000001
*aaaQueueReader: Oct 06 09:48:12.932:  proxyState....................00:11:22:33:44:55-00:00
*aaaQueueReader: Oct 06 09:48:12.932:  Packet contains 16 AVPs (not shown)
*aaaQueueReader: Oct 06 09:48:12.932: Putting the quth request in qid 5, srv=index 1
*aaaQueueReader: Oct 06 09:48:12.932: Request
Authenticator 3c:b3:09:34:95:be:ab:16:07:4a:7f:86:3b:58:77:26
*aaaQueueReader: Oct 06 09:48:12.932: 00:11:22:33:44:55 Sending the packet
to v4 host 172.20.227.52:1812
*aaaQueueReader: Oct 06 09:48:12.932: 00:11:22:33:44:55 Successful transmission of
Authentication Packet (id 13) to 172.20.227.52:1812 from server queue 5,
proxy state 00:11:22:33:44:55-00:00
. . .
*radiusTransportThread: Oct 06 09:48:12.941: 00:11:22:33:44:55 Access-Accept received from

RADIUS server 172.20.227.52 for mobile 00:11:22:33:44:55 receiveId = 0
*radiusTransportThread: Oct 06 09:48:12.941: AuthorizationResponse: 0x146c56b8
*radiusTransportThread: Oct 06 09:48:12.941: structureSize.............................263
*radiusTransportThread: Oct 06 09:48:12.941: resultCode.................................0
*radiusTransportThread: Oct 06 09:48:12.941:
protocolUsed.............................0x00000001
*radiusTransportThread: Oct 06 09:48:12.941:
proxyState.....................00:11:22:33:44:55-00:00
*radiusTransportThread: Oct 06 09:48:12.941: Packet contains 7 AVPs:
*radiusTransportThread: Oct 06 09:48:12.941: AVP[01] User-Name.................user1 (5
bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[02]
Class..........CACS:rs-acs5-6-0-22/230677882/20696 (35 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[03] Session-Timeout........0x0000001e (30)
 (4 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[04] Termination-Action....0x00000000 (0)
(4 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[05] Tunnel-Type......0x0100000d (16777229)
 (4 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[06] Tunnel-Medium-Type...0x01000006
(16777222) (4 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: AVP[07] Tunnel-Group-Id.......DATA (3 bytes)
*radiusTransportThread: Oct 06 09:48:12.941: Received radius callback for
test aaa radius request result 0 numAVPs 7.
```

Example: Access Failed

```
(Cisco Controller) > test aaa radius username user1
password C123 wlan-id 7 apgroup default-group server-index 2

Radius Test Request
  Wlan-id..................................... 7
  ApGroup Name................................ default-group
  Attributes                    Values
  ----------                    ------
  User-Name                     user1
  Called-Station-Id             00:00:00:00:00:00:EngineeringV81
  Calling-Station-Id            00:11:22:33:44:55
  Nas-Port                      0x0000000d (13)
  Nas-Ip-Address                172.20.227.39
  NAS-Identifier                WLC5520
  . . .
  Tunnel-Type                   0x0000000d (13)
  Tunnel-Medium-Type            0x00000006 (6)
  Tunnel-Group-Id               0x00000051 (81)
  Cisco / Audit-Session-Id      ac14e327000000c956140806
  Acct-Session-Id               56140806/00:11:22:33:44:55/217
test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) > test aaa show radius

Radius Test Request
  Wlan-id..................................... 7
  ApGroup Name................................ default-group
  Server Index................................ 2
Radius Test Response
Radius Server           Retry Status
-------------           ----- ------
172.20.227.52           1     Success
Authentication Response:
  Result Code: Authentication failed
  No AVPs in Response

(Cisco Controller) > debug aaa all enable

*emWeb: Oct 06 10:42:30.638: 00:11:22:33:44:55 Sending Accounting request
(2) for station 00:11:22:33:44:55
*emWeb: Oct 06 10:42:30.638: 00:11:22:33:44:55 Created Cisco-Audit-Session-ID for the
mobile: ac14e327000000c956140806
*aaaQueueReader: Oct 06 10:42:30.639: User user1 password lengths don't match
*aaaQueueReader: Oct 06 10:42:30.639: ReProcessAuthentication previous proto 8, next proto
 40000001
*aaaQueueReader: Oct 06 10:42:30.639: AuthenticationRequest: 0x2b6bdc3c
*aaaQueueReader: Oct 06 10:42:30.639:  Callback.....................................0x101cd740
*aaaQueueReader: Oct 06 10:42:30.639:  protocolType.................................0x40000001
*aaaQueueReader: Oct 06 10:42:30.639:  proxyState....................00:11:22:33:44:55-00:00
*aaaQueueReader: Oct 06 10:42:30.639:  Packet contains 16 AVPs (not shown)
*aaaQueueReader: Oct 06 10:42:30.639: Putting the quth request in qid 5, srv=index 1
*aaaQueueReader: Oct 06 10:42:30.639: Request Authenticator
34:73:58:fd:8f:11:ba:6c:88:96:8c:e5:e0:84:e4:a5
*aaaQueueReader: Oct 06 10:42:30.639: 00:11:22:33:44:55
Sending the packet to v4 host 172.20.227.52:1812
*aaaQueueReader: Oct 06 10:42:30.639: 00:11:22:33:44:55
Successful transmission of Authentication Packet (id 14) to 172.20.227.52:1812 from server
 queue 5,
proxy state 00:11:22:33:44:55-00:00
 . . .
*radiusTransportThread: Oct 06 10:42:30.647: 00:11:22:33:44:55 Access-Reject received from
 RADIUS
```

```
server 172.20.227.52 for mobile 00:11:22:33:44:55 receiveId = 0
*radiusTransportThread: Oct 06 10:42:30.647: 00:11:22:33:44:55 Returning AAA Error
'Authentication Failed' (-4) for mobile 00:11:22:33:44:55
*radiusTransportThread: Oct 06 10:42:30.647: AuthorizationResponse: 0x3eefd664
*radiusTransportThread: Oct 06 10:42:30.647:  structureSize.............................92
*radiusTransportThread: Oct 06 10:42:30.647:  resultCode.................................-4
*radiusTransportThread: Oct 06 10:42:30.647:
protocolUsed.............................0xffffffff
*radiusTransportThread: Oct 06 10:42:30.647:
proxyState.....................00:11:22:33:44:55-00:00
*radiusTransportThread: Oct 06 10:42:30.647:  Packet contains 0 AVPs:
*radiusTransportThread: Oct 06 10:42:30.647: Received radius callback for
test aaa radius request result -4 numAVPs 0.
```

Example: Unresponsive AAA Server

```
(Cisco Controller) > test aaa radius username user1
password C123 wlan-id 7 apgroup default-group server-index 3

Radius Test Request
  Wlan-id..................................... 7
  ApGroup Name................................ default-group
  Attributes                    Values
  ----------                    ------
  User-Name                     user1
  Called-Station-Id             00:00:00:00:00:00:EngineeringV81
  Calling-Station-Id            00:11:22:33:44:55
  Nas-Port                      0x0000000d (13)
  Nas-Ip-Address                172.20.227.39
  NAS-Identifier                WLC5520
  . . .
  Tunnel-Group-Id               0x00000051 (81)
  Cisco / Audit-Session-Id      ac14e327000000ca56140f7e
  Acct-Session-Id               56140f7e/00:11:22:33:44:55/218
test radius auth request successfully sent. Execute 'test aaa show radius' for response
(Cisco Controller) >test aaa show radius


 previous test command still not completed, try after some time

(Cisco Controller) > test aaa show radius
Radius Test Request
  Wlan-id..................................... 7
  ApGroup Name................................ default-group
  Server Index................................ 3
Radius Test Response
Radius Server            Retry Status
-------------            ----- ------
172.20.227.72            6     No response received from server
Authentication Response:
  Result Code: No response received from server
  No AVPs in Response

(Cisco Controller) > debug aaa all enable

*emWeb: Oct 06 11:42:20.674: 00:11:22:33:44:55 Sending Accounting request
(2) for station 00:11:22:33:44:55
*emWeb: Oct 06 11:42:20.674: 00:11:22:33:44:55 Created Cisco-Audit-Session-ID for the mobile:

ac14e327000000cc5614160c
*aaaQueueReader: Oct 06 11:42:20.675: User user1 password lengths don't match
*aaaQueueReader: Oct 06 11:42:20.675: ReProcessAuthentication previous proto 8, next proto
```

```
 40000001
*aaaQueueReader: Oct 06 11:42:20.675: AuthenticationRequest: 0x2b6d2414
*aaaQueueReader: Oct 06 11:42:20.675:  Callback.....................................0x101cd740
*aaaQueueReader: Oct 06 11:42:20.675:  protocolType.................................0x40000001
*aaaQueueReader: Oct 06 11:42:20.675:
proxyState.....................00:11:22:33:44:55-00:00
*aaaQueueReader: Oct 06 11:42:20.675:  Packet contains 16 AVPs (not shown)
*aaaQueueReader: Oct 06 11:42:20.675: Putting the quth request in qid 5, srv=index 2
*aaaQueueReader: Oct 06 11:42:20.675: Request
Authenticator 03:95:a5:d5:16:cd:fb:60:ef:31:5d:d1:52:10:8e:7e
*aaaQueueReader: Oct 06 11:42:20.675: 00:11:22:33:44:55 Sending the packet
 to v4 host 172.20.227.72:1812
*aaaQueueReader: Oct 06 11:42:20.675: 00:11:22:33:44:55 Successful transmission of
Authentication Packet (id 3) to
172.20.227.72:1812 from server queue 5, proxy state 00:11:22:33:44:55-00:00
. . .
*radiusTransportThread: Oct 06 11:42:22.789: 00:11:22:33:44:55 Retransmit the
'Access-Request' (id 3) to 172.20.227.72 (port 1812, qid 5) reached for mobile
00:11:22:33:44:55. message retransmit cnt 1, server retries 15
*radiusTransportThread: Oct 06 11:42:22.790: 00:11:22:33:44:55 Sending the packet to v4
host
172.20.227.72:1812
*radiusTransportThread: Oct 06 11:42:22.790: 00:11:22:33:44:55 Successful transmission of
Authentication Packet (id 3) to 172.20.227.72:1812 from server queue 5, proxy state
 00:11:22:33:44:55-00:00
. . .
*radiusTransportThread: Oct 06 11:42:33.991: 00:11:22:33:44:55 Max retransmit
of Access-Request (id 3) to 172.20.227.72 (port 1812, qid 5) reached for mobile
00:11:22:33:44:55. message retransmit cnt 6, server retransmit cnt 20
*radiusTransportThread: Oct 06 11:42:33.991: server_index is provided with test aaa radius
 request.
Not doing failover.
*radiusTransportThread: Oct 06 11:42:33.991: 00:11:22:33:44:55 Max servers (tried 1)
retransmission of Access-Request (id 3) to 172.20.227.72 (port 1812, qid 5) reached for
 mobile 00:11:22:33:44:55. message retransmit cnt 6, server r
*radiusTransportThread: Oct 06 11:42:33.991: 00:11:22:33:44:55 Returning AAA Error
'Timeout' (-5) for mobile 00:11:22:33:44:55
*radiusTransportThread: Oct 06 11:42:33.991: AuthorizationResponse: 0x3eefe934
*radiusTransportThread: Oct 06 11:42:33.991:  structureSize.............................92
*radiusTransportThread: Oct 06 11:42:33.991:  resultCode.................................-5
*radiusTransportThread: Oct 06 11:42:33.991:
protocolUsed.................................0xffffffff
*radiusTransportThread: Oct 06 11:42:33.991:
proxyState.....................00:11:22:33:44:55-00:00
*radiusTransportThread: Oct 06 11:42:33.991:  Packet contains 0 AVPs:
*radiusTransportThread: Oct 06 11:42:33.991: Received radius callback for
test aaa radius request result -5 numAVPs 0.
```

Example: NAS ID

```
(Cisco Controller) > show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.2.1.82
. . .
System Nas-Id.................................... WLC5520
WLC MIC Certificate Types........................ SHA1

(Cisco Controller) >show interface detailed engineering_v81

Interface Name................................... engineering_v81
MAC Address...................................... 50:57:a8:c7:32:4f
```

```
IP Address..................................... 10.10.81.2
. . .
NAS-Identifier................................. v81-nas-id
Active Physical Port........................... LAG (13)
. . .

(Cisco Controller) > test aaa radius username user1
password C123 wlan-id 7 apgroup default-group server-index 2

Radius Test Request
  Wlan-id....................................... 7
  ApGroup Name.................................. default-group
  Attributes                    Values
  ----------                    ------
  User-Name                     user1
  Called-Station-Id             00:00:00:00:00:00:EngineeringV81
  Calling-Station-Id            00:11:22:33:44:55
  Nas-Port                      0x0000000d (13)
  Nas-Ip-Address                172.20.227.39
  NAS-Identifier                v81-nas-id
  Airespace / WLAN-Identifier   0x00000007 (7)
 . . .

(Cisco Controller) > debug aaa all enable

*emWeb: Oct 06 13:54:52.543: 00:11:22:33:44:55 Sending Accounting request
(2) for station 00:11:22:33:44:55
*emWeb: Oct 06 13:54:52.543: 00:11:22:33:44:55 Created Cisco-Audit-Session-ID for the
 mobile: ac14e327000000ce5614351c
*aaaQueueReader: Oct 06 13:54:52.544: User user1 password lengths don't match
*aaaQueueReader: Oct 06 13:54:52.544: ReProcessAuthentication previous proto 8, next proto
 40000001
*aaaQueueReader: Oct 06 13:54:52.544: AuthenticationRequest: 0x2b6bf140
*aaaQueueReader: Oct 06 13:54:52.544:  Callback.....................................0x101cd740
*aaaQueueReader: Oct 06 13:54:52.544:  protocolType.................................0x40000001
*aaaQueueReader: Oct 06 13:54:52.544:  proxyState....................00:11:22:33:44:55-00:00
*aaaQueueReader: Oct 06 13:54:52.544:  Packet contains 16 AVPs (not shown)
*aaaQueueReader: Oct 06 13:54:52.544: Putting the quth request in qid 5, srv=index 1
*aaaQueueReader: Oct 06 13:54:52.544: Request
Authenticator bc:e4:8e:cb:56:9b:e8:fe:b7:f9:a9:04:15:25:10:26
*aaaQueueReader: Oct 06 13:54:52.544: 00:11:22:33:44:55 Sending the packet
 to v4 host 172.20.227.52:1812
*aaaQueueReader: Oct 06 13:54:52.544: 00:11:22:33:44:55
Successful transmission of Authentication Packet (id 16) to 172.20.227.52:1812 from server
 queue 5,
proxy state 00:11:22:33:44:55-00:00
*aaaQueueReader: Oct 06 13:54:52.545: 00000000: 01 10 00 f9 bc e4 8e cb  56 9b e8 fe b7 f9
 a9 04  ........V.......
*aaaQueueReader: Oct 06 13:54:52.545: 00000010: 15 25 10 26 01 07 75 73  65 72 31 1e 22 30
 30 3a  .%.&..user1."00:
*aaaQueueReader: Oct 06 13:54:52.545: 00000020: 30 30 3a 30 30 3a 30 30  3a 30 30 3a 30 30
 3a 45  00:00:00:00:00:E
*aaaQueueReader: Oct 06 13:54:52.545: 00000030: 6e 67 69 6e 65 65 72 69  6e 67 56 38 31 1f
 13 30  ngineeringV81..0
*aaaQueueReader: Oct 06 13:54:52.545: 00000040: 30 3a 31 31 3a 32 32 3a  33 33 3a 34 34 3a
 35 35  0:11:22:33:44:55
*aaaQueueReader: Oct 06 13:54:52.545: 00000050: 05 06 00 00 00 0d 04 06  ac 14 e3 27 20 0c
 76 38  ...........'..v8
*aaaQueueReader: Oct 06 13:54:52.545: 00000060: 31 2d 6e 61 73 2d 69 64  1a 0c 00 00 37 63
 01 06  1-nas-id....7c..
*aaaQueueReader: Oct 06 13:54:52.545: 00000070: 00 00 00 07 02 12 88 65  4b bf 0c 2c 86 6e
 b0 c7  .......eK..,.n..
*aaaQueueReader: Oct 06 13:54:52.545: 00000080: 7a c1 67 fa 09 12 06 06  00 00 00 08 0c 06
 00 00  z.g.............
```

```
*aaaQueueReader: Oct 06 13:54:52.545: 00000090: 05 14 3d 06 00 00 00 13  40 06 00 00 00 0d
 41 06  ..=.....@.....A.
*aaaQueueReader: Oct 06 13:54:52.545: 000000a0: 00 00 00 06 51 04 38 31  1a 31 00 00 00 09
 01 2b  ....Q.81.1.....+
*aaaQueueReader: Oct 06 13:54:52.545: 000000b0: 61 75 64 69 74 2d 73 65  73 73 69 6f 6e 2d
 69 64  audit-session-id
*aaaQueueReader: Oct 06 13:54:52.545: 000000c0: 3d 61 63 31 34 65 33 32  37 30 30 30 30 30
 30 63  =ac14e327000000c
*aaaQueueReader: Oct 06 13:54:52.545: 000000d0: 65 35 36 31 34 33 35 31  63 2c 20 35 36 31
 34 33  e5614351c,.56143
*aaaQueueReader: Oct 06 13:54:52.545: 000000e0: 35 31 63 2f 30 30 3a 31  31 3a 32 32 3a 33
 33 3a  51c/00:11:22:33:
*aaaQueueReader: Oct 06 13:54:52.545: 000000f0: 34 34 3a 35 35 2f 32 32  34
        44:55/224
*radiusTransportThread: Oct 06 13:54:52.560: 5.client sockfd 35 is set. process the msg
*radiusTransportThread: Oct 06 13:54:52.560: ****Enter processIncomingMessages: Received
Radius
response (code=3)
```

Example: Changing MAC Delimiter

```
(Cisco Controller) > test aaa radius username user1
password Cisco123 wlan-id 7 apgroup default-group server-index 2

Radius Test Request
  Wlan-id..................................... 7
  ApGroup Name................................ default-group
  Attributes                  Values
  ----------                  ------
  User-Name                   user1
  Called-Station-Id           00-00-00-00-00-00:EngineeringV81
  Calling-Station-Id          00-11-22-33-44-55
  Nas-Port                    0x0000000d (13)
  Nas-Ip-Address              0xac14e327 (-1407917273)
  NAS-Identifier              WLC5520
. . .
(Cisco Controller) > config radius auth mac-delimiter colon
(Cisco Controller) > test aaa radius username user1 password
Cisco123 wlan-id 7 apgroup default-group server-index 2


Radius Test Request
  Wlan-id..................................... 7
  ApGroup Name................................ default-group
  Attributes                  Values
  ----------                  ------
  User-Name                   user1
  Called-Station-Id           00:00:00:00:00:00:EngineeringV81
  Calling-Station-Id          00:11:22:33:44:55
  Nas-Port                    0x0000000d (13)
.......
```

Example: RADIUS Fallback

```
(Cisco Controller) > test aaa radius username user1 password Cisco123 wlan-id 7 apgroup
default-group

Radius Test Request
  Wlan-id..................................... 7
  ApGroup Name................................ default-group
```

```
  Attributes                    Values
  ----------                    ------
  User-Name                     user1
  Called-Station-Id             00:00:00:00:00:00:EngineeringV81
  Calling-Station-Id            00:11:22:33:44:55
  Nas-Port                      0x0000000d (13)
  Nas-Ip-Address                172.20.227.39
  NAS-Identifier                WLC5520
  . . .
(Cisco Controller) > test aaa show radius

Radius Test Request
  Wlan-id..................................... 7
  ApGroup Name................................ default-group
Radius Test Response
Radius Server            Retry Status
-------------            ----- ------
172.20.227.62            6     No response received from server
172.20.227.52            1     Success
Authentication Response:
  Result Code: Success
  Attributes                    Values
  ----------                    ------
  User-Name                     user1
. . .
```

Understanding Debug Client on Wireless Controllers

Use the Wireless Debug Analyzer tool to analyze the debug client output.

Deauthenticating Clients

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.

This section contains the following subsections:

Deauthenticating Clients (GUI)

Procedure

Step 1 Choose **Monitor** > **Clients**.

Step 2 On the **Clients** page, click the MAC address of the client.

Step 3 On the **Clients > Detail** page displayed, click **Remove**.

Step 4 Save the configuration.

Deauthenticating Clients (CLI)

Procedure

- **config client deauthenticate** {*mac-addr* | *ipv4-addr* | *ipv6-addr* | *user-name*}

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.

- The **debug** command enables diagnostic logging of specific events. The log output is directed to the terminal session in which the debug command is entered.
- Only one debug session at a time is active. If one terminal has debugging running, and a **debug** command is entered on another terminal, the debug session on the first terminal is terminated.
- To turn off all debugs, use the **debug disable-all** command.
- To filter the debugs based on client or AP MAC addresses, use the **debug mac addr** *mac-address* command. Up to 10 MAC addresses are supported.
- At the start of a debug session, a message is displayed indicating the following platform details for which the debug session is being started:
  - Timestamp
  - Cisco controller model
  - Cisco release version
  - Serial number
  - Hostname

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.
- **show logging config-history**: This command enhances the **show run-config** command output by displaying the following additional information:
  - List of commands executed arranged in chronological order with the timestamp.
  - User ID
  - The log of executed commands during the current and up to two previous sessions.

  The history log records commands that modified the controller configurations. The following commands are recorded in the log:

  - **config**
  - **save**
  - **transfer**
  - **upload**

- **download**
- **reset**
- **clear**

The log file is saved to the **diag_bundle/configlog/configHistory** folder in the controller.

Download the **Support Bundle** to view the commands that are executed during the current and up to two previous sessions. See the **Uploading Configuration Files** section under the **Managing Configuration** chapter.

Note The history log file is limited to 10240 entries. The oldest entry is replaced after the entries exceed 10240 entries limit from the time the controller is boot up.

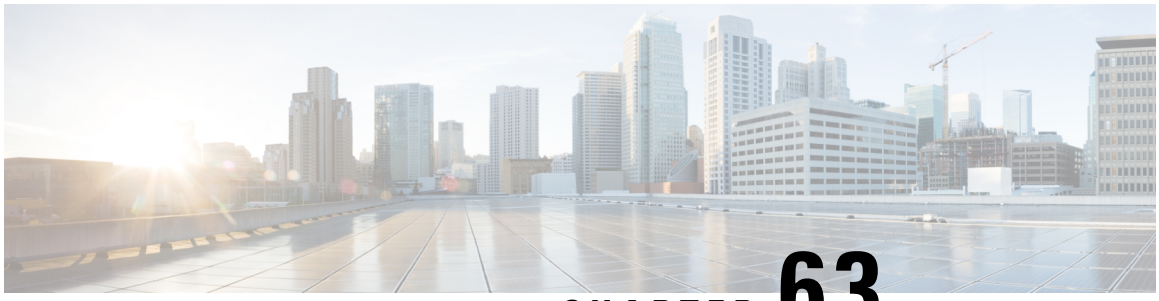
Potential Reasons for Controller Reset

This section lists all the potential reasons for a controller reset.

- User initiated reset
- Hard/Unknown reboot
- Reset due to switch-driver crash
- Reset due to DP crash
- Peer-RMI, peer-RP and management default gateway are reachable
- Both controllers are active, same timestamp, rebooting secondary controller
- Mandatory argument is missing for starting redundancy manager transport task
- Failed to create socket to communicate with peer
- Failed to create socket to communicate with peer via secondary link
- Failed bind socket to communicate with peer
- Failed bind socket to communicate with peer via secondary link
- License count was not received from primary controller
- Not reaching Hot Standby
- Standby has not received config files from Active
- Corrupted XMLs transferred from Active to Standby
- Corrupted XMLs in Active controller
- Standby TFTP failure
- New XML downloaded

- Active to Standby request
- Standby IPC failure
- Certificate installed in Standby controller
- Mandatory argument to start redundancy manager ping task is missing
- Self sanity check failed; both controllers are in maintenance state
- Self sanity check failed; in maintenance state because both controllers were active
- Self sanity check failed; current controller became Active before peer reboot
- User has initiated reset
- XML transfer was initiated but role negotiation was not done
- IPC timeout has occurred multiple times
- Role notification timeout has occurred
- Peer sanity check failed
- Active is down, Standby is not ready to take over
- Configuration out of sync
- Configuration download failure
- None of the ports is connected
- None of the local ports is connected
- Peer maintenance mode
- RF keepalive timeout
- Peer notification timeout
- Peer platform sync timeout
- Peer progression failed
- Standby default gateway is not reachable
- Active default gateway is not reachable
- Redundancy management interface and redundancy port are down
- Redundancy port is down
- Redundancy management interface is down
- Standby timeout
- Active timeout
- License count was not received from Primary controller
- XMLs were not transferred from Active to Standby
- Certificate transfer from Active to Standby failed

- Redundant pair assume same role
- Failed to create redundancy manager semaphore
- Failed to create redundancy manager keepalive task
- Failed to create redundancy manager main task
- Failed to create redundancy manager message queue
- Failed to start redundancy manager transport task
- Controller is not in proper state for more than expected time
- Mandatory argument is missing in redundancy manager main task
- Failed to create timer to send sanity messages
- Failed to create timer to send role negotiation message
- Failed to create timer to send the messages to peer
- Failed to create timer for handling max role negotiation time
- Mandatory argument to start keepalive task is missing
- Failed to create the semaphore used for sending keepalive messages
- Reset due to config download
- Watchdog reset
- Unknown reset reason



CHAPTER 63

Controller Unresponsiveness

- Upload Logs and Crash Files, on page 1299
- Uploading Core Dumps from the Controller, on page 1301
- Uploading Crash Packet Capture Files, on page 1304
- Monitoring Memory Leaks, on page 1307

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)

Procedure

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**

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)

Procedure

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

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.

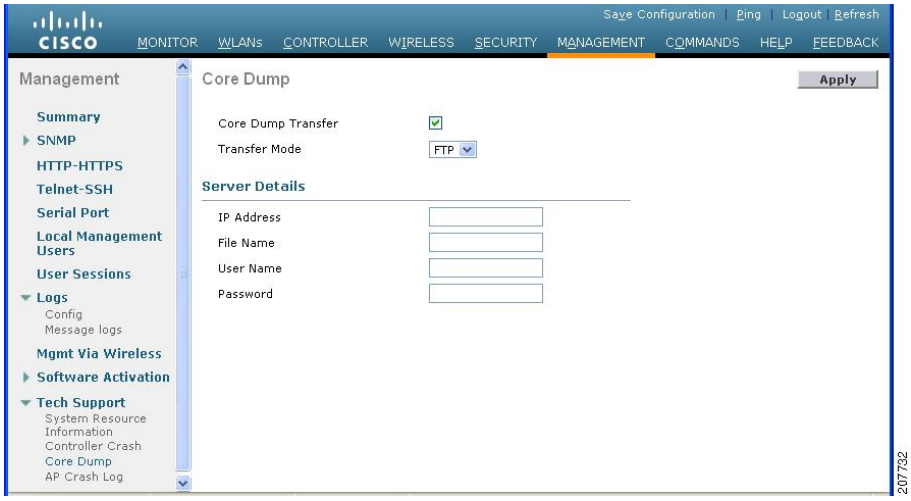
This section contains the following subsections:

Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (GUI)

Procedure

Step 1 Choose **Management** > **Tech Support** > **Core Dump** to open the Core Dump page.

Figure 85: 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)

Procedure

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)

Procedure

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 Crash 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.

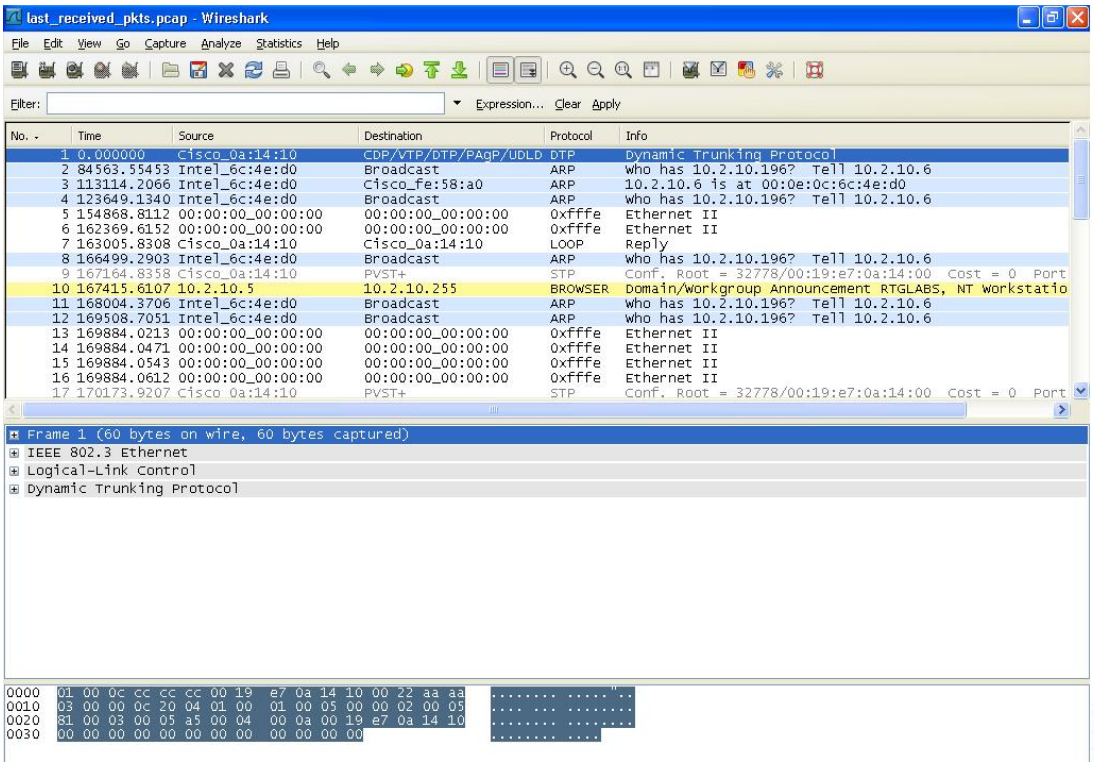
When a crash occurs, the controller generates a new packet capture file (*.pcap) file, and a message similar to the following appears in the controller crash file:

```
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 86: 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 Crash Packet Capture Files

- 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 Crash Packet Capture Files (GUI)

Procedure

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**

Step 4 In the **IP Address** field, enter the IP address of the server.

Step 5 In the **File Path** field, enter the directory path of the packet capture file.

Step 6 In the **File Name** field, 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** 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 8 Click **Upload** to upload the packet capture file from the controller. A message is displayed 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 Crash Packet Capture Files (CLI)

Procedure

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)

Procedure

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 Memory Leaks

To investigate the cause for low memory state, follow these steps:

Procedure

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*

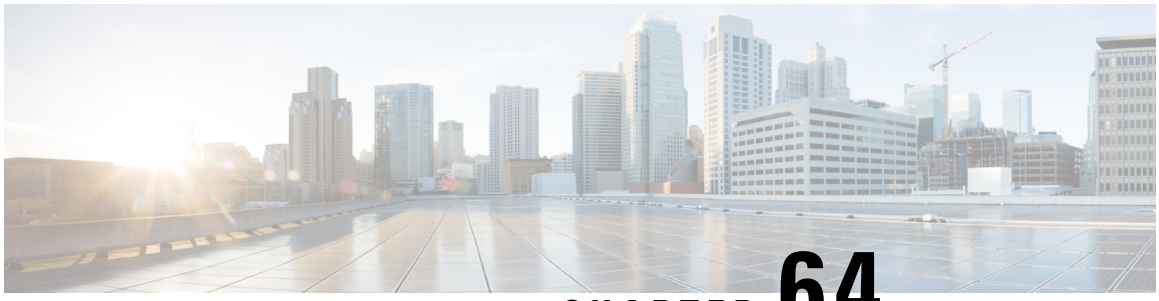
Step 5 **show system timers ticks-exhausted**

```
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.



CHAPTER 64

Debugging on Cisco Access Points

For in-depth debugging on lightweight APs, establish a terminal session into the APs. For more information about specific debugging commands, see the following documentation:

- For Wave 2 and 802.11ax APs, see https://www.cisco.com/c/en/us/td/docs/wireless/access_point/wave2-ap/command-reference/8-10/b-cisco-wave2-ap-cr-810/debug_commands.html.
- For troubleshooting wireless clients, see https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/200480-Troubleshooting-Guide-for-Wireless-Clien.html#anc52.

- Troubleshooting Access Points Using Telnet or SSH, on page 1311
- Debugging the Access Point Monitor Service, on page 1313
- Sending Commands to Access Points, on page 1313
- Understanding How Access Points Send Crash Information to the Controller, on page 1314
- Understanding How Access Points Send Radio Core Dumps to the Controller, on page 1314
- Viewing the AP Crash Log Information, on page 1316
- Viewing MAC Addresses of Access Points, on page 1317
- Disabling the Reset Button on Access Points to Lightweight Mode, on page 1318
- Viewing Access Point Event Logs, on page 1318
- Troubleshooting Clients on FlexConnect Access Points, on page 1319
- Troubleshooting OfficeExtend Access Points, on page 1320
- Link Test, on page 1321

Troubleshooting Access Points Using Telnet or SSH

The controller supports the use of the Telnet and Secure Shell (SSH) protocols to troubleshoot Cisco APs. Using these protocols makes debugging easier, especially when the AP is unable to join the controller.

- You can enable a Telnet or SSH session on unjoined access points with non default credentials.
- Telnet is not supported on Cisco Wave 2 and 802.11ax APs.

Troubleshooting Access Points Using Telnet or SSH (GUI)

Procedure

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)

Procedure

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

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.

Sending Commands to Access Points

You can enable the controller to send commands to an AP by entering this command:

debug ap {**enable** | **disable** | **command** *cmd*} *Cisco_AP*

When this feature is enabled, the controller sends commands to the AP as character strings. You can send any command supported by Cisco APs. The immediate output from the AP command is sent to the controller terminal session after pressing **Enter**; however, the output from AP debugging is not sent to the controller terminal.

Example

```
<Cisco Controller> debug ap enable AP3802i

<Cisco Controller>debug ap command "show clock" ap-name AP3802i

<Cisco Controller>*spamApTask7: May 05 16:52:05.406: a0:e0:af:f9:37:e0
AP3802i: *16:52:05 UTC Wed May 5 2021

<Cisco Controller> debug ap disable AP3802i
```

Understanding How Access Points Send Crash Information to the Controller

When an AP unexpectedly reboots, the AP 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 AP flash memory when the controller pulls it from the AP.

Understanding How Access Points Send Radio Core Dumps to the Controller

When a radio module in an AP generates a core dump, the AP 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 AP.

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 AP flash memory when the controller pulls it from the AP.

Restrictions

This feature is supported only on Cisco Wave 1 (IOS-based) and 802.11n APs.

Retrieving Radio Core Dumps (CLI)

Procedure

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

Information similar to the following appears:

```
Local Core Files:
lrad_APxxxx.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.
```

Uploading Radio Core Dumps (GUI)

Procedure

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**

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)

Procedure

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**.

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.

Restrictions

This feature is supported only on Cisco Wave 1 (IOS-based) and 802.11n APs.

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)

Procedure

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_APxxxx.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*

Viewing MAC Addresses of Access Points

There are some differences in the way that controllers show the MAC addresses of APs on information pages in the controller GUI:

- On the **AP Summary** window, the controller lists the Ethernet MAC addresses of the APs.
- On the **AP Detail** window, the controller lists the BSS MAC addresses and Ethernet MAC addresses of the APs.
- On the **Radio Summary** window, the controller lists APs by radio MAC address.

Disabling the Reset Button on Access Points to Lightweight Mode

You can disable the reset button on APs to lightweight mode. The reset button is labeled MODE on the outside of the AP.

Use this command to disable or enable the reset button on one or all APs joined to a controller:

config ap rst-button {**enable** | **disable**} {*ap-name*}

The reset button on APs is enabled by default.

Restrictions

This feature is supported only on Cisco Wave 1 (IOS-based) and 802.11n APs.

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 *ap-name*

  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 all access points or for a specific access point joined to the controller, enter this command:

  clear ap eventlog {**all** | *ap-name*}

Troubleshooting Clients on FlexConnect Access Points

FlexConnect client-based debugging allows client-specific debugging to be enabled for an AP or groups of APs. It also allows syslog server configuration to log the debug messages.

Using FlexConnect client-based debugging:

- You can debug client connectivity issue of AP by entering a particular MAC address of a client from either controller or AP console.
- You can debug client connectivity issue across FlexConnect site without entering debug commands on multiple APs or enabling multiple debugs. A single debug command enables the debugs.
- You need not enter debug command on multiple APs depending on where the client may roam to. By applying debug at the FlexConnect group level, all APs that are part of the FlexConnect group get this debug request.
- The logs are collected centrally at syslog server by providing the IP address of the server from the controller.

Note The driver debugs are not enabled on the controller. If you have access to the AP console, the driver debugs can be enabled.

Following are the debugging commands on the controller CLI:

- **debug flexconnect client ap** *ap-name* {**add** | **delete**} *mac-addr1 mac-addr2 mac-addr3 mac-addr4*
- **debug flexconnect client ap** *ap-name* **syslog** {*server-ip-address* | **disable**}
- **debug flexconnect client group** *group-name* {**add** | **delete**} *mac-addr1 mac-addr2 mac-addr3 mac-addr4*
- **debug flexconnect client group** *group-name* **syslog** {*server-ip-address* | **disable**}
- **show debug**

The debugging commands that can be entered on the AP console are listed below. These commands are applicable for debugging the client AP console when it is accessible. If you enter these commands on the AP console, the commands are not communicated to the controller.

Restrictions

- Controller High Availability is not supported.
- AP configuration is not saved across reboots.
- Adding an AP to and deleting an AP from a FlexConnect group impacts the AP's FlexConnect debug state.
- Until Release 8.5, the FlexConnect client-based debugging is supported only on Cisco Wave 1 (IOS-based) and 802.11n APs. Starting Release 8.10, the feature is supported also on Cisco Wave 2 and 802.11ax APs.

Troubleshooting OfficeExtend Access Points

This section provides troubleshooting information if you experience any problems with your OfficeExtend access points.

This section contains the following subsections:

Troubleshooting Common Problems with OfficeExtend Access Points

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.

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)

Procedure

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
```

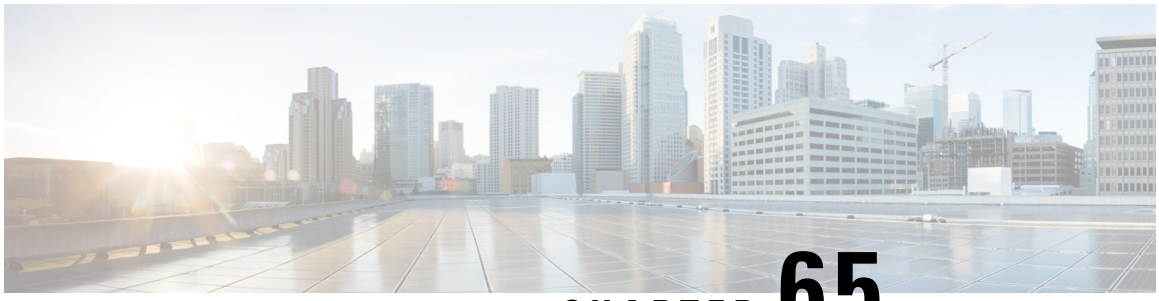
  When CCX v4 or later releases is not enabled on either the controller or the client being tested, fewer details appear:

```
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 65

Packet Capture

- Using the Debug Packet Logging Facility, on page 1325
- Wireless Sniffing, on page 1330

Using the Debug Packet Logging Facility

The debug packet logging 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)

Procedure

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 87: 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 88: 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?
```

Wireless Sniffing

The controller enables you to configure an AP 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.

For more information about wireless sniffing using Cisco APs in Sniffer mode, see https://www.cisco.com/c/en/us/support/docs/wireless-mobility/80211/200527-Fundamentals-of-802-11-Wireless-Sniffing.html#anc11.

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 controller. 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 controller. If WLAN 1 is disabled, the access point cannot send packets.
- **Issue**: AP disconnections, traffic destined to controller received using AP sniffer radio MAC address.

  Conditions: These issues are observed if APs are configured to operate in sniffer mode and controller sends sniffed traffic to configured destination. These issues impact scenarios where the controller is connected to Cisco Application Centric Infrastructure (ACI) Fabric and data gleaning is used for IP-MAC address binding.

  Workaround: Avoid using APs in sniffer mode or do not use data gleaning for IP-MAC address binding.

Configuring Sniffing on an Access Point (GUI)

Procedure

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)

Procedure

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*