Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Gibraltar 16.11.x

First Published: 2019-05-31

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)

© 2019 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface lvii

Document Conventions lvii

Related Documentation lix

Communications, Services, and Additional Information lix

Cisco Bug Search Tool lix

Documentation Feedback lix

CHAPTER 1

Overview of Cisco 9800 Series Wireless Controllers 1

Elements of the New Configuration Model 1

Configuration Workflow 2

Initial Setup 3

PART I

System Configuration 5

CHAPTER 2

System Configuration 7

Information About New Configuration Model 7

Configuring a Wireless Profile Policy (GUI) 10

Configuring a Wireless Profile Policy (CLI) 10

Configuring a Flex Profile (GUI) 11

Configuring a Flex Profile 12

Configuring an AP Profile (GUI) 13

Configuring an AP Profile (CLI) 17

Configuring User for AP Management (CLI) 18

Setting a Private Configuration Key for Password Encryption 19

Configuring an RF Profile (GUI) 20

Configuring an RF Profile (CLI) 20

Configuring a Site Tag (GUI) 21
Configuring a Site Tag (CLI) 21
Configuring Policy Tag (GUI) 23
Configuring a Policy Tag (CLI) 23
Configuring Wireless RF Tag (GUI) 24
Configuring Wireless RF Tag (CLI) 24
Attaching a Policy Tag and Site Tag to an AP (GUI) 25
Attaching Policy Tag and Site Tag to an AP (CLI) 26
AP Filter 27
Introduction to AP Filter 27
Set Tag Priority (GUI) 27
Set Tag Priority 27
Create an AP Filter (GUI) 28
Create an AP Filter (CLI) 29
Set Up and Update Filter Priority (GUI) 29
Set Up and Update Filter Priority 30
Verify AP Filter Configuration 30
Configuring Access Point for Location Configuration 31
Information About Location Configuration 31
Prerequisite for Location Configuration 32
Configuring a Location for an Access Point (GUI) 32
Configuring a Location for an Access Point (CLI) 32
Adding an Access Point to the Location (GUI) 33
Adding an Access Point to the Location (CLI) 34
Configuring SNMP in Location Configuration 34
SNMP MIB 34
Verifying Location Configuration 35
Verifying Location Statistics 35

CHAPTER 3 **RF Profile** 37
RF Tag Profiles 37
Configuring an AP Tag (GUI) 37
Configuring AP Tag (CLI) 38
Configuring RF Profile (GUI) 39

Configuring an RF Profile (CLI) 40
Configuring Wireless RF Tag (GUI) 42
Configuring Wireless RF Tag (CLI) 42

CHAPTER 4 BIOS Protection 45
BIOS Protection on the Controller 45
BIOS or ROMMON Upgrade with BIOS Protection 45
Upgrading BIOS 46

CHAPTER 5 Smart Licensing 47
Information About Cisco Smart Licensing 47
Creating a Smart Account 49
Using Smart Licensing 50
Reregister a License (GUI) 50
Using Specified License Reservation (SLR) 50
Enabling Smart Software Licensing 51
Enabling Smart Call Home Reporting 52
Configuring AIR License Level (GUI) 52
Configuring AIR License Level (CLI) 53
Configuring AIR Network Essentials License Level 53
Configuring AIR Network Advantage License Level 54
Verifying Smart Licensing Configurations 54

CHAPTER 6 Best Practices 57
Introduction 57

PART II Lightweight Access Points 59

CHAPTER 7 Country Codes 61
Information About Country Codes 61
Prerequisites for Configuring Country Codes 61
Configuring Country Codes (GUI) 62
Configuring Country Codes (CLI) 62
Configuration Examples for Configuring Country Codes 64

Viewing Channel List for Country Codes 64

CHAPTER 8 Sniffer Mode 67

Information about Sniffer 67

Prerequisites for Sniffer 67

Restrictions on Sniffer 68

How to Configure Sniffer 68

Configuring an Access Point as Sniffer (GUI) 68

Configuring an Access Point as Sniffer (CLI) 69

Enabling or Disabling Sniffing on the Access Point (GUI) 69

Enabling or Disabling Sniffing on the Access Point (CLI) 70

Verifying Sniffer Configurations 70

Examples for Sniffer Configurations and Monitoring 70

CHAPTER 9 Monitor Mode 73

Introduction to Monitor Mode 73

Enable Monitor Mode (GUI) 73

Enable Monitor Mode (CLI) 74

CHAPTER 10 Sensor Mode 75

Introduction to Sensor Mode 75

Enabling Sensor Mode 75

Verifying Sensor Mode Configuration 78

CHAPTER 11 AP Priority 79

Failover Priority for Access Points 79

Setting AP Priority (GUI) 79

Setting AP Priority 80

CHAPTER 12 FlexConnect 81

Information About FlexConnect 81

FlexConnect Authentication 83

Guidelines and Restrictions for FlexConnect 85

Configuring a Site Tag 88
Configuring a Policy Tag (CLI) 89
Attaching a Policy Tag and a Site Tag to an Access Point (GUI) 90
Attaching Policy Tag and Site Tag to an AP (CLI) 91
Linking an ACL Policy to the Defined ACL (GUI) 92
Applying ACLs on FlexConnect 92
Configuring FlexConnect 93
Configuring a Switch at a Remote Site 93
Configuring the Controller for FlexConnect 94
Configuring Local Switching in FlexConnect Mode (GUI) 95
Configuring Local Switching in FlexConnect Mode (CLI) 95
Configuring Central Switching in FlexConnect Mode (GUI) 96
Configuring Central Switching in FlexConnect Mode 96
Configuring an Access Point for FlexConnect 96
Configuring an Access Point for Local Authentication on a WLAN (GUI) 97
Configuring an Access Point for Local Authentication on a WLAN (CLI) 97
Connecting Client Devices to WLANs 97
Configuring FlexConnect Ethernet Fallback 98
Information About FlexConnect Ethernet Fallback 98
Configuring FlexConnect Ethernet Fallback 98
Flex AP Local Authentication (GUI) 99
Flex AP Local Authentication (CLI) 100
Flex AP Local Authentication with External Radius Server 102
Configuration Example: FlexConnect with Central and Local Authentication 105
NAT-PAT for FlexConnect 105
Configuring NAT-PAT for a WLAN or a Remote LAN 105
Creating a WLAN 105
Configuring a Wireless Profile Policy and NAT-PAT (GUI) 106
Configuring a Wireless Profile Policy and NAT-PAT 106
Mapping a WLAN to a Policy Profile 107
Configuring a Site Tag 108
Attaching a Policy Tag and a Site Tag to an Access Point (GUI) 108
Attaching a Policy Tag and a Site Tag to an Access Point 109
Split Tunneling for FlexConnect 109

Configuring Split Tunneling for a WLAN or Remote LAN 110
Defining an Access Control List for Split Tunneling (GUI) 110
Defining an Access Control List for Split Tunneling 110
Linking an ACL Policy to the Defined ACL 111
Creating a WLAN 112
Configuring a Wireless Profile Policy and a Split MAC ACL Name (GUI) 112
Configuring a Wireless Profile Policy and a Split MAC ACL Name 113
Mapping a WLAN to a Policy Profile (GUI) 114
Mapping WLAN to a Policy Profile 114
Configuring a Site Tag 115
Attaching a Policy Tag and Site Tag to an Access Point 115
VLAN-based Central Switching for FlexConnect 116
Configuring VLAN-based Central Switching (GUI) 116
Configuring VLAN-based Central Switching (CLI) 117
OfficeExtend Access Points for FlexConnect 118
Configuring OfficeExtend Access Points 119
Disabling OfficeExtend Access Point 119
Clearing Personal SSID from an OfficeExtend Access Point 120
Example: Viewing OfficeExtend Configuration 120
Proxy ARP 121
Enabling Proxy ARP for FlexConnect APs (GUI) 121
Enabling Proxy ARP for FlexConnect APs 121

CHAPTER 13 **Data DTLS 123**
Information About Data Datagram Transport Layer Security 123
Configuring Data DTLS (GUI) 123
Configuring Data DTLS (CLI) 124

CHAPTER 14 **Converting Autonomous Access Points to Lightweight Mode 127**
Guidelines for Converting Autonomous Access Points to Lightweight Mode 127
Information About Autonomous Access Points Converted to Lightweight Mode 128
Reverting from Lightweight Mode to Autonomous Mode 128
Using DHCP Option 43 and DHCP Option 60 128
How Converted Access Points Send Crash Information to the Device 129

Uploading Memory Core Dumps from Converted Access Points 129
Displaying MAC Addresses for Converted Access Points 129
Configuring a Static IP Address for a Lightweight Access Point 129
How to Convert a Lightweight Access Point Back to an Autonomous Access Point 130
Converting a Lightweight Access Point Back to an Autonomous Access Point (CLI) 130
Converting a Lightweight Access Point Back to an Autonomous Access Point (Using the Mode Button and a TFTP Server) 130
Authorizing Access Points 131
Authorizing Access Points Using Local Database (CLI) 131
Authorizing Access Points Using RADIUS Server (CLI) 132
Disabling the Reset Button on Converted Access Points (CLI) 134
Monitoring the AP Crash Log Information 134
How to Configure a Static IP Address on an Access Point 135
Configuring a Static IP Address on an Access Point (CLI) 135
Configuring a Static IP Address on an Access Point (GUI) 136
Recovering the Access Point Using the TFTP Recovery Procedure 137
Configuration Examples for Converting Autonomous Access Points to Lightweight Mode 137
Example: Displaying the IP Address Configuration for Access Points 137
Example: Displaying Access Point Crash File Information 137
AP MAC Authorization 138
Configuring AP MAC Authorization (CLI) 138
Ethernet VLAN Tagging on Access Points 139
Information About Ethernet VLAN Tagging on Access Points 139
Configuring Ethernet VLAN Tagging on Access Points (GUI) 139
Configuring Ethernet VLAN Tagging on Access Points (CLI) 139

CHAPTER 15 **AP Crash File Upload** 141
AP Crash File Upload 141
Configuring AP Crash File Upload (CLI) 142

CHAPTER 16 **Rogue per AP** 143
Rogue per AP 143
Enabling Rogue Detection 144
Configuring an AP Profile (GUI) 144

Configure an AP Profile 148
Define a Wireless Site Tag and Assign an AP Profile (GUI) 150
Define a Wireless Site Tag and Assign an AP Profile (CLI) 150
Associating Wireless Tag to an AP (GUI) 150
Associate Wireless Tag to an AP (CLI) 151

CHAPTER 17 **Access Point Plug-n-Play** 153
Overview of Access Point Plug-n-Play 153
Provisioning AP from PnP Server 153
Verifying AP Tag Configuration 154

CHAPTER 18 **802.11 Parameters for Cisco Access Points** 155
2.4-GHz Radio Support 155
Configuring 2.4-GHz Radio Support for the Specified Slot Number 155
5-GHz Radio Support 157
Configuring 5-GHz Radio Support for the Specified Slot Number 157
Information About Dual-Band Radio Support 160
Configuring Default XOR Radio Support 161
Configuring XOR Radio Support for the Specified Slot Number (GUI) 163
Configuring XOR Radio Support for the Specified Slot Number 163
Receiver Only Dual-Band Radio Support 165
Information About Receiver Only Dual-Band Radio Support 165
Configuring Receiver Only Dual-Band Parameters for Access Points 166
Enabling CleanAir with Receiver Only Dual-Band Radio on a Cisco Access Point (GUI) 166
Enabling CleanAir with Receiver Only Dual-Band Radio on a Cisco Access Point 166
Disabling Receiver Only Dual-Band Radio on a Cisco Access Point (GUI) 166
Disabling Receiver Only Dual-Band Radio on a Cisco Access Point 167
Configuring Client Steering (CLI) 167
Verifying Cisco Access Points with Dual-Band Radios 169

CHAPTER 19 **802.1x Support** 171
Introduction to the 802.1X Authentication 171
EAP-FAST Protocol 171
EAP-TLS/EAP-PEAP Protocol 172

Limitations of the 802.1X Authentication 172
Topology - Overview 173
Configuring 802.1X Authentication Type and LSC AP Authentication Type (GUI) 173
Configuring 802.1X Authentication Type and LSC AP Authentication Type 174
Configuring the 802.1X Username and Password (GUI) 175
Configuring the 802.1X Username and Password (CLI) 175
Enabling 802.1X on the Switch Port 176
Verifying 802.1X on the Switch Port 178
Verifying the Authentication Type 178

CHAPTER 20 **CAPWAP Link Aggregation Support** 179
Information About CAPWAP LAG Support 179
Restrictions for CAPWAP LAG Support 180
Enabling CAPWAP LAG Support on Controller (GUI) 180
Enabling CAPWAP LAG Support on Controller 180
Enabling CAPWAP LAG Globally on Controller 181
Disabling CAPWAP LAG Globally on Controller 181
Enabling CAPWAP LAG for an AP Profile (GUI) 181
Enabling CAPWAP LAG for an AP Profile 182
Disabling CAPWAP LAG for an AP Profile 182
Disabling CAPWAP LAG Support on Controller 183
Verifying CAPWAP LAG Support Configurations 183

CHAPTER 21 **DHCP and NAT Functionality on Root Access Point** 185
Information About DHCP and NAT Functionality on Root AP (RAP) 185
Configuring DHCP Server on Root Access Point (RAP) 186
Verifying DHCP Server for Root AP Configuration 186

CHAPTER 22 **Configuring Bi-Directional Rate Limiting Support with AAA Override** 187
Information About Bi-Directional Rate Limiting with AAA Override 187
Configuring Time of Day 188
Creating a Class Map 188
Creating a Policy Map 189
Creating a Service Template 190

Verifying Time of Day Configuration 191

PART III **Radio Resource Management** 193

CHAPTER 23 **Radio Resource Management** 195

Information About Radio Resource Management 195

Radio Resource Monitoring 196

Information About RF Groups 196

RF Group Leader 197

RF Group Name 199

Secure RF Groups 200

Transmit Power Control 200

Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings 200

Dynamic Channel Assignment 201

Dynamic Bandwidth Selection 203

Coverage Hole Detection and Correction 203

Restrictions for Radio Resource Management 203

How to Configure RRM 204

Configuring Neighbor Discovery Type (GUI) 204

Configuring Neighbor Discovery Type (CLI) 204

Configuring RF Groups 204

Configuring RF Group Selection Mode (GUI) 205

Configuring RF Group Selection Mode (CLI) 205

Configuring an RF Group Name (CLI) 206

Configuring Members in an 802.11 Static RF Group (GUI) 206

Configuring Members in an 802.11 Static RF Group (CLI) 207

Configuring Transmit Power Control 207

Configuring Transmit Power (GUI) 207

Configuring the Tx-Power Control Threshold (CLI) 208

Configuring the Tx-Power Level (CLI) 208

Configuring 802.11 RRM Parameters 209

Configuring Advanced 802.11 Channel Assignment Parameters (GUI) 209

Configuring Advanced 802.11 Channel Assignment Parameters (CLI) 210

Configuring 802.11 Coverage Hole Detection (GUI) 213

Configuring 802.11 Coverage Hole Detection (CLI) 213
Configuring 802.11 Event Logging (CLI) 215
Configuring 802.11 Statistics Monitoring (GUI) 215
Configuring 802.11 Statistics Monitoring (CLI) 216
Configuring the 802.11 Performance Profile (GUI) 217
Configuring the 802.11 Performance Profile (CLI) 217
Configuring Advanced 802.11 RRM 218
Enabling Channel Assignment (GUI) 218
Enabling Channel Assignment (CLI) 219
Restarting DCA Operation 219
Updating Power Assignment Parameters (GUI) 220
Updating Power Assignment Parameters (CLI) 220
Configuring Rogue Access Point Detection in RF Groups 220
Configuring Rogue Access Point Detection in RF Groups (CLI) 220
Monitoring RRM Parameters and RF Group Status 222
Monitoring RRM Parameters 222
Verifying RF Group Status (CLI) 222
Examples: RF Group Configuration 223
Information About ED-RRM 223
Configuring ED-RRM on the Cisco Wireless LAN Controller (CLI) 223

CHAPTER 24 **Coverage Hole Detection** 227
Coverage Hole Detection and Correction 227
Configuring Coverage Hole Detection (GUI) 227
Configuring Coverage Hole Detection (CLI) 228
Configuring CHD for RF Tag Profile (GUI) 230
Configuring CHD for RF Profile (CLI) 230

CHAPTER 25 **Optimized Roaming** 233
Optimized Roaming 233
Restrictions for Optimized Roaming 233
Configuring Optimized Roaming (GUI) 234
Configuring Optimized Roaming (CLI) 234

CHAPTER 26 **Cisco Flexible Radio Assignment** 237

Information About Flexible Radio Assignment 237

Benefits of the FRA 238

Configuring an FRA Radio (CLI) 238

Configuring an FRA Radio (GUI) 240

CHAPTER 27 **XOR Radio Support** 243

Information About Dual-Band Radio Support 243

Configuring Default XOR Radio Support 244

Configuring XOR Radio Support for the Specified Slot Number (GUI) 246

Configuring XOR Radio Support for the Specified Slot Number 246

CHAPTER 28 **Cisco Receiver Start of Packet** 249

Information About Receiver Start of Packet Detection Threshold 249

Restrictions for Rx SOP 249

Configuring Rx SOP (CLI) 250

Customizing RF Profile (CLI) 250

CHAPTER 29 **Client Limit** 253

Information About Client Limit 253

Configuring Client Limit Per WLAN (GUI) 253

Configuring Client Limit Per WLAN (CLI) 253

CHAPTER 30 **IP Theft** 255

Introduction to IP Theft 255

Configuring IP Theft (GUI) 256

Configuring IP Theft 256

Configuring the IP Theft Exclusion Timer 256

Adding Static Entries for Wired Hosts 257

Verifying IP Theft Configuration 258

CHAPTER 31 **Unscheduled Automatic Power Save Delivery** 261

Information About Unscheduled Automatic Power Save Delivery 261
Viewing Unscheduled Automatic Power Save Delivery (CLI) 261

CHAPTER 32 Enabling USB Port on Access Points 263
USB Port as Power Source for Access Points 263
Configuring an AP Profile (CLI) 264
Configuring USB Settings for an Access Point (CLI) 264
Monitoring USB Configurations for Access Points (CLI) 265

CHAPTER 33 Dynamic Frequency Selection 267
Information About Dynamic Frequency Selection 267
Configuring Dynamic Frequency Selection (GUI) 267
Configuring Dynamic Frequency Selection 267
Verifying DFS 268

PART IV Network Management 269

CHAPTER 34 AP Packet Capture 271
Introduction to AP Client Packet Capture 271
Enabling Packet Capture (GUI) 271
Enabling Packet Capture (CLI) 272
Create AP Packet Capture Profile and Map to an AP Join Profile (GUI) 272
Create AP Packet Capture Profile and Map to an AP Join Profile 272
Start or Stop Packet Capture 273

CHAPTER 35 DHCP Option82 275
Information About DHCP Option 82 275
Configuring DHCP Option 82 Global Interface 276
Configuring DHCP Option 82 Globally Through Server Override (CLI) 276
Configuring DHCP Option 82 Globally Through Different SVIs (GUI) 277
Configuring DHCP Option 82 Globally Through Different SVIs (CLI) 277
Configuring DHCP Option 82 Format 278
Configuring DHCP Option82 Through a VLAN Interface 279
Configuring DHCP Option 82 Through Option-Insert Command (CLI) 279

Configuring DHCP Option 82 Through the server-ID-override Command (CLI) 280
Configuring DHCP Option 82 Through a Subscriber-ID (CLI) 281
Configuring DHCP Option 82 Through server-ID-override and subscriber-ID Commands (CLI) 282
Configuring DHCP Option 82 Through Different SVIs (CLI) 283

CHAPTER 36 **RADIUS Realm** 285
Information About RADIUS Realm 285
Enabling RADIUS Realm 286
Configuring Realm to Match the RADIUS Server for Authentication and Accounting 286
Configuring the AAA Policy for a WLAN 287
Verifying the RADIUS-Realm Configuration 289

CHAPTER 37 **Cisco StadiumVision** 291
Cisco StadiumVision Overview 291
Configure Parameters for Cisco StadiumVision (GUI) 292
Configure Parameters for Cisco StadiumVision (CLI) 292
Verify StadiumVision Configurations 293

CHAPTER 38 **Persistent SSID Broadcast** 295
Persistent SSID Broadcast 295
Configuring Persistent SSID Broadcast 295
Verifying Persistent SSID Broadcast 296

CHAPTER 39 **Network Monitoring** 297
Network Monitoring 297
Status Information Received Synchronously - Configuration Examples 297
Alarm and Event Information Received Asynchronously - Configuration Examples 299

CHAPTER 40 **Creating a Lobby Ambassador Account** 301
Information About Lobby Ambassador Account 301
Creating a Lobby Ambassador User Account (GUI) 301
Creating a User Account 302
Logging In Using the Lobby Account 303

Creating a Lobby Ambassador Account (CLI) 303

CHAPTER 41 Guest User Accounts 305

Information About Creating Guest User Accounts 305

Creating a Guest User Account (GUI) 305

Creating a Guest User Account (CLI) 306

Verifying Guest User Account 307

Assigning Username to Guest Users in a WLAN (CLI) 308

PART V System Management 309

CHAPTER 42 Network Mobility Services Protocol 311

Information About Network Mobility Services Protocol 311

Radioactive Tracing for NMSP 312

Enabling NMSP on Premises Services 312

Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues 313

Modifying the NMSP Notification Threshold for Clients, RFID Tags, and Rogues 313

Configuring NMSP Strong Cipher 314

Verifying NMSP Settings 314

Examples: NMSP Settings Configuration 317

NMSP by AP Groups with Subscription List from CMX 317

Verifying NMSP by AP Groups with Subscription List from CMX 317

Probe RSSI Location 319

Configuring Probe RSSI 319

RFID Tag Support 321

Configuring RFID Tag Support 321

Verifying RFID Tag Support 322

CHAPTER 43 Application Visibility and Control 325

Information About Application Visibility and Control 325

Prerequisites for Application Visibility and Control 327

Restrictions for Application Visibility and Control 327

AVC Configuration Overview 327

Create a Flow Monitor 328

Configuring a Flow Monitor (GUI) 330
Create a Flow Record 330
Create a Flow Exporter 332
Configuring a Policy Tag 333
Attaching a Policy Profile to a WLAN Interface (GUI) 334
Attaching a Policy Profile to a WLAN Interface (CLI) 334
Attaching a Policy Profile to an AP 335
Verify the AVC Configuration 336
Default DSCP on AVC 337
Configuring Default DSCP for AVC Profile (GUI) 337
Configuring Default DSCP for AVC Profile 337
Creating Class Map 337
Creating Policy Map 338
AVC-Based Selective Reanchoring 339
Restrictions for AVC-Based Selective Reanchoring 340
Configuring the Flow Exporter 340
Configuring the Flow Monitor 340
Configuring the AVC Reanchoring Profile 341
Configuring the Wireless WLAN Profile Policy 342
Verifying AVC Reanchoring 343

CHAPTER 44 **Cisco Hyperlocation** 347
Information About Cisco Hyperlocation 347
Restrictions on Cisco Hyperlocation 349
Configuring Cisco Hyperlocation (GUI) 350
Configuring Cisco Hyperlocation (CLI) 350
Configuring Hyperlocation BLE Beacon Parameters for AP (GUI) 351
Configuring Hyperlocation BLE Beacon Parameters for AP (CLI) 352
Configuring Hyperlocation BLE Beacon Parameters (CLI) 352
Verifying Cisco Hyperlocation 353
Verifying Hyperlocation BLE Beacon Configuration 356
Verifying Hyperlocation BLE Beacon Configuration for AP 356

CHAPTER 45 **BLE Beacons in CiscoWave 2 Access Points** 359

Managing BLE Beacons in Cisco Wave 2 and 802.11ax Access Points 359
Monitoring BLE Management 361

CHAPTER 46 Cisco Connected Mobile Experiences Cloud 363
Configuring Cisco CMX Cloud 363
Verifying Cisco CMX Cloud Configuration 364

CHAPTER 47 EDCA Parameters 367
Enhanced Distributed Channel Access Parameters 367
Configuring EDCA Parameters (GUI) 367
Configuring EDCA Parameters (CLI) 368

CHAPTER 48 802.11 parameters and Band Selection 371
Information About Configuring Band Selection, 802.11 Bands, and Parameters 371
Band Select 371
802.11 Bands 372
802.11n Parameters 372
802.11h Parameters 372
Restrictions for Band Selection, 802.11 Bands, and Parameters 373
How to Configure 802.11 Bands and Parameters 373
Configuring Band Selection (GUI) 373
Configuring Band Selection (CLI) 374
Configuring the 802.11 Bands (GUI) 375
Configuring the 802.11 Bands (CLI) 376
Configuring a Band-Select RF Profile (GUI) 378
Configuring a Band-Select RF Profile (CLI) 378
Configuring 802.11n Parameters (GUI) 379
Configuring 802.11n Parameters (CLI) 380
Configuring 802.11h Parameters (CLI) 382
Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters 383
Verifying Configuration Settings Using Band Selection and 802.11 Bands Commands 383
Example: Viewing the Configuration Settings for the 5-GHz Band 383
Example: Viewing the Configuration Settings for the 2.4-GHz Band 385
Example: Viewing the status of 802.11h Parameters 386

Example: Verifying the Band-Selection Settings 387
Configuration Examples for Band Selection, 802.11 Bands, and Parameters 388
Examples: Band Selection Configuration 388
Examples: 802.11 Bands Configuration 389
Examples: 802.11n Configuration 389
Examples: 802.11h Configuration 390

CHAPTER 49 **Predownloading an Image to an Access Point** 391
Information About Predownloading an Image to an Access Point 391
Restrictions for Predownloading an Image to an Access Point 391
Predownloading an Image to Access Points (CLI) 392
Monitoring the Access Point Predownload Process 393

CHAPTER 50 **Efficient Image Upgrade** 395
Efficient Image Upgrade 395
Enable Pre-Download (GUI) 395
Enable Pre-Download (CLI) 396
Configuring a Site Tag (CLI) 396
Attaching Policy Tag and Site Tag to an AP (CLI) 397
Trigger Predownload to a Site Tag 398

CHAPTER 51 **N+1 Hitless Rolling AP Upgrade** 401
N+1 Hitless Rolling AP Upgrade 401
Configuring Hitless Upgrade 402
Verifying Hitless Upgrade 403

CHAPTER 52 **Wireless Sub-Package for Switch** 405
Introduction to Wireless Sub-package 405
Booting in Install Mode 406
Installing Sub-Package in a Single Step (GUI) 407
Installing Sub-Package in a Single Step 407
Multi-step Installation of Sub-Package 408
Installing on a Stack 409
Upgrading to a Newer Version of Wireless Package 409

Deactivating the Wireless Package 409
Enabling or Disabling Auto-Upgrade 410

CHAPTER 53 NBAR Protocol Discovery 411
Introduction to NBAR Protocol Discovery 411
Configuring NBAR Protocol Discovery 411
Verifying Protocol Discovery Statistics 412

CHAPTER 54 NBAR Dynamic Protocol Pack Upgrade 413
NBAR Dynamic Protocol Pack Upgrade 413
Upgrading the NBAR2 Protocol Pack 414

CHAPTER 55 Conditional Debug, Radioactive Tracing, and Packet Tracing 415
Introduction to Conditional Debugging 415
Introduction to Radioactive Tracing 416
Conditional Debugging and Radioactive Tracing 416
Location of Tracefiles 417
Configuring Conditional Debugging (GUI) 417
Configuring Conditional Debugging 418
Radioactive Tracing for L2 Multicast 419
Recommended Workflow for Trace files 419
Copying Tracefiles Off the Box 420
Configuration Examples for Conditional Debugging 420
Verifying Conditional Debugging 421
Example: Verifying Radioactive Tracing Log for SISF 421
Information About Packet Tracing 422
Configuring Conditional Debugging Packet Tracing 423
Configuring Conditional Debugging Packet Tracing per AP 424
Configuring Conditional Debugging Packet Tracing per Client (GUI) 425
Configuring Conditional Debugging Packet Tracing per Client 425
Verifying Conditional Debugging Packet Tracing Configuration 425

CHAPTER 56 Aggressive Client Load Balancing 427
Information About Aggressive Client Load Balancing 427

Enabling Aggressive Client Load Balancing (GUI) 428
Configuring Aggressive Client Load Balancing (GUI) 428
Configuring Aggressive Client Load Balancing (CLI) 429

CHAPTER 57 Accounting Identity List 431
Configuring Accounting Identity List (GUI) 431
Configuring Accounting Identity List (CLI) 431
Configuring Client Accounting (GUI) 432
Configuring Client Accounting (CLI) 432

CHAPTER 58 Wireless Multicast 435
Information About Wireless Multicast 435
Multicast Optimization 436
IPv6 Global Policies 436
Information About IPv6 Snooping 436
IPv6 Neighbor Discovery Inspection 436
Prerequisites for Configuring Wireless Multicast 438
Restrictions on Configuring Wireless Multicast 439
Restrictions for IPv6 Snooping 439
Configuring Wireless Multicast 439
Configuring Wireless Multicast-MCMC Mode (CLI) 439
Configuring Wireless Multicast-MCUC Mode 439
Configuring Multicast Listener Discovery Snooping (GUI) 440
Configuring IPv6 MLD Snooping 440
Verifying the Multicast VLAN Configuration 441
IPv6 Multicast-over-Multicast 441
Configuring IPv6 Multicast-over-Multicast (GUI) 442
Configuring IPv6 Multicast-over-Multicast 442
Verifying IPv6 Multicast-over-Multicast 443
Verifying the Multicast Connection Between the Controller and the AP 443
Directed Multicast Service 443
Configuring Directed Multicast Service(GUI) 444
Configuring Directed Multicast Service 444
Verifying the Directed Multicast Service Configuration 445

Wireless Broadcast, Non-IP Multicast and Multicast VLAN 446
Configuring Non-IP Wireless Multicast (CLI) 446
Configuring Wireless Broadcast (GUI) 447
Configuring Wireless Broadcast (CLI) 447
Configuring Multicast-over-Multicast for AP Multicast Groups (CLI) 448
Verifying Wireless Multicast 448
Multicast Optimization 449
Configuring IP Multicast VLAN for WLAN (GUI) 450
Configuring IP Multicast VLAN for WLAN 450
Verifying the Multicast VLAN Configuration 451
Multicast Filtering 452
Information About Multicast Filtering 452
Configuring Multicast Filtering 452
Verifying Multicast Filtering 452

CHAPTER 59 **Map-Server Per-Site Support** 455
Information About Map Server Per Site Support 455
Configuring the Default Map Server (GUI) 456
Configuring the Default Map Server (CLI) 456
Configuring a Map Server Per Site (GUI) 457
Configuring a Map Server Per Site (CLI) 457
Creating a Map Server for Each VNID (GUI) 458
Creating a Map Server for Each VNID 458
Creating a Fabric Profile and Associating a Tag and VNID (GUI) 459
Creating a Fabric Profile and Associating a Tag and VNID (CLI) 459
Verifying the Map Server Configuration 460

CHAPTER 60 **Volume Metering** 463
Configuring Volume Metering 463

CHAPTER 61 **Enabling Syslog Messages in Access Points and Controller for Syslog Server** 465
Information About Enabling Syslog Messages in Access Points and Controller for Syslog Server 465
Configuring Syslog Server for an AP Profile 466
Configuring Syslog Server for the Controller (GUI) 468

Configuring Syslog Server for the Controller 468
Verifying Syslog Server Configurations 470

CHAPTER 62 Software Maintenance Upgrade 475
Introduction to Software Maintenance Upgrade 475
Installing a SMU (GUI) 477
Installing SMU 478
Roll Back an Image (GUI) 479
Rollback SMU 479
Deactivate SMU 479
Configuration Examples for SMU 480
Information About AP Device Package 480
Installing AP Device Package (GUI) 481
Installing AP Device Package (CLI) 482
Verifying APDP on the Controller 483
Information About Per Site or Per AP Model Service Pack (APSP) 483
Rolling AP Upgrade 484
Rolling AP Upgrade Process 484
Installing AP Service Package (GUI) 485
Installing AP Service Package (CLI) 486
Adding a Site to a Filter 487
Deactivating an Image 487
Roll Back APSP 488
Canceling the Upgrade 488
Verifying the Upgrade 489
Verifying of AP Upgrade on the Controller 490

PART VI Security 493

CHAPTER 63 IPv4 ACLs 495
Information about Network Security with ACLs 495
ACL Overview 495
Access Control Entries 495
ACL Supported Types 496

Supported ACLs 496
ACL Precedence 496
Port ACLs 496
Router ACLs 497
ACEs and Fragmented and Unfragmented Traffic 498
ACEs and Fragmented and Unfragmented Traffic Examples 498
Standard and Extended IPv4 ACLs 499
IPv4 ACL Switch Unsupported Features 499
Access List Numbers 499
Numbered Standard IPv4 ACLs 500
Numbered Extended IPv4 ACLs 501
Named IPv4 ACLs 501
ACL Logging 502
Hardware and Software Treatment of IP ACLs 502
IPv4 ACL Interface Considerations 503
Restrictions for Configuring IPv4 Access Control Lists 503
How to Configure ACLs 504
Configuring IPv4 ACLs (GUI) 504
Configuring IPv4 ACLs 504
Creating a Numbered Standard ACL (GUI) 505
Creating a Numbered Standard ACL (CLI) 505
Creating a Numbered Extended ACL (GUI) 507
Creating a Numbered Extended ACL (CLI) 507
Creating Named Standard ACLs (GUI) 511
Creating Named Standard ACLs 511
Creating Extended Named ACLs (GUI) 513
Creating Extended Named ACLs 513
Applying an IPv4 ACL to an Interface (GUI) 515
Applying an IPv4 ACL to an Interface (CLI) 515
Applying ACL to Policy Profile (GUI) 516
Applying ACL to Policy Profile 516
Configuration Examples for ACLs 517
Examples: Including Comments in ACLs 517
Examples: Applying an IPv4 ACL to a Policy Profile in a Wireless Environment 517

IPv4 ACL Configuration Examples 518
ACLs in a Small Networked Office 518
Examples: ACLs in a Small Networked Office 519
Example: Numbered ACLs 519
Examples: Extended ACLs 520
Examples: Named ACLs 520
Monitoring IPv4 ACLs 521

CHAPTER 64 DNS-Based Access Control Lists 523
Information About DNS-Based Access Control Lists 523
Defining ACLs 524
Applying ACLs 524
Types of URL Filters 525
Restrictions on DNS-Based Access Control Lists 526
Flex Mode 527
Applying URL Filter List to Flex Profile 527
Configuring ISE for Central Web Authentication (GUI) 527
Local Mode 528
Defining URL Filter List 528
Applying URL Filter List to Policy Profile (GUI) 529
Applying URL Filter List to Policy Profile 530
Configuring ISE for Central Web Authentication 530
Creating Authorization Profiles 530
Mapping Authorization Profiles to Authentication Rule 531
Mapping Authorization Profiles to Authorization Rule 531
Viewing DNS-Based Access Control Lists 532
Configuration Examples for DNS-Based Access Control Lists 532
Verifying DNS Snoop Agent (DSA) 533
Information About Flex Client IPv6 Support with WebAuth Pre and Post ACL 535
Enabling Pre-Authentication ACL for LWA and EWA (GUI) 536
Enabling Pre-Authentication ACL for LWA and EWA 536
Enabling Post-Authentication ACL for LWA and EWA (GUI) 538
Enabling Post-Authentication ACL for LWA and EWA 538
Enabling DNS ACL for LWA and EWA (GUI) 538

Enabling DNS ACL for LWA and EWA 539
Verifying Flex Client IPv6 Support with WebAuth Pre and Post ACL 539

CHAPTER 65 **Allowed List of Specific URLs** 541
Allowed List of Specific URLs 541
Adding URL to Allowed List 541
Verifying URLs on the Allowed List 543

CHAPTER 66 **Web-Based Authentication** 545
Local Web Authentication Overview 545
Device Roles 547
Authentication Process 548
Local Web Authentication Banner 548
Customized Local Web Authentication 551
Guidelines 551
Redirection URL for Successful Login Guidelines 553
How to Configure Local Web Authentication 553
Configuring Default Local Web Authentication 553
Configuring AAA Authentication (GUI) 553
Configuring AAA Authentication (CLI) 554
Configuring the HTTP/HTTPS Server (GUI) 555
Configuring the HTTP Server (CLI) 555
Creating a Parameter Map (GUI) 556
Creating Parameter Maps 557
Configuring Local Web Authentication (GUI) 557
Configuring the Internal Local Web Authentication (CLI) 558
Configuring the Customized Local Web Authentication (CLI) 558
Configuring the External Local Web Authentication (CLI) 560
Configuring the Web Authentication WLANs 561
Configuring Pre-Auth Web Authentication ACL (GUI) 562
Configuring Pre-Auth Web Authentication ACL (CLI) 562
Configuring the Maximum Web Authentication Request Retries 564
Configuring a Local Banner in Web Authentication Page (GUI) 564
Configuring a Local Banner in Web Authentication Page (CLI) 565

Configuring Type WebAuth, Consent, or Both 565
Configuring Preauthentication ACL 566
Configuring TrustPoint for Local Web Authentication 567
Configuration Examples for Local Web Authentication 568
Example: Obtaining Web Authentication Certificate 568
Example: Displaying a Web Authentication Certificate 569
Example: Choosing the Default Web Authentication Login Page 570
Example: Choosing a Customized Web Authentication Login Page from an IPv4 External Web Server 570
Example: Choosing a Customized Web Authentication Login Page from an IPv6 External Web Server 571
Example: Assigning Login, Login Failure, and Logout Pages per WLAN 571
Example: Configuring Preauthentication ACL 571
Example: Configuring Webpassthrough 572
Verifying Web Authentication Type 572
External Web Authentication (EWA) 573
Configuring EWA with Single WebAuth Server Address and Default Ports (80/443) (CLI) 573
Configuring EWA with Multiple Web Servers and/or Ports Different than Default (80/443) 575
Configuring Wired Guest EWA with Multiple Web Servers and/or Ports Different than Default (80/443) 577
Authentication for Sleeping Clients 578
Information About Authenticating Sleeping Clients 578
Restrictions on Authenticating Sleeping Clients 578
Configuring Authentication for Sleeping Clients (GUI) 579
Configuring Authentication for Sleeping Clients (CLI) 579

CHAPTER 67 **Central Web Authentication** 581
Information About Central Web Authentication 581
Prerequisites for Central Web Authentication 582
How to Configure ISE 582
Creating an Authorization Profile 582
Creating an Authentication Rule 583
Creating an Authorization Rule 583
How to Configure Central Web Authentication on the Controller 584

Configuring WLAN (GUI) 584
Configuring WLAN (CLI) 585
Configuring Policy Profile (CLI) 586
Configuring a Policy Profile (GUI) 588
Creating Redirect ACL 588
Configuring AAA for Central Web Authentication 589
Configuring Redirect ACL in Flex Profile (GUI) 590
Configuring Redirect ACL in Flex Profile (CLI) 591
Authentication for Sleeping Clients 591
Information About Authenticating Sleeping Clients 591
Restrictions on Authenticating Sleeping Clients 592
Configuring Authentication for Sleeping Clients (GUI) 592
Configuring Authentication for Sleeping Clients (CLI) 593

CHAPTER 68 ISE Simplification and Enhancements 595
Utilities for Configuring Security 595
Configuring Multiple Radius Servers 596
Verifying AAA and Radius Server Configurations 597
Configuring Captive Portal Bypassing for Local and Central Web Authentication 597
Information About Captive Bypassing 597
Configuring Captive Bypassing for WLAN in LWA and CWA (GUI) 598
Configuring Captive Bypassing for WLAN in LWA and CWA (CLI) 599
Sending DHCP Options 55 and 77 to ISE 600
Information about DHCP Option 55 and 77 600
Configuration to Send DHCP Options 55 and 77 to ISE (GUI) 600
Configuration to Send DHCP Options 55 and 77 to ISE (CLI) 600
Configuring EAP Request Timeout (GUI) 601
Configuring EAP Request Timeout 602
Configuring EAP Request Timeout in Wireless Security (CLI) 602
Captive Portal 603
Captive Portal Configuration 603
Configuring Captive Portal (GUI) 603
Configuring Captive Portal 604
Captive Portal Configuration - Example 606

CHAPTER 69 **Authentication and Authorization Between Multiple RADIUS Servers** 609

Information About Authentication and Authorization Between Multiple RADIUS Servers 609

Configuring 802.1X Security for WLAN with Split Authentication and Authorization Servers 610

Configuring Explicit Authentication and Authorization Server List (GUI) 610

Configuring Explicit Authentication Server List (GUI) 611

Configuring Explicit Authentication Server List (CLI) 611

Configuring Explicit Authorization Server List (GUI) 612

Configuring Explicit Authorization Server List (CLI) 613

Configuring Authentication and Authorization List for 802.1X Security (GUI) 614

Configuring Authentication and Authorization List for 802.1X Security 614

Configuring Web Authentication for WLAN with Split Authentication and Authorization Servers 615

Configuring Authentication and Authorization List for Web Authentication (GUI) 615

Configuring Authentication and Authorization List for Web Authentication 616

Verifying Split Authentication and Authorization Configuration 617

Configuration Examples 618

CHAPTER 70 **AAA Dead-Server Detection** 619

Information About AAA Dead-Server Detection 619

Prerequisites for AAA Dead-Server Detection 620

Restrictions for AAA Dead-Server Detection 620

Configuring AAA Dead-Server Detection (CLI) 620

Verifying AAA Dead-Server Detection 621

CHAPTER 71 **RADIUS Server Load Balancing** 623

Information About RADIUS Server Load Balancing 623

Prerequisites for RADIUS Server Load Balancing 625

Restrictions for RADIUS Server Load Balancing 625

Enabling Load Balancing for a Named RADIUS Server Group (CLI) 625

CHAPTER 72 **Secure LDAP** 627

Information About SLDAP 627

Prerequisite for Configuring SLDAP 629

Restrictions for Configuring SLDAP 629

Configuring SLDAP 629
Configuring an AAA Server Group (GUI) 630
Configuring a AAA Server Group 631
Configuring Search and Bind Operations for an Authentication Request 632
Configuring a Dynamic Attribute Map on an SLDAP Server 633
Verifying the SLDAP Configuration 633

CHAPTER 73 RADIUS DTLS 635
Information About RADIUS DTLS 635
Prerequisites 637
Configuring RADIUS DTLS Server 637
Configuring RADIUS DTLS Connection Timeout 638
Configuring RADIUS DTLS Idle Timeout 638
Configuring Source Interface for RADIUS DTLS Server 639
Configuring RADIUS DTLS Port Number 640
Configuring RADIUS DTLS Connection Retries 640
Configuring RADIUS DTLS Trustpoint 641
Configuring DTLS Dynamic Author 642
Enabling DTLS for Client 642
Configuring Client Trustpoint for DTLS 643
Configuring DTLS Idle Timeout 644
Configuring Server Trustpoint for DTLS 644
Verifying the RADIUS DTLS Server Configuration 645
Clearing RADIUS DTLS Specific Statistics 645

CHAPTER 74 Internet Protocol Security 647
Information about Internet Protocol Security 647
Internet Key Exchange Version 1 Transform Sets 648
Configure IPSec Using Internet Key Exchange Version 1 649
Internet Key Exchange Version 2 Transform Sets 651
Configure IPSec Using Internet Key Exchange Version 2 652
IPsec Transforms and Lifetimes 654
Use of X.509 With Internet Key Exchange Version 655
For IKEv2 Commands 656

IPsec Session Interuption and Recovery 656
Example: Configure IPSec Using ISAKMP 657
Verifying IPSec Traffic 657
Example: Configure IPSec Using Internet Key Exchange Version 2 658
Verifying IPSec With Internet Key Exchange Version 2 Traffic 659

CHAPTER 75 **MAC Filtering** 663
MAC Filtering 663
MAC Filtering Configuration Guidelines 663
Configuring MAC Filtering for Local Authentication (CLI) 664
Configuring MAC Filtering (GUI) 666
Configuring MAB for External Authentication (CLI) 666

CHAPTER 76 **IP Source Guard** 669
Information About IP Source Guard 669
Configuring IP Source Guard (GUI) 669
Configuring IP Source Guard 670

CHAPTER 77 **Managing Rogue Devices** 671
Rogue Detection 671
Rogue Devices 671
AP Impersonation Detection 673
Configuring Rogue Detection (GUI) 673
Configuring Rogue Detection (CLI) 674
Configuring RSSI Deviation Notification Threshold for Rogue APs (CLI) 675
Configuring Management Frame Protection (GUI) 675
Configuring Management Frame Protection (CLI) 676
Verifying Management Frame Protection 676
Verifying Rogue Events 677
Verifying Rogue Detection 678
Examples: Rogue Detection Configuration 679
Configuring Rogue Policies (GUI) 680
Configuring Rogue Policies (CLI) 680
Rogue Location Discovery Protocol (RLDP) 681

Rogue Location Discovery Protocol 681
Configuring RLDP for Generating Alarms (GUI) 683
Configuring an RLDP for Generating Alarms (CLI) 684
Configuring a Schedule for RLDP (GUI) 684
Configuring a Schedule for RLDP (CLI) 685
Configuring an RLDP for Auto-Contain (GUI) 685
Configuring an RLDP for Auto-Contain (CLI) 686
Configuring RLDP Retry Times on Rogue Access Points (GUI) 686
Configuring RLDP Retry Times on Rogue Access Points (CLI) 687
Verifying Rogue AP RLDP 687
Rogue Detection Security Level 687
Setting Rogue Detection Security-level 688
Wireless Service Assurance Rogue Events 689
Monitoring Wireless Service Assurance Rogue Events 690

CHAPTER 78 **Classifying Rogue Access Points** 691
Information About Classifying Rogue Access Points 691
Guidelines and Restrictions for Classifying Rogue Access Points 693
How to Classify Rogue Access Points 693
Classifying Rogue Access Points and Clients Manually (GUI) 693
Classifying Rogue Access Points and Clients Manually (CLI) 694
Configuring Rogue Classification Rules (GUI) 695
Configuring Rogue Classification Rules (CLI) 696
Monitoring Rogue Classification Rules 699
Examples: Classifying Rogue Access Points 699

CHAPTER 79 **Configuring Secure Shell** 701
Information About Configuring Secure Shell 701
SSH and Device Access 701
SSH Servers, Integrated Clients, and Supported Versions 701
SSH Configuration Guidelines 702
Secure Copy Protocol Overview 702
Secure Copy Protocol 703
SFTP Support 703

Prerequisites for Configuring Secure Shell 703
Restrictions for Configuring Secure Shell 704
How to Configure SSH 704
Setting Up the Device to Run SSH 704
Configuring the SSH Server 705
Monitoring the SSH Configuration and Status 707

CHAPTER 80 Private Shared Key 709
Information About Private Preshared Key 709
Configuring a PSK in a WLAN (CLI) 710
Configuring a PSK in a WLAN (GUI) 711
Applying a Policy Profile to a WLAN (GUI) 712
Applying a Policy Profile to a WLAN (CLI) 712
Verifying a Private PSK 713

CHAPTER 81 Multi-Preshared Key 717
Information About Multi-Preshared Key 717
Restrictions on Multi-PSK 718
Configuring Multi-Preshared Key (GUI) 718
Configuring Multi-Preshared Key (CLI) 721
Verifying Multi-PSK Configurations 722

CHAPTER 82 Multiple Authentications for a Client 725
Information About Multiple Authentications for a Client 725
Information About Supported Combination of Authentications for a Client 725
Configuring Multiple Authentications for a Client 726
Configuring WLAN for 802.1X and Local Web Authentication (GUI) 726
Configuring WLAN for 802.1X and Local Web Authentication (CLI) 726
Configuring WLAN for Preshared Key (PSK) and Local Web Authentication (GUI) 728
Configuring WLAN for Preshared Key (PSK) and Local Web Authentication 728
Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication (GUI) 730
Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication 730
Configuring WLAN 730

Applying Policy Profile to a WLAN 731
Verifying Multiple Authentication Configurations 732

CHAPTER 83 Cisco TrustSec 737
Information about Cisco TrustSec 737
Cisco TrustSec Features 738
Security Group Access Control List 740
Inline Tagging 741
Policy Enforcement 741
SGACL Support for Wireless Guest Access 742
Enabling SGACL on the AP (GUI) 742
Enabling SGACL on the AP 743
Enabling SGACL Policy Enforcement Globally (CLI) 744
Enabling SGACL Policy Enforcement Per Interface (CLI) 745
Manually Configure a Device SGT (CLI) 745
Configuring SGACL, Inline Tagging, and SGT in Local Mode (GUI) 746
Configuring SGACL, Inline Tagging, and SGT in Local Mode 746
Configuring ISE for TrustSec 747
Verifying Cisco TrustSec Configuration 748

CHAPTER 84 SGT Inline Tagging and SXPv4 751
Introduction to SGT Inline Tagging on AP and SXPv4 751
Creating an SXP Profile 751
Configuring SGT Inline Tagging on Access Points 752
Configuring an SXP Connection (GUI) 752
Configuring an SXP Connection 753
Verifying SGT Push to Access Points 754

CHAPTER 85 Locally Significant Certificates 757
Information About Locally Significant Certificates 757
Certificate Provisioning in Controllers 758
Device Certificate Enrollment Operation 758
Certificate Provisioning on Lightweight Access Point 758
Restrictions for Locally Significant Certificates 759

Provisioning Locally Significant Certificates 759
Configuring RSA Key for PKI Trustpoint 759
Configuring PKI Trustpoint Parameters 760
Authenticating and Enrolling a PKI Trustpoint (GUI) 761
Authenticating and Enrolling the PKI Trustpoint with CA Server (CLI) 761
Configuring AP Join Attempts with LSC Certificate (GUI) 763
Configuring AP Join Attempts with LSC Certificate (CLI) 763
Configuring Subject-Name Parameters in LSC Certificate 763
Configuring Key Size for LSC Certificate 764
Configuring Trustpoint for LSC Provisioning on an Access Point 764
Configuring an AP LSC Provision List (GUI) 765
Configuring an AP LSC Provision List (CLI) 766
Configuring LSC Provisioning for all the APs (GUI) 766
Configuring LSC Provisioning for All APs (CLI) 767
Configuring LSC Provisioning for the APs in the Provision List 767
Verifying LSC Configuration 768
Configuring Management Trustpoint to LSC (GUI) 769
Configuring Management Trustpoint to LSC (CLI) 769

CHAPTER 86 **Cisco Umbrella WLAN 771**
Information About Cisco Umbrella WLAN 771
Registering Controller to Cisco Umbrella Account 772
Configuring Cisco Umbrella WLAN 773
Importing CA Certificate to the Trust Pool 773
Creating a Local Domain RegEx Parameter Map 774
Configuring Parameter Map Name in WLAN (GUI) 775
Configuring the Umbrella Parameter Map 775
Enabling or Disabling DNScrypt (GUI) 776
Enabling or Disabling DNScrypt 776
Configuring Timeout for UDP Sessions 777
Configuring Parameter Map Name in WLAN (GUI) 778
Configuring Parameter Map Name in WLAN 778
Verifying the Cisco Umbrella Configuration 778

CHAPTER 87 FIPS 781

FIPS 781
Guidelines and Restrictions for FIPS 781
FIPS Self-Tests 782
Configuring FIPS 783
Configuring FIPS in HA Setup 783
Monitoring FIPS 784
CC 785
Information About Common Criteria 785
Configuring Common Criteria 785
Verifying CC Configuration 786
Check Points for CC Mode Operation 786

PART VII Mobility 789

CHAPTER 88 Mobility 791

Introduction to Mobility 791
SDA Roaming 794
Definitions of Mobility-related Terms 795
Mobility Groups 795
Guidelines and Restrictions 796
Configuring Mobility (GUI) 798
Configuring Mobility (CLI) 799
Configuring Inter-Release Controller Mobility (GUI) 801
Configuring Inter-Release Controller Mobility 801
Verifying Mobility 805

CHAPTER 89 Static IP Client Mobility 811

Information About Static IP Client Mobility 811
Restrictions 811
Configuring Static IP Client Mobility (GUI) 812
Configuring Static IP Client Mobility (CLI) 812
Verifying Static IP Client Mobility 813

PART VIII **High Availability** 815

CHAPTER 90 **High Availability** 817

Feature History for High Availability 817

Information About High Availability 817

Prerequisites for High Availability 818

Restrictions on High Availability 819

Configuring High Availability (CLI) 820

Disabling High Availability 822

System and Network Fault Handling 822

Verifying High Availability Configurations 828

Verifying AP or Client SSO Statistics 829

Verifying High Availability 831

PART IX **Quality of Service** 835

CHAPTER 91 **Quality of Service** 837

Wireless QoS Overview 837

Wireless QoS Targets 837

SSID Policies 838

Client Policies 838

Supported QoS Features on Wireless Targets 838

Wireless QoS Mobility 839

Precious Metal Policies for Wireless QoS 839

Prerequisites for Wireless QoS 840

Restrictions for QoS on Wireless Targets 840

Metal Policy Format 841

Metal Policy Format 841

Auto QoS Policy Format 845

Architecture for Voice, Video and Integrated Data (AVVID) 847

How to apply Bi-Directional Rate Limiting 848

Information about Bi-Directional Rate Limiting 848

Prerequisites for Bi-Directional Rate Limiting 849

Configure Metal Policy on SSID 849
Configure Metal Policy on Client 850
Configure Bi-Directional Rate Limiting for All Traffic 851
Configure Bi-Directional Rate Limiting Based on Traffic Classification 851
Apply Bi-Directional Rate Limiting Policy Map to Policy Profile 853
Apply Metal Policy with Bi-Directional Rate Limiting 854
How to apply Per Client Bi-Directional Rate Limiting 855
Information About Per Client Bi-Directional Rate Limiting 855
Prerequisites for Per Client Bi-Directional Rate Limiting 856
Restrictions on Per Client Bi-Directional Rate Limiting 856
Configuring Per Client Bi-Directional Rate Limiting (GUI) 856
Verifying Per Client Bi-Directional Rate Limiting 857
Configuring BDRL Using AAA Override 857
Verifying Bi-Directional Rate-Limit 858
How to Configure Wireless QoS 859
Configuring a Policy Map with Class Map (GUI) 859
Configuring a Class Map (CLI) 860
Configuring Policy Profile to Apply QoS Policy (GUI) 861
Configuring Policy Profile to Apply QoS Policy (CLI) 861
Applying Policy Profile to Policy Tag (GUI) 862
Applying Policy Profile to Policy Tag (CLI) 862
Attaching Policy Tag to an AP 863
SIP Call Admission Control (CAC) 864
Configuring SIP CAC (GUI) 864
Configuring SIP CAC 865
Verifying SIP CAC 867
SIP Voice Call Snooping 867
Configuring SIP Voice Call Snooping (GUI) 868
Configuring SIP Voice Call Snooping 868
Verifying SIP Voice Call Snooping 869

CHAPTER 92 **Wireless Auto-QoS** 871
Information About Auto QoS 871
How to Configure Wireless AutoQoS 872

Configuring Wireless AutoQoS on Profile Policy 872
Disabling Wireless AutoQoS 873
Rollback AutoQoS Configuration (GUI) 873
Rollback AutoQoS Configuration 873
Clearing Wireless AutoQoS Policy Profile (GUI) 874
Clearing Wireless AutoQoS Policy Profile 874
Viewing AutoQoS on policy profile 875

CHAPTER 93 **Native Profiling** 877
Information About Native Profiling 877
Creating a Class Map (GUI) 878
Creating a Class Map (CLI) 879
Creating a Service Template (GUI) 881
Creating a Service Template (CLI) 882
Creating a Parameter Map 883
Creating a Policy Map (GUI) 883
Creating a Policy Map (CLI) 884
Configuring Native Profiling in Local Mode 886
Verifying Native Profile Configuration 886

CHAPTER 94 **Air Time Fairness** 889
Information About Air Time Fairness 889
Restrictions on Cisco Air Time Fairness 891
Cisco Air Time Fairness (ATF) Use Cases 892
Configuring Cisco Air Time Fairness (ATF) 892
Configuring Cisco Air Time Fairness 892
Creating a Cisco ATF Profile (GUI) 892
Creating Cisco ATF Profile (CLI) 893
Attaching Cisco ATF Profile to a Policy Profile (GUI) 894
Attaching Cisco ATF Profile to a Policy Profile (CLI) 894
Enabling ATF in the RF Profile (GUI) 895
Enabling ATF in the RF Profile (CLI) 895
Verifying Cisco ATF Configurations 896
Verifying Cisco ATF Statistics 896

PART X IPv6 899

CHAPTER 95 IPv6 Client IP Address Learning 901

Information About IPv6 Client Address Learning 901

Address Assignment Using SLAAC 901

Stateful DHCPv6 Address Assignment 902

Router Solicitation 903

Router Advertisement 903

Neighbor Discovery 903

Neighbor Discovery Suppression 904

Router Advertisement Guard 904

Router Advertisement Throttling 905

Prerequisites for IPv6 Client Address Learning 905

Configuring RA Throttle Policy (CLI) 905

Applying RA Throttle Policy on VLAN (GUI) 906

Applying RA Throttle Policy on a VLAN (CLI) 907

Configuring IPv6 Interface on a Switch (GUI) 907

Configuring IPv6 on Interface (CLI) 908

Configuring DHCP Pool on Switch (GUI) 909

Configuring DHCP Pool on Switch (CLI) 909

Configuring Stateless Auto Address Configuration Without DHCP on Switch (CLI) 910

Configuring Stateless Auto Address Configuration With DHCP on Switch 911

Configuring Stateless Address Auto Configuration Without DHCP on Switch (CLI) 913

Native IPv6 914

Information About IPv6 914

Configuring IPv6 Addressing 915

Creating an AP Join Profile (GUI) 916

Creating an AP Join Profile (CLI) 916

Configuring the Primary and Backup Controller (GUI) 917

Configuring Primary and Backup Controller (CLI) 917

Verifying IPv6 Configuration 918

CHAPTER 96 IPv6 ACL 919

Information About IPv6 ACL 919
Understanding IPv6 ACLs 919
Types of ACL 919
Per User IPv6 ACL 919
Filter ID IPv6 ACL 920
Prerequisites for Configuring IPv6 ACL 920
Restrictions for Configuring IPv6 ACL 920
Configuring IPv6 ACLs 920
Default IPv6 ACL Configuration 921
Interaction with Other Features and Switches 921
How To Configure an IPv6 ACL 921
Creating an IPv6 ACL (GUI) 921
Creating an IPv6 ACL 922
Creating WLAN IPv6 ACL (GUI) 926
Creating WLAN IPv6 ACL 926
Verifying IPv6 ACL 926
Displaying IPv6 ACLs 926
Configuration Examples for IPv6 ACL 927
Example: Creating an IPv6 ACL 927
Example: Applying an IPv6 ACL to a Policy Profile in a Wireless Environment 927
Displaying IPv6 ACLs 928
Example: Displaying IPv6 ACLs 928
Example: Configuring RA Throttling 929

CHAPTER 97 **IPv6 Client Mobility** 931
Information About IPv6 Client Mobility 931
Using Router Advertisment 932
Router Advertisement Throttling 932
IPv6 Address Learning 933
Handling Multiple IP Addresses 933
IPv6 Configuration 933
Prerequisites for IPv6 Client Mobility 933
Monitoring IPv6 Client Mobility 934

CHAPTER 98 **IPv6 Support on Flex and Mesh** 935

IPv6 Support on Flex + Mesh Deployment 935

Configuring IPv6 Support for Flex + Mesh 935

Configuring Preferred IP Address as IPv6 (GUI) 936

Configuring Preferred IP Address as IPv6 937

Verifying IPv6 on Flex+Mesh 937

PART XI **CleanAir** 939

CHAPTER 99 **Cisco CleanAir** 941

Information About Cisco CleanAir 941

Cisco CleanAir-Related Terms 942

Cisco CleanAir Components 942

Interference Types that Cisco CleanAir can Detect 943

EDRRM and AQR Update Mode 944

Prerequisites for CleanAir 944

Restrictions for CleanAir 945

How to Configure CleanAir 945

Enabling CleanAir for the 2.4-GHz Band (GUI) 945

Enabling CleanAir for the 2.4-GHz Band (CLI) 946

Configuring Interference Reporting for a 2.4-GHz Device (GUI) 946

Configuring Interference Reporting for a 2.4-GHz Device (CLI) 947

Enabling CleanAir for the 5-GHz Band (GUI) 948

Enabling CleanAir for the 5-GHz Band (CLI) 949

Configuring Interference Reporting for a 5-GHz Device (GUI) 949

Configuring Interference Reporting for a 5-GHz Device (CLI) 950

Configuring Event Driven RRM for a CleanAir Event (GUI) 951

Configuring EDRRM for a CleanAir Event (CLI) 952

Verifying CleanAir Parameters 953

Monitoring Interference Devices 954

Configuration Examples for CleanAir 954

CleanAir FAQs 955

CHAPTER 100 **Bluetooth Low Energy** 957

Information About Bluetooth Low Energy 957

Enabling Bluetooth Low Energy Beacon (GUI) 958

Enabling Bluetooth Low Energy Beacon 958

CHAPTER 101 **Spectrum Intelligence** 961

Spectrum Intelligence 961

Configuring Spectrum Intelligence 962

Verifying Spectrum Intelligence Information 962

PART XII **Mesh Access Points** 965

CHAPTER 102 **Mesh Access Points** 967

Introduction to the Mesh Network 968

Restrictions for Mesh Access Points 969

MAC Authorization 970

Preshared Key Provisioning 970

EAP Authentication 971

Bridge Group Names 971

Background Scanning 972

Mesh Backhaul at 2.4 GHz and 5 GHz 972

Dynamic Frequency Selection 973

Country Codes 973

Intrusion Detection System 973

Mesh Interoperability Between Controllers 973

Information About DHCP and NAT Functionality on Root AP (RAP) 974

Mesh Convergence 974

Noise-Tolerant Fast 975

Ethernet Bridging 975

Multicast Over Mesh Ethernet Bridging Network 976

Radio Resource Management on Mesh 976

Air Time Fairness on Mesh 977

Spectrum Intelligence for Mesh 977

Indoor Mesh Interoperability with Outdoor Mesh 978
Workgroup Bridge 978
Link Test 978
Mesh Daisy Chaining 979
Mesh Leaf Node 979
Flex+Bridge Mode 979
Backhaul Client Access 980
Mesh CAC 980
Configuring MAC Authorization (GUI) 981
Configuring MAC Authorization (CLI) 981
Configuring MAP Authorization - EAP (GUI) 983
Configuring MAP Authorization (CLI) 983
Configuring PSK Provisioning (CLI) 984
Configuring a Bridge Group Name (GUI) 985
Configuring a Bridge Group Name (CLI) 985
Configuring Background Scanning (GUI) 986
Configuring Background Scanning 986
Configuring Backhaul Client Access (GUI) 987
Configuring Backhaul Client Access (CLI) 987
Configuring Wireless Backhaul Data Rate (CLI) 988
Configuring Dynamic Frequency Selection (CLI) 988
Configuring the Intrusion Detection System (CLI) 989
Configuring Ethernet Bridging (GUI) 990
Configuring Ethernet Bridging (CLI) 990
Configuring Multicast Modes over Mesh 991
Configuring RRM on Mesh Backhaul (CLI) 992
Selecting a Preferred Parent (GUI) 993
Selecting a Preferred Parent (CLI) 993
Changing the Role of an AP (GUI) 994
Changing the Role of an AP (CLI) 995
Configuring the Mesh Leaf Node (CLI) 995
Configuring the Mesh Leaf Node (GUI) 995
Configuring Subset Channel Synchronization 996
Provisioning LSC for Bridge-Mode and Mesh APs (GUI) 996

Provisioning LSC for Bridge-Mode and Mesh APs 997
Specifying the Backhaul Slot for the Root AP (GUI) 998
Specifying the Backhaul Slot for the Root AP (CLI) 998
Using a Link Test on Mesh Backhaul (GUI) 999
Using a Link Test on Mesh Backhaul 999
Configuring Battery State for Mesh AP (GUI) 1000
Configuring Battery State for Mesh AP 1000
Configuring DHCP Server on Root Access Point (RAP) 1000
Configuring Mesh CAC (CLI) 1001
Configuring Fast Teardown for a Mesh AP Profile (CLI) 1001
Verifying DHCP Server for Root AP Configuration 1002
Verifying Mesh Configuration 1003

PART XIII **VideoStream** 1013

CHAPTER 103 **VideoStream** 1015
Information about Media Stream 1015
Prerequisites for Media Stream 1015
How to Configure Media Stream 1016
Configuring Multicast-Direct Globally for Media Stream (CLI) 1016
Configuring Media Stream for 802.11 Bands (CLI) 1017
Configuring a WLAN to Stream Video(GUI) 1019
Configuring a WLAN to Stream Video (CLI) 1019
Deleting a Media Stream (GUI) 1020
Deleting a Media Stream (CLI) 1020
Monitoring Media Streams 1021
Configuring the General Parameters for a Media Stream (GUI) 1021
Adding Media Stream (CLI) 1022
Enabling a Media Stream per WLAN (GUI) 1023
Enabling a Media Stream per WLAN (CLI) 1023
Configuring the General Parameters for a Media Stream (GUI) 1024
Configuring the General Parameters for a Media Stream (CLI) 1024
Configuring Multicast Direct Admission Control (GUI) 1025
Configuring Multicast Direct Admission Control (CLI) 1025

Create and Attach Policy-based QoS Profile 1027
Create a QoS Profile (GUI) 1027
Create a QoS Profile (CLI) 1028
Create a Service Template (GUI) 1029
Create a Service Template (CLI) 1029
Map the Service Template to the Policy Map (GUI) 1030
Map the Service Template to the Policy Map (CLI) 1030
Map the Policy Map (GUI) 1032
Map the Policy Map (CLI) 1032
Viewing Media Stream Information 1032

PART XIV **Software-Defined Access Wireless** 1035

CHAPTER 104 **Software-Defined Access Wireless** 1037
Information to Software-Defined Access Wireless 1037
Configuring SD-Access Wireless 1040
Configuring Default Map Server (GUI) 1040
Configuring Default Map Server (CLI) 1041
Configuring SD-Access Wireless Profile (GUI) 1041
Configuring SD-Access Wireless Profile (CLI) 1042
Configuring Map Server in Site Tag (GUI) 1042
Configuring Map Server in Site Tag (CLI) 1043
Configuring Map Server per L2-VNID (GUI) 1043
Configuring Map Server per L2-VNID (CLI) 1044
Verifying SD-Access Wireless 1044

CHAPTER 105 **Passive Client** 1045
Information About Passive Clients 1045
Enabling Passive Client on WLAN Policy Profile (GUI) 1046
Enabling Passive Client on WLAN Policy Profile (CLI) 1046
Enabling ARP Broadcast on VLAN (GUI) 1046
Enabling ARP Broadcast on VLAN (CLI) 1047
Configuring Passive Client in Fabric Deployment 1047
Enabling Broadcast Underlay on VLAN 1048

Enabling ARP Flooding 1049
Verifying Passive Client Configuration 1051

CHAPTER 106 Encrypted Traffic Analytics 1053
Information About Encrypted Traffic Analytics 1053
Exporting Records to IPv4 Flow Export Destination 1054
Configuring ETA Flow Export Destination (GUI) 1054
Enabling In-Active Timer 1055
Enabling ETA on WLAN Policy Profile 1055
Attaching Policy Profile to VLAN (GUI) 1056
Attaching Policy Profile to VLAN 1056
Verifying ETA Configuration 1057

PART XV VLAN 1061

CHAPTER 107 Configuring VLANs 1063
Information About VLANs 1063
Logical Networks 1063
Supported VLANs 1063
VLAN Port Membership Modes 1063
VLAN Configuration Files 1064
Normal-Range VLAN Configuration Guidelines 1065
Extended-Range VLAN Configuration Guidelines 1065
Prerequisites for VLANs 1065
Restrictions for VLANs 1066
How to Configure VLANs 1066
How to Configure Normal-Range VLANs 1066
Creating or Modifying an Ethernet VLAN 1067
Assigning Static-Access Ports to a VLAN (GUI) 1068
Assigning Static-Access Ports to a VLAN 1068
How to Configure Extended-Range VLANs 1069
Creating an Extended-Range VLAN (GUI) 1069
Creating an Extended-Range VLAN 1070
Monitoring VLANs 1070

CHAPTER 108 VLAN Groups 1071

Information About VLAN Groups 1071
Prerequisites for VLAN Groups 1072
Restrictions for VLAN Groups 1072
Creating a VLAN Group (GUI) 1072
Creating a VLAN Group (CLI) 1073
Adding a VLAN Group to Policy Profile (GUI) 1073
Adding a VLAN Group to a Policy Profile 1074
Viewing the VLANs in a VLAN Group 1074

PART XVI WLAN 1075

CHAPTER 109 WLANs 1077

Information About WLANs 1077
Band Selection 1078
Off-Channel Scanning Deferral 1078
DTIM Period 1078
Prerequisites for Configuring Cisco Client Extensions 1079
Peer-to-Peer Blocking 1079
Diagnostic Channel 1079
Prerequisites for WLANs 1080
Restrictions for WLANs 1080
How to Configure WLANs 1081
Creating WLANs (GUI) 1081
Creating WLANs (CLI) 1081
Deleting WLANs (GUI) 1082
Deleting WLANs 1082
Searching WLANs (CLI) 1083
Enabling WLANs (GUI) 1083
Enabling WLANs (CLI) 1084
Disabling WLANs (GUI) 1084
Disabling WLANs (CLI) 1084
Configuring General WLAN Properties (CLI) 1085

Configuring Advanced WLAN Properties (CLI) 1086
Configuring Advanced WLAN Properties (GUI) 1088
Verifying WLAN Properties (CLI) 1089

CHAPTER 110 Remote LANs 1091
Information About Remote LANs 1091
Configuring Remote LANs (RLANs) 1093
Enabling or Disabling all RLANs 1093
Creating RLAN Profile (GUI) 1093
Creating RLAN Profile (CLI) 1093
Configuring RLAN Profile Parameters (GUI) 1094
Configuring RLAN Profile Parameters (CLI) 1095
Creating RLAN Policy Profile (GUI) 1096
Creating RLAN Policy Profile (CLI) 1096
Configuring RLAN Policy Profile Parameters (GUI) 1097
Configuring RLAN Policy Profile Parameters (CLI) 1098
Configuring Policy Tag and Mapping an RLAN Policy Profile to an RLAN Profile (CLI) 1100
Configuring LAN Port (CLI) 1101
Attaching Policy Tag to an Access Point (GUI) 1101
Attaching Policy Tag to an Access Point (CLI) 1101
Verifying RLAN Configuration 1102

CHAPTER 111 Network Access Server Identifier 1107
Information About Network Access Server Identifier 1107
Creating a NAS ID Policy(GUI) 1108
Creating a NAS ID Policy 1108
Attaching a Policy to a Tag (GUI) 1109
Attaching a Policy to a Tag (CLI) 1109
Verifying the NAS ID Configuration 1110

CHAPTER 112 DHCP for WLANs 1113
Information About Dynamic Host Configuration Protocol 1113
Internal DHCP Servers 1113
External DHCP Servers 1114

DHCP Assignments 1114
DHCP Option 82 1115
Restrictions for Configuring DHCP for WLANs 1116
How to Configure DHCP for WLANs 1116
Configuring DHCP Scopes (GUI) 1116
Configuring DHCP Scopes (CLI) 1117
Configuring the Internal DHCP Server 1118
Configuring the Internal DHCP Server Under Client VLAN SVI (GUI) 1118
Configuring the Internal DHCP Server Under Client VLAN SVI (CLI) 1118
Configuring the Internal DHCP Server Under a Wireless Policy Profile (GUI) 1121
Configuring the Internal DHCP Server Under a Wireless Policy Profile 1121
Configuring the Internal DHCP Server Globally (GUI) 1124
Configuring the Internal DHCP Server Globally (CLI) 1124
Verifying Internal DHCP Configuration 1126

CHAPTER 113 **WLAN Security** 1129
Information About WPA1 and WPA2 1129
Information About AAA Override 1130
Prerequisites for Layer 2 Security 1130
How to Configure WLAN Security 1131
Configuring Static WEP Layer 2 Security Parameters (GUI) 1131
Configuring Static WEP Layer 2 Security Parameters (CLI) 1131
Configuring WPA + WPA2 Layer 2 Security Parameters (GUI) 1133
Configuring WPA + WPA2 Layer 2 Security Parameters (CLI) 1133

CHAPTER 114 **Workgroup Bridges** 1137
Cisco Workgroup Bridges 1137
Configuring Workgroup Bridge on a WLAN 1139
Verifying the Status of a Workgroup Bridge on the Controller 1140
Configuring Access Points as Workgroup Bridge 1141
Turning Cisco Aironet 2700/3700/1572 Series AP into Autonomous Mode 1141
Configuring Cisco Wave 2 APs in Workgroup Bridge or CAPWAP AP Mode (CLI) 1141
Configure an SSID Profile for Cisco Wave 2 APs (CLI) 1142
Configuring a Dot1X Credential (CLI) 1143

Configuring an EAP Profile (CLI) 1144
Configuring Manual-Enrollment of a Trustpoint for Workgroup Bridge (CLI) 1145
Configuring Auto-Enrollment of a Trustpoint for Workgroup Bridge (CLI) 1146
Configuring Manual Certificate Enrolment Using TFTP Server (CLI) 1148
Importing the PKCS12 Format Certificates from the TFTP Server (CLI) 1149
Configuring Radio Interface for Workgroup Bridges (CLI) 1150
Configuring Workgroup Bridge Timeouts (CLI) 1152
Configuring Bridge Forwarding for Workgroup Bridge (CLI) 1153

CHAPTER 115 **Peer-to-Peer Client Support** 1155
Information About Peer-to-Peer Client Support 1155
Configure Peer-to-Peer Client Support 1155

CHAPTER 116 **Wireless Guest Access** 1157
Wireless Guest Access 1157
Foreign Map Overview 1159
Wireless Guest Access: Use Cases 1160
Load Balancing Among Multiple Guest Controllers 1160
Guidelines and Limitations for Wireless Guest Access 1161
Troubleshooting IPv6 1161
Configure Mobility Tunnel for Guest Access (GUI) 1161
Configure Mobility Tunnel for Guest Access (CLI) 1161
Configuring Guest Access Policy (GUI) 1162
Configuring Guest Access Policy (CLI) 1162
Viewing Guest Access Debug Information (CLI) 1164
Configure Guest Access Using Different Security Methods 1165
Open Authentication 1165
Configure a WLAN Profile for Guest Access with Open Authentication (GUI) 1165
Configure a WLAN Profile For Guest Access with Open Authentication (CLI) 1165
Configuring a Policy Profile 1166
Local Web Authentication 1167
Configure a Parameter Map (GUI) 1167
Configure a Parameter Map (CLI) 1168
Configure a WLAN Profile for Guest Access with Local Web Authentication (GUI) 1168

Configure a WLAN Profile for Guest Access with Local Web Authentication (CLI) 1169
Configure an AAA Server for Local Web Authentication (GUI) 1169
Configure an AAA Server for Local Web Authentication (CLI) 1170
Global Configuration 1170
Central Web Authentication 1171
Configure a WLAN Profile for Guest Access with Central Web Authentication (GUI) 1171
Configure a WLAN Profile for Guest Access with Central Web Authentication (CLI) 1172
AAA Server Configuration (GUI) 1173
AAA Server Configuration (CLI) 1173
Configure Web Authentication on MAC Address Bypass failure (GUI) 1174
Configure Web Authentication on MAC Address Bypass Failure (CLI) 1175

CHAPTER 117 802.11r BSS Fast Transition 1177
Information About 802.11r Fast Transition 1177
Restrictions for 802.11r Fast Transition 1178
Monitoring 802.11r Fast Transition (CLI) 1179
Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI) 1180
Configuring 802.11r Fast Transition in an Open WLAN (CLI) 1181
Configuring 802.11r Fast Transition on a PSK Security–Enabled WLAN (CLI) 1183
Disabling 802.11r Fast Transition (GUI) 1184
Disabling 802.11r Fast Transition (CLI) 1184

CHAPTER 118 Assisted Roaming 1185
802.11k Neighbor List and Assisted Roaming 1185
Restrictions for Assisted Roaming 1186
How to Configure Assisted Roaming 1186
Configuring Assisted Roaming (GUI) 1186
Configuring Assisted Roaming (CLI) 1187
Verifying Assisted Roaming 1188
Configuration Examples for Assisted Roaming 1188

CHAPTER 119 802.11v 1191
Information About 802.11v 1191
Enabling 802.11v Network Assisted Power Savings 1191

Prerequisites for Configuring 802.11v 1192
Restrictions for 802.11v 1192
Enabling 802.11v BSS Transition Management 1192
Configuring 802.11v BSS Transition Management (GUI) 1193
Configuring 802.11v BSS Transition Management (CLI) 1193

CHAPTER 120 802.11w 1195
Information About 802.11w 1195
Prerequisites for 802.11w 1198
Restrictions for 802.11w 1198
How to Configure 802.11w 1199
Configuring 802.11w (GUI) 1199
Configuring 802.11w (CLI) 1199
Disabling 802.11w 1200
Monitoring 802.11w 1201

CHAPTER 121 Ethernet over GRE 1203
Introduction to EoGRE 1203
EoGRE Configuration Overview 1204
Create a Tunnel Gateway 1205
Configuring a Tunnel Domain 1206
Configuring EoGRE Global Parameters 1207
Configuring a Tunnel Profile 1207
Associating WLAN to a Wireless Policy Profile 1209
Attaching a Policy Tag and a Site Tag to an AP 1209
Verifying the EoGRE Tunnel Configuration 1210

PART XVII Multicast Domain Name System 1219

CHAPTER 122 Multicast Domain Name System 1221
Introduction to mDNS Gateway 1221
Enabling mDNS Gateway (GUI) 1222
Enabling or Disabling mDNS Gateway (GUI) 1223
Enabling or Disabling mDNS Gateway (CLI) 1223

Creating Default Service Policy 1224
Creating Custom Service Definition (GUI) 1225
Creating Custom Service Definition 1225
Creating Service List (GUI) 1226
Creating Service List 1226
Creating Service Policy (GUI) 1228
Creating Service Policy 1228
Configuring an mDNS Flex Profile (GUI) 1229
Configuring an mDNS Flex Profile (CLI) 1230
Applying an mDNS Flex Profile to a Wireless Flex Connect Profile (GUI) 1231
Applying an mDNS Flex Profile to a Wireless Flex Connect Profile (CLI) 1231
Associating mDNS Service Policy with Wireless Profile Policy (GUI) 1232
Associating mDNS Service Policy with Wireless Profile Policy 1232
Enabling or Disabling mDNS Gateway for WLAN (GUI) 1234
Enabling or Disabling mDNS Gateway for WLAN 1234
mDNS Gateway with Guest Anchor Support and mDNS Bridging 1235
Configuring mDNS Gateway on Guest Anchor 1236
Configuring mDNS Gateway on Guest Foreign (Guest WLAN) 1236
Verifying mDNS Gateway Configurations 1237

Preface

This preface describes the conventions of this document and information on how to obtain other documentation. It also provides information on what's new in Cisco product documentation.

- Document Conventions , on page lvii
- Related Documentation, on page lix
- Communications, Services, and Additional Information, on page lix

Document Conventions

This document uses the following conventions:

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

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

Reader Alert Conventions

This document may use the following conventions for reader alerts:

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Read the installation instructions before using, installing, or connecting the system to the power source. Use the statement number provided at the end of each warning statement to locate its translation in the translated safety warnings for this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Documentation

Note Before installing or upgrading the device, refer to the release notes at https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-release-notes-list.html.

- Cisco Catalyst 9800-40 Wireless Controller documentation, located at:

  http://www.cisco.com/go/c9800

- Cisco Catalyst 9800-80 Wireless Controller documentation, located at:

  http://www.cisco.com/go/c9800

- Cisco Catalyst 9800-L Wireless Controller documentation, located at:

  http://www.cisco.com/go/c9800

Communications, Services, and Additional Information

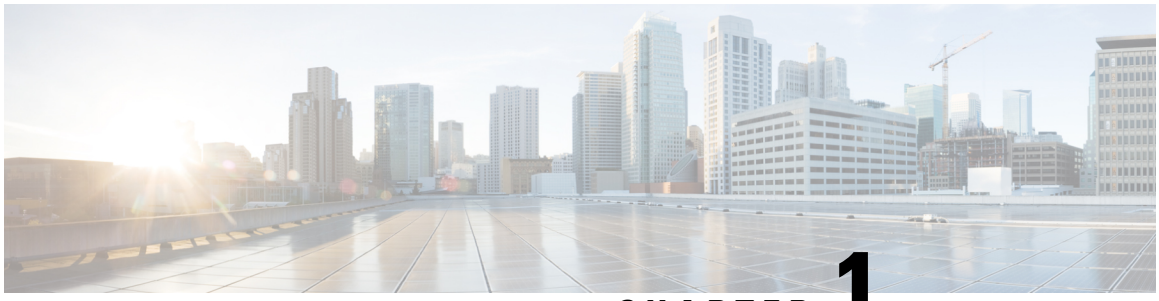
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class 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.



CHAPTER 1

Overview of Cisco 9800 Series Wireless Controllers

Cisco Catalyst 9800 Series Wireless Controllers are the next generation of wireless controllers built for the Intent-based networking. The Cisco Catalyst 9800 Series Controllers controllers are IOS XE based and integrates the RF Excellence from Aironet with Intent-based Networking capabilities of IOS XE to create the best-in-class wireless experience for your evolving and growing organization.

The controllers are deployable in physical and virtual (private and public cloud) form factors and can be managed using Cisco Catalyst Center, Netconf/YANG, Cisco Prime Infrastructure, web-based GUI, or CLI.

The Cisco Catalyst 9800 Series Wireless Controllers are available in multiple form factors to cater to your deployment options:

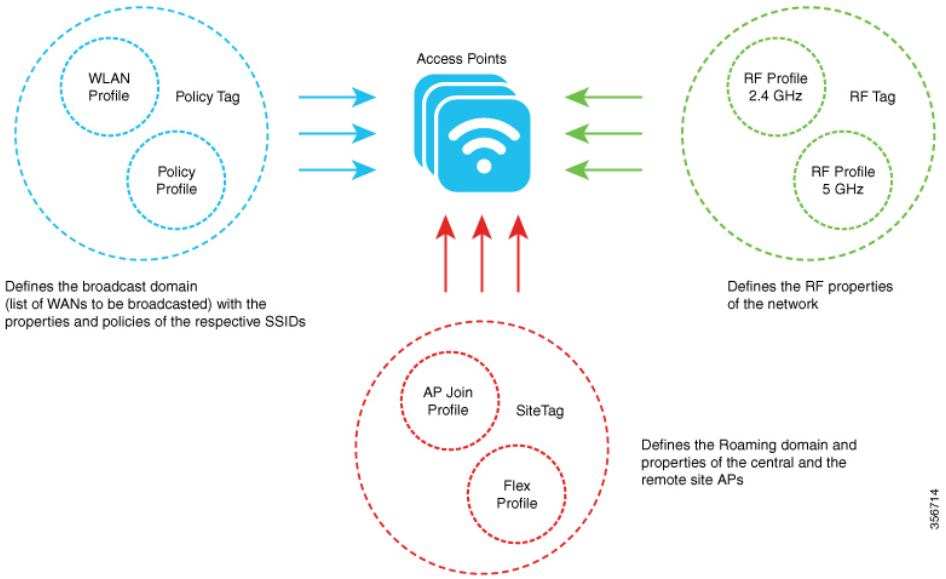
- Cisco Catalyst 9800 Series Wireless Controller Appliance
- Cisco Catalyst 9800 Series Wireless Controller for Cloud
- Cisco Catalyst 9800 Embedded Wireless for Switch

The configuration data model is based on design principles of reusability, simplified provisioning, enhanced flexibility and modularization to help manage networks as they scale up and simplify the management of dynamically changing business and IT requirements.

- Elements of the New Configuration Model, on page 1
- Configuration Workflow, on page 2
- Initial Setup, on page 3

Elements of the New Configuration Model

The following diagram depicts the elements of the new configuration model.



Tags

The property of a tag is defined by the property of the policies associated to it, which in turn is inherited by an associated client or an AP. There are various type of tags, each of which is associated to different profiles. Every tag has a default that is created when the system boots up.

Profiles

Profiles represent a set of attributes that are applied to the clients associated to the APs or the APs themselves. Profiles are reusable entities that can be used across tags.

Configuration Workflow

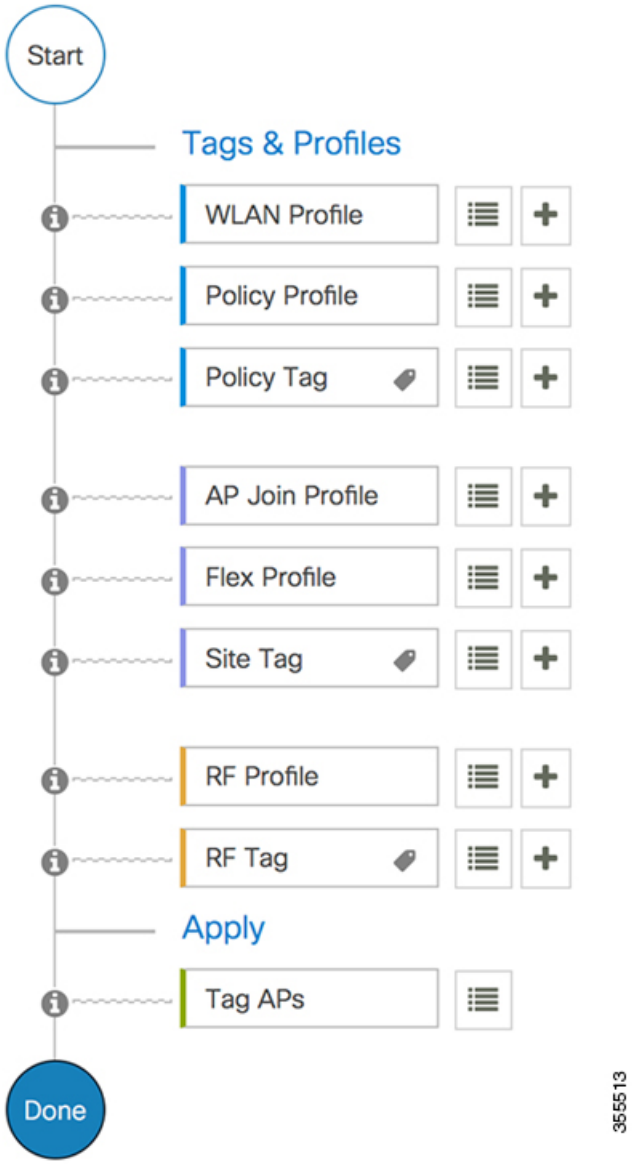
The following set of steps defines the logical order of configuration. Apart from the WLAN profile, all the profiles and tags have a default object associated with it.

1. Create the following profiles:
    - WLAN
    - Policy
    - AP Join
    - Flex
    - RF
2. Create the following tags:
    - Policy
    - Site

- RF

3. Associate tags to an AP.

Figure 1: Configuration Workflow



Initial Setup

Setting up the Controller

The initial configuration wizard in Cisco Catalyst 9800 Series Wireless Controller is a simplified, out-of-the-box installation and configuration interface for controller. 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.

Setting Up the Controller Using GUI

To set up the controller using GUI, see the *Configuring Wireless Controller* section in Cisco Catalyst 9800 Wireless Controller Series Web UI Deployment Guide.

Note If you make configuration changes in the Command Line Interface (CLI) and in the GUI simultaneously, you must click the **Refresh** button in the GUI to synch both the changes. You should always click the **Refresh** button in the GUI, to update the changes done through CLI.

Setting Up the Controller Using CLI

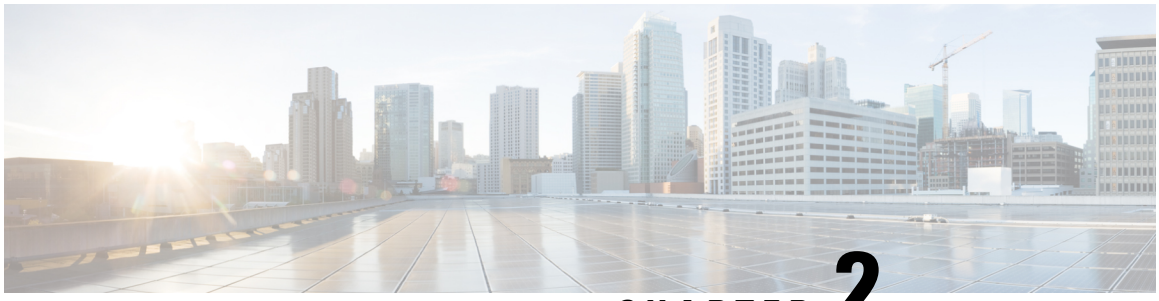
To set up the controller using CLI, see the *Performing the Initial Configuration on the Controller* section of your respective controller installation guides.

- Cisco Catalyst 9800-80 Wireless Controller Hardware Installation Guide
- Cisco Catalyst 9800-40 Wireless Controller Hardware Installation Guide
- Cisco Catalyst 9800-L Wireless Controller Hardware Installation Guide
- Cisco Catalyst 9800-CL Cloud Wireless Controller Installation Guide

PART I

System Configuration

- System Configuration, on page 7
- RF Profile, on page 37
- BIOS Protection, on page 45
- Smart Licensing, on page 47
- Best Practices, on page 57



CHAPTER 2

System Configuration

- Information About New Configuration Model, on page 7
- Configuring a Wireless Profile Policy (GUI), on page 10
- Configuring a Wireless Profile Policy (CLI), on page 10
- Configuring a Flex Profile (GUI), on page 11
- Configuring a Flex Profile, on page 12
- Configuring an AP Profile (GUI), on page 13
- Configuring an AP Profile (CLI), on page 17
- Configuring User for AP Management (CLI), on page 18
- Setting a Private Configuration Key for Password Encryption, on page 19
- Configuring an RF Profile (GUI), on page 20
- Configuring an RF Profile (CLI), on page 20
- Configuring a Site Tag (GUI), on page 21
- Configuring a Site Tag (CLI), on page 21
- Configuring Policy Tag (GUI), on page 23
- Configuring a Policy Tag (CLI), on page 23
- Configuring Wireless RF Tag (GUI), on page 24
- Configuring Wireless RF Tag (CLI), on page 24
- Attaching a Policy Tag and Site Tag to an AP (GUI), on page 25
- Attaching Policy Tag and Site Tag to an AP (CLI), on page 26
- AP Filter, on page 27
- Configuring Access Point for Location Configuration, on page 31

Information About New Configuration Model

The configuration of Cisco Catalyst 9800 Series Wireless Controllers is simplified using different tags, namely rf-tag, policy-tag, and site-tag. The access points would derive their configuration from the profiles that are contained within the tags.

Profiles are a collection of feature-specific attributes and parameters applied to tags. The rf-tag contains the radio profiles, the site-tag contains flex-profile and ap-join-profile, and the policy-tag contains the WLAN profile and policy profile.

The FlexConnect configuration helps the central controller to manage sites that are geo-distributed, for example, retail, campus, and so on.

Policy Tag

The policy tag constitutes mapping of the WLAN profile to the policy profile. The WLAN profile defines the wireless characteristics of the WLAN. The policy profile defines the network policies and the switching policies for the client (Quality of Service [QoS] is an exception which constitutes AP policies as well).

The policy tag contains the map of WLAN policy profile. There are 16 such entries per policy tag. Changes to the map entries are effected based on the status of the WLAN profile and policy profile. For example, if a map (WLAN1 and Policy1) is added to the policy tag, and both the WLAN profile and the policy profile are enabled, the definitions are pushed to the APs using the policy tag. However, if one of them is in disabled state, the definition is not pushed to the AP. Similarly, if a WLAN profile is already being broadcast by an AP, it can be deleted using the no form of the command in the policy tag.

Site Tag

The site tag defines the properties of a site and contains the flex profile and the AP join profile. The attributes that are specific to the corresponding flex or remote site are part of the flex profile. Apart from the flex profile, the site tag also comprises attributes that are specific to the physical site (and hence cannot be a part of the profile that is a reusable entity). For example, the list of primary APs for efficient upgrade is a part of a site tag rather than that of a flex profile.

If a flex profile name or an AP profile name is changed in the site tag, the AP is forced to rejoin the controller by disconnecting the Datagram Transport Layer Security (DTLS) session. When a site tag is created, the AP and flex profiles are set to default values (default-ap-profile and default-flex-profile).

RF Tag

The RF tag contains the 2.4 GHz and 5 GHz RF profiles. The default RF tag contains the global configuration. Both these profiles contain the same default values for global RF profiles for the respective radios.

Profiles

Profiles are a collection of feature-specific attributes and parameters applied to tags. Profiles are reusable entities that can be used across tags. Profiles (used by tags) define the properties of the APs or its associated clients.

WLAN Profile

WLAN profiles are configured with same or different service set identifiers (SSIDs). An SSID identifies the specific wireless network for the controller to access. Creating WLANs with the same SSID allows to assign different Layer 2 security policies within the same wireless LAN.

To distinguish WLANs having the same SSID, create a unique profile name for each WLAN. WLANs with the same SSID must have unique Layer 2 security policies so that clients can select a WLAN based on the information advertised in the beacon and probe responses. The switching and network policies are not part of the WLAN definition.

Policy Profile

Policy profile broadly consists of network and switching policies. Policy profile is a reusable entity across tags. Anything that is a policy for a client that is applied on an AP or controller is moved to the policy profile, for example, VLAN, ACL, QoS, session timeout, idle timeout, AVC profile, bonjour profile, local profiling, device classification, BSSID QoS, and so on. However, all the wireless-related security attributes and features on the WLAN are grouped under the WLAN profile.

Flex Profile

Flex profile contains policy attributes and remote site-specific parameters. For example, the EAP profiles that can be used when the AP acts as an authentication server for local RADIUS server information, VLAN-ACL mapping, VLAN name-to-ID mapping, and so on.

AP Join Profile

The default AP join profile values will have the global AP parameters and the AP group parameters. The AP join profile contains attributes that are specific to AP, such as CAPWAP, IPv4 and IPv6, UDP Lite, High Availability, Retransmit config parameters, Global AP failover, Hyperlocation config parameters, Telnet and SSH, 11u parameters, and so on.

Note Telnet is not supported for the following Cisco AP models: 1542D, 1542I, 1562D, 1562E, 1562I, 1562PS, 1800S, 1800T, 1810T, 1810W,1815M, 1815STAR, 1815TSN, 1815T, 1815W, 1832I, 1840I, 1852E, 1852I, 2802E, 2802I, 2802H, 3700C, 3800, 3802E, 3802I, 3802P, 4800, IW6300, ESW6300, 9105AXI, 9105AXW, 9115AXI, 9115AXE, 9117I, APVIRTUAL, 9120AXI, 9120AXE, 9124AXI, 9124AXD, 9130AXI, 9130AXE, 9136AXI, 9162I, 9164I, and 9166I.

RF Profile

RF profile contains the common radio configuration for the APs. RF profiles are applied to all the APs that belong to an AP group, where all the APs in that group have the same profile settings.

Association of APs

APs can be associated using different ways. The default option is by using Ethernet MAC address, where the MAC is associated with policy-tag, site tag, and RF tag.

In filter-based association, APs are mapped using regular expressions. A regular expression (regex) is a pattern to match against an input string. Any number of APs matching that regex will have policy-tag, site tag, and RF tag mapped to them, which is created as part of the AP filter.

In AP-based association, tag names are configured at the PnP server and the AP stores them and sends the tag name as part of discovery process.

In location-based association, tags are mapped as per location and are pushed to any AP Ethernet MAC address mapped to that location.

Modifying AP Tags

Modifying an AP tag results in DTLS connection reset, forcing the AP to rejoin the controller. If only one tag is specified in the configuration, default tags are used for other types, for example, if only policy tag is specified, the default-site-tag and default-rf-tag will be used for site tag and RF tag.

Configuring a Wireless Profile Policy (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, click **Add**.

Step 3 In the **Add Policy Profile** window, in **General** tab, enter a name and description for the policy profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces. Do not use spaces as it causes system instability.

Step 4 To enable the policy profile, set **Status** as **Enabled**.

Step 5 Use the slider to enable or disable **Passive Client** and **Encrypted Traffic Analytics**.

Step 6 In the **CTS Policy** section, choose the appropriate status for the following:

- Inline Tagging—a transport mechanism using which a controller or access point understands the source SGT.
- SGACL Enforcement

Step 7 Specify a default **SGT**. The valid range is from 2 to 65519.

Step 8 In the WLAN Switching Policy section, choose the following, as required:

- Central Switching: Tunnels 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.
- Central Authentication: Tunnels client data to the controller, as the controller handles client authentication.
- Central DHCP: 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.
- Central Association Enable: When central association is enabled, all switching is done on the controller.
- Flex NAT/PAT: Enables Network Address Translation(NAT) and Port Address Translation (PAT) mode.

Step 9 Click **Save & Apply to Device**.

Configuring a Wireless Profile Policy (CLI)

Follow the procedure given below to configure a wireless profile policy:

Note When a client moves from an old controller to a new controller (managed by Cisco Prime Infrastructure), the old IP address of the client is retained, if the IP address is learned by ARP or data gleaning. To avoid this scenario, ensure that you enable **ipv4 dhcp required** command in the policy profile. Otherwise, the IP address gets refreshed only after a period of 24 hours.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**idle-timeout** *timeout* **Example:** `Device(config-wireless-policy)# idle-timeout 1000`	(Optional) Configures the duration of idle timeout, in seconds.
Step 4	**vlan** *vlan-id* **Example:** `Device(config-wireless-policy)# vlan 24`	Configures VLAN name or VLAN ID.
Step 5	**accounting-list** *list-name* **Example:** `Device(config-wireless-policy)# accounting-list user1-list`	Sets the accounting list for IEEE 802.1x.
Step 6	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.
Step 7	**show wireless profile policy summary** **Example:** `Device# show wireless profile policy summary`	Displays the configured policy profiles. **Note** (Optional) To view detailed information about a policy profile, use the **show wireless profile policy detailed** *policy-profile-name* command.

Configuring a Flex Profile (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > Flex**.

Step 2 Click **Add**.

Step 3 Enter the **Name** of the Flex Profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 In the **Description** field, enter a description for the Flex Profile.

Step 5 Click **Apply to Device**.

Configuring a Flex Profile

Follow the procedure given below to set a flex profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex rr-xyz-flex-profile`	Configures a Flex profile and enters Flex profile configuration mode.
Step 3	**description** **Example:** `Device(config-wireless-flex-profile)# description xyz-default-flex-profile`	(Optional) Enables default parameters for the flex profile.
Step 4	**arp-caching** **Example:** `Device(config-wireless-flex-profile)# arp-caching`	(Optional) Enables ARP caching.
Step 5	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.
Step 6	**show wireless profile flex summary** **Example:** `Device# show wireless profile flex summary`	(Optional) Displays the flex-profile parameters. **Note** To view detailed parameters about the flex profile, use the **show wireless profile flex detailed** *flex-profile-name* command.

Configuring an AP Profile (GUI)

Before you begin

The default AP join profile values will have the global AP parameters and the AP group parameters. The AP join profile contains attributes that are specific to AP, such as CAPWAP, IPv4/IPv6, UDP Lite, High Availability, retransmit configuration parameters, global AP failover, Hyperlocation configuration parameters, Telnet/SSH, 11u parameters, and so on.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join Profile** page, click **Add**.

The **Add AP Join Profile** page is displayed.

Step 3 In the **General** tab, enter a name and description for the AP join profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Check the **LED State** check box to set the LED state of all APs connected to the device to blink so that the APs are easily located.

Step 5 In the **Client** tab and **Statistics Timer** section, enter the time in seconds that the AP sends its 802.11 statistics to the controller.

Step 6 In the **TCP MSS Configuration** section, check the **Adjust MSS Enable** check box to enter value for Adjust MSS. You can enter or update the maximum segment size (MSS) for transient packets that traverse a router. TCP MSS adjustment enables the configuration of the maximum segment size (MSS) for transient packets that traverse a router, specifically TCP segments with the SYN bit set.

In a CAPWAP environment, a lightweight access point discovers a device by using CAPWAP discovery mechanisms, and then sends a CAPWAP join request to the device. The device sends a CAPWAP join response to the access point that allows the access point to join the device.

When the access point joins the device, the device manages its configuration, firmware, control transactions, and data transactions.

Step 7 In the **CAPWAP** tab, you can configure the following:

- High Availability

  You can configure primary and secondary backup controllers for all access points (which are used if primary, secondary, or tertiary controllers are not responsive) in this order: primary, secondary, tertiary, primary backup, and secondary backup. In addition, you can configure 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.

a) In the **High Availability** tab, enter the time (in seconds) in the **Fast Heartbeat Timeout** field to configure the heartbeat timer for all access points. Specifying a small heartbeat interval reduces the amount of time it takes to detect device failure.

b) In the **Heartbeat Timeout** field, enter the time (in seconds) to configure the heartbeat timer for all access points. Specifying a small heartbeat interval reduces the amount of time it takes to detect device failure.
c) In the **Discovery Timeout** field, enter a value between 1 and 10 seconds (inclusive) to configure the AP discovery request timer.
d) In the **Primary Discovery Timeout** field, enter a value between 30 and 3000 seconds (inclusive) to configure the access point primary discovery request timer.
e) In the **Primed Join Timeout** field, enter a value between 120 and 43200 seconds (inclusive) to configure the access point primed join timeout.
f) In the **Retransmit Timers Count** field, enter the number of times that you want the AP to retransmit the request to the device and vice-versa. Valid range is between 3 and 8.
g) In the **Retransmit Timers Interval** field, enter the time duration between retransmission of requests. Valid range is between 2 and 5.
h) Check the **Enable Fallback** check box to enable fallback.
i) Enter the **Primary Controller** name and IP address.
j) Enter the **Secondary Controller** name and IP address.
k) Click **Save & Apply to Device**.

Note The primary and secondary settings in the AP join profile are not used for AP fallback. This means that the AP will not actively probe for those controllers (which are a part of the AP join profile), when it has joined one of them.

This setting is used only when the AP loses its connection with the controller, and then prioritizes which other controller it should join. These controllers have a priority of 4 and 5, following APs in the **High Availability** tab of the AP page.

The APs that are added as the primary, secondary, and tertiary APs in the **High Availability** tab of the AP configuration page, are actively probed and are used for the AP fallback option.

- Advanced

a) In the **Advanced** tab, check the **Enable VLAN Tagging** check box to enable VLAN tagging.
b) Check the **Enable Data Encryption** check box to enable Datagram Transport Layer Security (DTLS) data encryption.
c) Check the **Enable Jumbo MTU** to enable big maximum transmission unit (MTU). MTU is the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are divided into smaller packets before transmission. Jumbo frames are frames that are bigger than the standard Ethernet frame size, which is 1518 bytes (including Layer 2 (L2) header and FCS). The definition of frame size is vendor-dependent, as these are not part of the IEEE standard.
d) Use the **Link Latency** drop-down list to select the link latency. Link latency monitors the round-trip time of the CAPWAP heartbeat packets (echo request and response) from the AP to the controller and back.
e) From the **Preferred Mode** drop-down list, choose the mode.
f) Click **Save & Apply to Device**.

Step 8 In the **AP** tab, you can configure the following:

- General

a) In the **General** tab, check the **Switch Flag** check box to enable switches.
b) Check the **Power Injector State** check box if power injector is being used. Power Injector increases wireless LAN deployment flexibility of APs by providing an alternative powering option to local power, inline power-capable multiport switches, and multiport power patch panels.

Power Injector Selection parameter enables you to protect your switch port from an accidental overload if the power injector is inadvertently bypassed.

c) From the **Power Injector Type** drop-down list, choose power injector type from the following options:

- 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.

d) In the **Injector Switch MAC** field, enter the MAC address of the switch.
e) From the **EAP Type** drop-down list, choose the EAP type as *EAP-FAST*, *EAP-TLS*, or *EAP-PEAP*.
f) From the **AP Authorization Type** drop-down list, choose the type as either *CAPWAP DTLS +* or *CAPWAP DTLS*.
g) In the **Client Statistics Reporting Interval** section, enter the interval for 5 GHz and 2.4 GHz radios in seconds.
h) Check the **Enable** check box to enable extended module.
i) From the **Profile Name** drop-down list, choose a profile name for mesh.
j) Click **Save & Apply to Device**.

- Hyperlocation: Cisco Hyperlocation is a location solution that allows to track the location of wireless clients with the accuracy of one meter. Selecting this option disables all other fields in the screen, except NTP Server.

a) In the **Hyperlocation** tab, check the **Enable Hyperlocation** check box.
b) Enter the **Detection Threshold** value to filter out packets with low RSSI. The valid range is –100 dBm to –50 dBm.
c) Enter the **Trigger Threshold** value to set the number of scan cycles before sending a BAR to clients. The valid range is 0 to 99.
d) Enter the **Reset Threshold** value to reset value in scan cycles after trigger. The valid range is 0 to 99.
e) Enter the **NTP Server** IP address.
f) Click **Save & Apply to Device**.

- BLE: If your APs are Bluetooth Low Energy (BLE) enabled, they can transmit beacon messages that are packets of data or attributes transmitted over a low energy link. These BLE beacons are frequently used for health monitoring, proximity detection, asset tracking, and in-store navigation. For each AP, you can customize BLE Beacon settings configured globally for all APs.

a) In the **BLE** tab, enter a value in the **Beacon Interval** field to indicate how often you want your APs to send out beacon advertisements to nearby devices. The range is from 1 to 10, with a default of 1.
b) In the **Advertised Attenuation Level** field, enter the attenuation level. The range is from 40 to 100, with a default of 59.
c) Click **Save & Apply to Device**.

- Packet Capture: Packet Capture feature allows to capture the packets on the AP for the wireless client troubleshooting. The packet capture operation is performed on the AP by the radio drivers on the current channel on which it is operational, based on the specified packet capture filter.

a) In the **Packet Capture** tab, choose an **AP Packet Capture Profile** from the drop-down list.
b) You can also create a new profile by clicking the **+** sign.
c) Enter a name and description for the AP packet capture profile.
d) Enter the **Buffer Size**.
e) Enter the **Duration**.
f) Enter the **Truncate Length** information.
g) In the **Server IP** field, enter the IP address of the TFTP server.
h) In the **File Path** field, enter the directory path.
i) Enter the username and password details.
j) From the **Password Type** drop-down list, choose the type.
k) In the **Packet Classifiers** section, use the option to select or enter the packets to be captured.
l) Click **Save**.
m) Click **Save & Apply to Device**.

Step 9 In the **Management** tab, you can configure the following:

- Device

a) In the **Device** tab, enter the **IPv4/IPv6 Address** of the TFTP server, **TFTP Downgrade** section.
b) In the **Image File Name** field, enter the name of the software image file.
c) From the **Facility Value** drop-down list, choose the appropriate facility.
d) Enter the IPv4 or IPv6 address of the host.
e) Choose the appropriate **Log Trap Value**.
f) Enable Telnet and/or SSH configuration, if required.
g) Enable core dump, if required.
h) Click **Save & Apply to Device**.

- User

a) In the **User** tab, enter username and password details.
b) Choose the appropriate password type.
c) In the **Secret** field, enter a custom secret code.
d) Choose the appropriate secret type.
e) Choose the appropriate encryption type.
f) Click **Save & Apply to Device**.

- Credentials

a) In the **Credentials** tab, enter local username and password details.
b) Choose the appropriate local password type.

c) Enter 802.1x username and password details.
d) Choose the appropriate 802.1x password type.
e) Enter the time in seconds after which the session should expire.
f) Enable local credentials and/or 802.1x credentials as required.
g) Click **Save & Apply to Device**.

- CDP Interface

a) In the **CDP Interface** tab, enable the CDP state, if required.
b) Click **Save & Apply to Device**.

Step 10 In the **Rogue AP** tab, check the **Rogue Detection** check box to enable rogue detection.

Step 11 In the **Rogue Detection Minimum RSSI** field, enter the RSSI value.

This field specifies the minimum RSSI value for which a Rogue AP should be reported. All Rogue APs with RSSI lower than what is configured will not be reported to controller.

Step 12 In the **Rogue Detection Transient Interval** field, enter the transient interval value.

This field indicates how long the Rogue AP should be seen before reporting the controller.

Step 13 In the **Rogue Detection Report Interval** field, enter the report interval value.

This field indicates the frequency (in seconds) of Rogue reports sent from AP to controller.

Step 14 Check the **Rogue Containment Automatic Rate Selection** check box to enable rogue containment automatic rate selection.

Here, the AP selects the best rate for the target Rogue, based on its RSSI.

Step 15 Check the **Auto Containment on FlexConnect Standalone** check box to enable the feature.

Here, the AP will continue containment in case it moves to flexconnect standalone mode.

Step 16 Click **Save & Apply to Device**.

Configuring an AP Profile (CLI)

Follow the procedure given below to configure and AP profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode. **Note** In an AP profile, the **EAP-FAST** is the default EAP type.

	Command or Action	Purpose
		Note When you delete a named profile, the APs associated with that profile will not revert to the default profile.
Step 3	**description** *ap-profile-name* **Example:** `Device(config-ap-profile)# description "xyz ap profile"`	Adds a description for the ap profile.
Step 4	**cdp** **Example:** `Device(config-ap-profile)# cdp`	Enables CDP for all Cisco APs.
Step 5	**end** **Example:** `Device(config-ap-profile)# end`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.
Step 6	**show ap profile name***profile-name* **detailed** **Example:** `Device# show ap profile name xyz-ap-profile detailed`	(Optional) Displays detailed information about an AP join profile.

Configuring User for AP Management (CLI)

Follow the procedure given below to configure a user for the AP management:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile default-ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**mgmtuser username <username> password {0 | 8}** *<password>* **Example:** `Device(config-ap-profile)# mgmtuser username myusername password 0 12345678`	Specifies the AP management username and password for managing all of the access points configured to the controller. • **0**: Specifies an UNENCRYPTED password.

	Command or Action	Purpose
		• **8**: Specifies an AES encrypted password. **Note** While configuring an username, ensure that special characters are not used as it results in error with bad configuration.
Step 4	**end** **Example:** `Device(configure-ap-profile)# end`	Returns to privileged EXEC mode.

Setting a Private Configuration Key for Password Encryption

Follow the procedure given below to set a private configuration key for password encryption:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**key config-key password encrypt** key *<config-key>* **Example:** `Device(config)# key config-key password-encrypt 12345678`	Sets the password encryption keyword. Here, *config-key* refers to any key value with minimum 8 characters. **Note** The *config-key* value must not begin with the following special characters: !, #, and ;
Step 3	**password encryption aes** **Example:** `Device(config)# password encryption aes`	Enables the encrypted preshared key.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring an RF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF**.

Step 2 On the **RF Profile** page, click **Add**.

Step 3 In the **General** tab, enter a name for the RF profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Choose the appropriate **Radio Band**.

Step 5 To enable the profile, set the status as **Enable**.

Step 6 Enter a **Description** for the RF profile.

Step 7 Click **Save & Apply to Device**.

Configuring an RF Profile (CLI)

Follow the procedure given below to configure an RF profile:

Before you begin

Ensure that you use the same RF profile name that you create here, when configuring the wireless RF tag too. If there is a mismatch in the RF profile name (for example, if the RF tag contains an RF profile that does not exist), the corresponding radios will not come up.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz rf-profile** *rf-profile* **Example:** `Device(config)# ap dot11 24ghz rf-profile rfprof24_1`	Configures an RF profile and enters RF profile configuration mode. **Note** Use the **24ghz** command to configure the 802.11b parameters. Use the **5ghz** command to configure the 802.11a parameters.
Step 3	**default** **Example:** `Device(config-rf-profile)# default`	(Optional) Enables default parameters for the RF profile.

	Command or Action	Purpose
Step 4	**no shutdown** **Example:** `Device(config-rf-profile)# no shutdown`	Enables the RF profile on the device.
Step 5	**end** **Example:** `Device(config-rf-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.
Step 6	**show ap rf-profile summary** **Example:** `Device# show ap rf-profile summary`	(Optional) Displays the summary of the available RF profiles.
Step 7	**show ap rf-profile name** *rf-profile* **detail** **Example:** `Device# show ap rf-profile name rfprof24_1 detail`	(Optional) Displays detailed information about a particular RF profile.

Configuring a Site Tag (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 On the **Manage Tags** page, click the **Site** tab.

Step 3 Click **Add** to view the **Add Site Tag** window.

Step 4 Enter a name and description for the site tag. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 5 Choose the required **AP Join Profile** to be attached to the site tag.

Step 6 Choose the required **Control Plane Name**.

Step 7 If required, enable the **Local Site**.

Disabling Local Site means that the site is remote and the deployment is FlexConnect mode.

Step 8 Click **Save & Apply to Device**.

Configuring a Site Tag (CLI)

Follow the procedure given below to configure a site tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site rr-xyz-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**flex-profile** *flex-profile-name* **Example:** `Device(config-site-tag)# flex-profile rr-xyz-flex-profile`	Configures a flex profile. **Note** You cannot remove the flex profile configuration from a site tag if local site is configured on the site tag. **Note** The **no local-site** command needs to be used to configure the Site Tag as Flexconnect, otherwise the Flex profile config does not take effect.
Step 4	**description** *site-tag-name* **Example:** `Device(config-site-tag)# description "default site tag"`	Adds a description for the site tag.
Step 5	**end** **Example:** `Device(config-site-tag)# end`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.
Step 6	**show wireless tag site summary** **Example:** `Device# show wireless tag site summary`	(Optional) Displays the number of site tags. **Note** To view detailed information about a site, use the **show wireless tag site detailed** *site-tag-name* command. **Note** The output of the **show wireless loadbalance tag affinity wncd** *wncd-instance-number* command displays default tag (site-tag) type, if both site tag and policy tag are not configured.

Configuring Policy Tag (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags** > **Policy**.

Step 2 Click **Add** to view the **Add Policy Tag** window.

Step 3 Enter a name and description for the policy tag. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Click **Add** to map WLAN and policy.

Step 5 Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.

Step 6 Click **Save & Apply to Device**.

Configuring a Policy Tag (CLI)

Follow the procedure given below to configure a policy tag:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wireless tag policy** *policy-tag-name* **Example:** `Device(config-policy-tag)# wireless tag policy default-policy-tag`	Configures policy tag and enters policy tag configuration mode. **Note** When performing LWA, the clients connected to a controller gets disconnected intermittently before session timeout.
Step 4	**description** *description* **Example:** `Device(config-policy-tag)# description "default-policy-tag"`	Adds a description to a policy tag.
Step 5	**remote-lan** *name* **policy** *profile-policy-name* {**ext-module**| **port-id** }	Maps a remote-LAN profile to a policy profile.

	Command or Action	Purpose
	Example: `Device(config-policy-tag)# remote-lan rr-xyz-rlan-aa policy rr-xyz-rlan-policy1 port-id 2`	
Step 6	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan rr-xyz-wlan-aa policy rr-xyz-policy-1`	Maps a policy profile to a WLAN profile.
Step 7	**end** **Example:** `Device(config-policy-tag)# end`	Exits policy tag configuration mode, and returns to privileged EXEC mode.
Step 8	**show wireless tag policy summary** **Example:** `Device# show wireless tag policy summary`	(Optional) Displays the configured policy tags. **Note** To view detailed information about a policy tag, use the **show wireless tag policy detailed** *policy-tag-name* command.

Configuring Wireless RF Tag (GUI)

Procedure

Step 1 a) Choose **Configuration** > **Tags & Profiles** > **Tags** > **RF**.

Step 2 Click **Add** to view the **Add RF Tag** window.

Step 3 Enter a name and description for the RF tag. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Choose the required **5 GHz Band RF Profile** and **2.4 GHz Band RF Profile** to be associated with the RF tag.

Step 5 Click **Update & Apply to Device**.

Configuring Wireless RF Tag (CLI)

Follow the procedure given below to configure a wireless RF tag:

Before you begin

- You can use only two profiles (2.4-GHz and 5-GHz band RF profiles) in an RF tag.
- Ensure that you use the same AP tag name that you created when configuring the AP tag task too.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag rf** *rf-tag* **Example:** `Device(config)# wireless tag rf rftag1`	Creates an RF tag and enters wireless RF tag configuration mode.
Step 3	**24ghz-rf-policy** *rf-policy* **Example:** `Device(config-wireless-rf-tag)# 24ghz-rf-policy rfprof24_1`	Attaches an IEEE 802.11b RF policy to the RF tag. To configure a dot11a policy, use the **5ghz-rf-policy** command.
Step 4	**description** *policy-description* **Example:** `Device(config-wireless-rf-tag)# description Test`	Adds a description for the RF tag.
Step 5	**end** **Example:** `Device(config-wireless-rf-tag)# end`	Exits configuration mode and returns to privileged EXEC mode.
Step 6	**show wireless tag rf summary** **Example:** `Device# show wireless tag rf summary`	Displays the available RF tags.
Step 7	**show wireless tag rf detailed** *rf-tag* **Example:** `Device# show wireless tag rf detailed rftag1`	Displays detailed information of a particular RF tag.

Attaching a Policy Tag and Site Tag to an AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

The **All Access Points** section displays details of all the APs on your network.

Step 2 To edit the configuration details of an AP, select the row for that AP.

The **Edit AP** window is displayed.

Step 3 In the **General** tab and **Tags** section, specify the appropriate policy, site, and RF tags, that you created on the **Configuration** > **Tags & Profiles** > **Tags** page.

Step 4 Click **Update & Apply to Device**.

Attaching Policy Tag and Site Tag to an AP (CLI)

Follow the procedure given below to attach a policy tag and a site tag to an AP:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures a Cisco AP and enters AP profile configuration mode. **Note** The *mac-address* should be a wired mac address.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag rr-xyz-policy-tag`	Maps a policy tag to the AP.
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag rr-xyz-site`	Maps a site tag to the AP.
Step 5	**rf-tag** *rf-tag-name* **Example:** `Device(config-ap-tag)# rf-tag rf-tag1`	Associates the RF tag.
Step 6	**end** **Example:** `Device(config-ap-tag)# end`	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.
Step 7	**show ap tag summary** **Example:** `Device# show ap tag summary`	(Optional) Displays AP details and the tags associated to it.
Step 8	**show ap name** <*ap-name*> **tag info** **Example:**	(Optional) Displays the AP name with tag information.

	Command or Action	Purpose
	`Device# show ap name ap-name tag info`	
Step 9	**show ap name** <*ap-name*> **tag detail** **Example:** `Device# show ap name ap-name tag detail`	(Optional) Displays the AP name with tag detals.

AP Filter

Introduction to AP Filter

The introduction of tags in the new configuration model in the Cisco Catalyst 9800 Series Wireless Controller has created multiple sources for tags to be associated with access points (APs). Tag sources can be static configuration, AP filter engine, per-AP PNP, or default tag sources. In addition to this, the precedence of the tags also plays an important role. The AP filter feature addresses these challenges in a seamless and intuitive manner.

AP filters are similar to the access control lists (ACLs) used in the controller and are applied at the global level. You can add AP names as filters, and other attributes can be added as required. Add the filter criteria as part of the discovery requests.

The AP Filter feature organizes tag sources with the right priority, based on the configuration.

You cannot disable the AP filter feature. However, the relative priority of a tag source can be configured using **ap filter-priority** *priority filter-name* command.

Note You can configure tag names at the PnP server (similar to the Flex group and AP group) and the AP stores and send the tag name as part of discovery and join requests.

Set Tag Priority (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags** > **AP** > **Tag Source**.

Step 2 Drag and Drop the Tag Sources to change priorities.

Set Tag Priority

Multiple tag sources might result in ambiguity for network administrators. To address this, you can define priority for tags. When an AP joins the controller, the tags are picked based on priority. If precedence is not set, the defaults are used.

Use the following procedure to set tag priority:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**ap tag-source-priority** *source-priority* **source {filter | pnp}** **Example:** `Device(config)# ap tag-source-priority 2 source pnp`	Configures AP tag source priority. **Note** It is not mandatory to configure AP filter. It comes with default priorities for Static, Filter, and PnP.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode and returns to privileged EXEC mode.
Step 4	**ap tag-sources revalidate** **Example:** `Device# ap tag-sources revalidate`	Revalidates AP tag sources. The priorities become active only after this command is run. **Note** If you change the priorities for Filter and PnP, and want to evaluate them, run the **revalidate** command.

Create an AP Filter (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags** > **AP** > **Filter**.

Step 2 Click **Add**.

Step 3 In the **Associate Tags to AP** dialog box which is displayed, enter the **Rule Name**, the **AP name regex** and the **Priority**. Optionally, you can also choose the policy tag from the **Policy Tag Name** drop-down list, the site tag from the **Site Tag Name** drop-down list and the RF tag from the **RF Tag Name** drop-down list.

Step 4 Click **Apply to Device**.

Create an AP Filter (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**ap filter name** *filter_name* **Example:** `Device(config)# ap filter filter-1`	Configures an AP filter.
Step 3	**ap name-regex** *regular-expression* **Example:** `Device(config-ap-filter)# ap name-regex testany`	Configures the AP filter based on regular expression. For example, if you have named an AP as **ap-lab-12**, then you can configure the filter with a regular expression, such as **ap-lab-\d+** , to match the AP name.
Step 4	**tag policy** *policy-tag* **Example:** `Device(config-ap-filter)# tag policy pol-tag1`	Configures a policy tag for this filter.
Step 5	**tag rf** *rf-tag* **Example:** `Device(config-ap-filter)# tag rf rf-tag1`	Configures an RF tag for this filter.
Step 6	**tag site** *site-tag* **Example:** `Device(config-ap-filter)# tag site site1`	Configures a site tag for this filter.
Step 7	**end** **Example:** `Device(config-ap-filter)# end`	Exits configuration mode and returns to privileged EXEC mode.

Set Up and Update Filter Priority (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags** > **AP** > **Filter**.

Step 2

a) If you want to setup a new AP filter, then click **Add**. In the **Associate Tags to AP** dialog box which is displayed, enter the **Rule Name**, the **AP name regex** and the **Priority**. Optionally, you can also select the **Policy Tag Name**, the **Site Tag Name** and the **RF Tag Name**. Click **Apply to Device**.

b) If you want to update the priority of an existing AP filter, click on the Filter and in the **Edit Tags** dialog box and change the **Priority**. In case the Filter is Inactive, no priority can be set to it. Click **Update and Apply to Device**.

Set Up and Update Filter Priority

Follow the procedure given below to set and update filter priority:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap filter priority** *priority* **filter-name** *filter-name* **Example:** `Device(config)# ap filter priority 10 filter-name test1`	Configure AP filter priority. Valid values range from 0 to 1023; 0 is the highest priority. **Note** A filter without a priority is not active. Similarly, you cannot set a filter priority without a filter.
Step 3	**end** **Example:** `Device(config-ap)# end`	Exits configuration mode and returns to privileged EXEC mode.

Verify AP Filter Configuration

The following **show** commands are used to display tag sources and filters, and their priorities.

To view the tag source priorities, use the following command:

```
Device# show ap tag sources

Priority Tag source
--------------------------------
0 Static
1 Filter
2 AP
3 Default
```

To view the available filters, use the following command:

```
Device# show ap filter all

Filter Name             regex             Policy Tag              RF Tag              Site
 Tag
-------------------------------------------------------------------------------------------
```

```
first                   abcd              pol-tag1                 rf-tag1
site-tag1
test1                  testany                                                  site1

filter1                 testany
```

To view the list of active filters, use the following command:

```
Device# show ap filters active

Priority   Filter Name       regex          Policy Tag              RF Tag
Site Tag
-------------------------------------------------------------------------------------------------------------
10         test1             testany
site1
```

To view the source of an AP tag, use the following command:

```
Device# show ap tag summary

Number of APs: 4

AP Name          AP Mac         Site Tag Name    Policy Tag Name    RF Tag Name
Misconfigured Tag Source
-------------------------------------------------------------------------------------------------------------
AP002A.1034.CA78 002a.1034.ca78 named-site-tag   named-policy-tag   named-rf-tag   No Filter

AP00A2.891C.2480 00a2.891c.2480 named-site-tag   named-policy-tag   named-rf-tag   No Filter

AP58AC.78DE.9946 58ac.78de.9946 default-site-tag default-policy-tag default-rf-tag No AP
AP0081.C4F4.1F34 0081.c4f4.1f34 default-site-tag default-policy-tag default-rf-tag No Default
```

Configuring Access Point for Location Configuration

Information About Location Configuration

During location configuration, you can perform the following:

- Configure a site or location for an AP.
- Configure a set of tags for this location.
- Add APs to this location.

Any location comprises of the following components:

- A set of unique tags, one for each kind, namely: Policy, RF and Site.
- A set of ethernet MAC addresses that applies to the tags.

This feature works in conjunction with the existing tag resolution scheme. The location is considered as a new tag source to the existing system. Similar, to the static tag source.

Prerequisite for Location Configuration

If you configure an access point in one location, you cannot configure the same access point in another location.

Configuring a Location for an Access Point (GUI)

Before you begin

Note When you create local and remote sites in the Basic Setup workflow, corresponding policies and tags are created in the backend. These tags and policies that are created in the Basic Setup cannot be modified using the Advanced workflow, and vice versa.

Procedure

Step 1 Choose **Configuration** > **Wireless Setup** > **Basic**.

Step 2 On the **Basic Wireless Setup** page, click **Add**.

Step 3 In the **General** tab, enter a name and description for the location.

Step 4 Set the **Location Type** as either *Local* or *Flex*.

Step 5 Use the slider to set **Client Density** as *Low*, *Typical* or *High*.

Step 6 Click **Apply**.

Configuring a Location for an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap location name** *location_name* **Example:** `Device(config)# ap location name location1`	Configures a location for an access point. Run the **no** form of this command to remove location for an access point.
Step 3	**tag** {**policy** *policy_name*| **rf** *rf_name* | **site** **site_name**} **Example:** `Device(config-ap-location)# tag policy policy_tag`	Configures tags for the location.

	Command or Action	Purpose
	`Device(config-ap-location)# tag rf rf_tag` `Device(config-ap-location)# tag site site_tag`	
Step 4	**location** *description* **Example:** `Device(config-ap-location)# location description`	Adds description to the location.
Step 5	**end** **Example:** `Device(config-ap-location)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Adding an Access Point to the Location (GUI)

Note When the tag source is not set to location, the AP count and AP location tagging will not be correctly reflected on the web UI. To change static tag source on the AP, run the **no ap** *ap-mac* command on the controller to change AP tag source to default (which is location).

Procedure

Step 1 Choose **Configuration** > **Wireless Setup** > **Basic**.

Step 2 On the**Basic Wireless Setup** page, click **Add** to configure the following:

- General
- Wireless Networks
- AP Provisioning

Step 3 In the **AP Provisioning** tab and **Add/Select APs** section, enter the AP MAC address and click the right arrow to add the AP to the associated list.

You can also add a CSV file from your system. Ensure that the CSV has the MAC Address column.

Step 4 Use the search option in the **Available AP List** to select the APs from the Selected AP list and click the right arrow to add the AP to the associated list.

Step 5 Click **Apply**.

Adding an Access Point to the Location (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap location name** *location_name* **Example:** `Device(config)# ap location name location1`	Configures a location for an access point.
Step 3	**ap-eth-mac** *ap_ethernet_mac* **Example:** `Device(config-ap-location)# ap-eth-mac 188b.9dbe.6eac`	Adds an access point to the location.
Step 4	**end** **Example:** `Device(config-ap-location)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. **Note** After adding an AP to a location, the AP may reset automatically to get the new configuration

Configuring SNMP in Location Configuration

SNMP MIB

The SNMP MIB provides information on a set of managed objects that represent logical and physical entities, and relationships between them.

Table 1: MIB Objects and Notes

MIB Objects	Notes
cLApLocationName	Provides the name of the AP location.
cLApLocationPolicyTag	Provides the policy tag configured on the location.
cLApLocationSitetag	Provides the site tag configured on the location.
cLApLocationRfTag	Provides the RF tag configured on the location.
cLAssociatedApsApMac	Provides the configured APs on the location.

Verifying Location Configuration

To view the summary of AP location configuration, use the following command:

```
Device# show ap location summary

Location Name    Description     Policy Tag           RF Tag           Site Tag
-------------------------------------------------------------------------------------------
first            first floor     default-policy-tag   default-rf-tag   default-site-tag
second           second floor    default-policy-tag   default-rf-tag   default-site-tag
```

To view the AP location configuration details for a specific location, use the following command:

```
Device# show ap location details first

Location Name.....................: first
Location description..............: first floor
Policy tag........................: default-policy-tag
Site tag..........................: default-site-tag
RF tag............................: default-rf-tag

Configured list of APs
005b.3400.0af0
005b.3400.0bf0
```

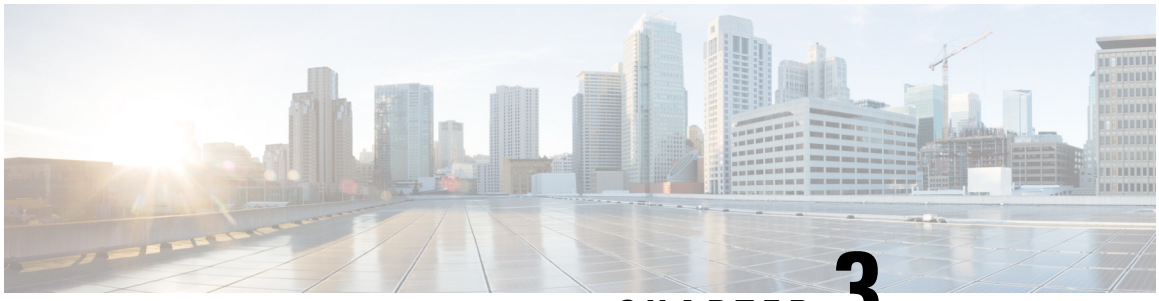
To view the AP tag summary, use the following command:

```
Device# show ap tag summary

Number of APs: 4
AP Name      AP Mac           Site Tag Name      Policy Tag Name      RF Tag Name
Misconfigured  Tag Source
-------------------------------------------------------------------------------------------------------
Asim_5-1     005b.3400.02f0   default-site-tag   default-policy-tag   default-rf-tag   Yes
            Filter
Asim_5-2     005b.3400.03f0   default-site-tag   default-policy-tag   default-rf-tag   No
            Default
Asim_5-9     005b.3400.0af0   default-site-tag   default-policy-tag   default-rf-tag   No
            Location
Asim_5-10    005b.3400.0bf0   default-site-tag   default-policy-tag   default-rf-tag   No
            Location
```

Verifying Location Statistics

To view the AP location statistics, use the following command:

```
Device# show ap location stats

Location name    APs joined     Clients joined     Clients on 11a     Clients on 11b
-------------------------------------------------------------------------------------------
first             2             0                   3                  4
second            0             0                   0                  0
```



CHAPTER 3

RF Profile

- RF Tag Profiles, on page 37
- Configuring an AP Tag (GUI), on page 37
- Configuring AP Tag (CLI), on page 38
- Configuring RF Profile (GUI), on page 39
- Configuring an RF Profile (CLI), on page 40
- Configuring Wireless RF Tag (GUI), on page 42
- Configuring Wireless RF Tag (CLI), on page 42

RF Tag Profiles

RF Profiles allows you to group set of APs that share a common coverage zone together and selectively change how RRM 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 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 RF tags allows you to optimize the RF settings for set of APs that operate in different environments or coverage zones. RF profiles are created for the IEEE 802.11 radios and are applied to all APs that are mapped to an RF tag, where all APs with that RF tag have the same profile settings.

Configuring an AP Tag (GUI)

Before you begin

Ensure that you have configured an AP Join Profile prior to configuring the primary and backup controllers.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 On the **Manage Tags** page, click the AP tab.

Step 3 In the **Tag Source** tab, drag and drop the tag sources to change priorities.

Step 4 Check the **Revalidate Tag Sources on APs** check box, if required.

Step 5 Click **Apply**.
Step 6 In the **Static** tab, click **Add**.
Step 7 In the **Associate Tags to AP** window, enter a MAC address.
Step 8 Choose the appropriate **Policy Tag Name**, **Site Tag Name**, and **RF Tag Name**.
Step 9 Click **Save & Apply to Device**.
Step 10 In the **Filter** tab, click **Add**.
Step 11 In the **Associate Tags to AP** window, enter a rule and AP name regex.
Step 12 Use the slider to enable **Active**.
Step 13 Enter the **Priority**. The valid range is from 0 to 127.
Step 14 Choose the appropriate **Policy Tag Name**, **Site Tag Name**, and **RF Tag Name.**
Step 15 Click **Save & Apply to Device**.

Configuring AP Tag (CLI)

Follow the procedure given below to create an AP tag:

Before you begin

Ensure that you use the same AP tag created here in Wireless RF tag.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap 188b.9dbe.6eac`	Enters the AP tag configuration mode. **Important** Use only AP MAC address. Do not use Ethernet MAC address.
Step 3	**rf-tag** *rf-tag* **Example:** `Device(config-ap-tag)# rf-tag rftag1`	Configures a named RF tag and adds the AP mac-address to the tag.
Step 4	**end** **Example:** `Device(config-ap-tag)# end`	Exits the configuration mode and returns to privileged EXEC mode.
Step 5	**show ap tag summary** **Example:** `Device# show ap tag summary`	Displays the tag summary of available APs.

What to do next

Configure Wireless RF tag.

Configuring RF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF**.

Step 2 On the**RF Profile** page, click **Add** to configure the following:

- General
- 802.11
- RRM
- Advanced

Step 3 In the **General** tab, proceed as follows:

a) Enter a name and description for the RF profile.
b) Choose the appropriate radio band.
c) To enable the profile, set the status as *Enable*.
d) Click **Save & Apply to Device**.

Step 4 In the **802.11** tab, proceed as follows:

a) Choose the required operational rates.
b) Select the required 802.11n MCS Rates by checking the corresponding check boxes.
c) Click **Save & Apply to Device**.

Step 5 In the **RRM > General** tab, proceed as follows:

a) Enter the foreign interference threshold between 0 and 100 percent in the Interference field. The default is 10.
b) In the **Clients** field, enter the client threshold between 1 and 75 clients. The default is 12.
c) In the **Noise** field, enter the foreign noise threshold between –127 and 0 dBm. The default is –70.
d) In the **Utilization** percentage field, enter the RF utilization threshold between 0 and 100 percent. The default is 80.

Step 6 In the **RRM > Coverage** tab, proceed as follows:

a) Enter the client level in the Minimum Client Level field.
b) In the **Data RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 to -90 dBm and the default value is –80 dBm.
c) In the **Voice RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 to -90 dBm and the default value is –75.
d) In the **Exception Level** field, enter the maximum desired percentage of clients on an AP's radio operating below the desired coverage threshold. Value ranges from 0 to 100% and the default value is 25%.

Step 7 In the **RRM > TPC** tab, proceed as follows:

a) Enter the power level assignment on this radio in the **Maximum Power Level** field. If you configure maximum transmit power, RRM does not allow any access point attached to the device to exceed this transmit power level (whether the power is set by RRM TPC or by coverage hole detection).
b) In the **Minimum Power Level** field, enter the minimum power level assignment on this radio.
c) In the **Power Threshold V1** field, enter the cutoff signal level used by RRM when determining whether to reduce an access point's power.

Step 8 In the **RRM > DCA** tab, proceed as follows:

a) Check the **Avoid AP 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 unselect 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.
b) Choose the appropriate channel width.
c) In the **DCA Channels** section, the DCA Channels field shows the channels that are currently selected. To choose a channel, select the appropriate check box. Extended UNII-2 channels in the 802.11a/n/ac band do not appear in the channel list: 100, 104, 108, 112, 116, 132, 136, and 140. To include these channels in the channel list, select the Extended UNII-2 Channels check box.
d) Click **Save & Apply to Device**.

Step 9 In the **Advanced** tab, enter the following information in the **High Density Parameters** section:

a) In the **Max Clients** field, set the maximum number of clients allowed globally.
b) Use the **Multicast Data Rate** drop-down to choose the data rate for multicast traffic.

   Choose auto to configure the device to use the radio's default data rate.

c) Use the **Rx SOP Threshold** drop-down to set the Receiver Start of Packet Detection Threshold (Rx SOP) to determine the Wi-Fi signal level in dBm at which AP radios will demodulate and decode a packet. The higher the RXSOP level, the less sensitive the radio is and the smaller the receiver cell size will be. Reducing the cell size ensures that clients connect to the nearest access point using highest possible data rates. Choose auto to configure the device to use the radio's default threshold.

Step 10 In the **Client Distribution** section, enter the following:

- **Load Balancing Window**—Enter a value between 1 and 20 to specify the load-balancing window and the number of client associations on the AP with the lightest load.
- **Load Balancing Denial Count**—Enter a value between 0 and 10 to specify the number of times the client associations will be rejected for a particular AP.

Step 11 In the **High Speed Roam** section, check the **Mode Enable** check box to enable the mode.

Step 12 In the **Neighbor Timeout** field, enter the neighbor timeout value.

Step 13 From the **Client Network Preference** drop-down list, choose the client network preference.

Step 14 In the **ATF Configuration** section, use the slider to enable or disable **Status** and **Bridge Client Access**.

Step 15 Click **Save & Apply to Device**.

Configuring an RF Profile (CLI)

Follow the procedure given below to configure an RF profile:

Before you begin

Ensure that you use the same RF profile name that you create here, when configuring the wireless RF tag too. If there is a mismatch in the RF profile name (for example, if the RF tag contains an RF profile that does not exist), the corresponding radios will not come up.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz rf-profile** *rf-profile* **Example:** `Device(config)# ap dot11 24ghz rf-profile rfprof24_1`	Configures an RF profile and enters RF profile configuration mode. **Note** Use the **24ghz** command to configure the 802.11b parameters. Use the **5ghz** command to configure the 802.11a parameters.
Step 3	**default** **Example:** `Device(config-rf-profile)# default`	(Optional) Enables default parameters for the RF profile.
Step 4	**no shutdown** **Example:** `Device(config-rf-profile)# no shutdown`	Enables the RF profile on the device.
Step 5	**end** **Example:** `Device(config-rf-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.
Step 6	**show ap rf-profile summary** **Example:** `Device# show ap rf-profile summary`	(Optional) Displays the summary of the available RF profiles.
Step 7	**show ap rf-profile name** *rf-profile* **detail** **Example:** `Device# show ap rf-profile name rfprof24_1 detail`	(Optional) Displays detailed information about a particular RF profile.

Configuring Wireless RF Tag (GUI)

Procedure

Step 1 a) Choose **Configuration** > **Tags & Profiles** > **Tags** > **RF**.

Step 2 Click **Add** to view the **Add RF Tag** window.

Step 3 Enter a name and description for the RF tag. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Choose the required **5 GHz Band RF Profile** and **2.4 GHz Band RF Profile** to be associated with the RF tag.

Step 5 Click **Update & Apply to Device**.

Configuring Wireless RF Tag (CLI)

Follow the procedure given below to configure a wireless RF tag:

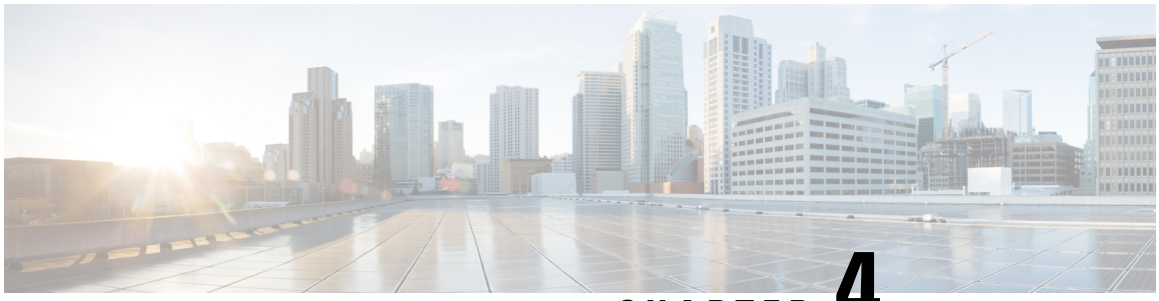
Before you begin

- You can use only two profiles (2.4-GHz and 5-GHz band RF profiles) in an RF tag.
- Ensure that you use the same AP tag name that you created when configuring the AP tag task too.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag rf** *rf-tag* **Example:** `Device(config)# wireless tag rf rftag1`	Creates an RF tag and enters wireless RF tag configuration mode.
Step 3	**24ghz-rf-policy** *rf-policy* **Example:** `Device(config-wireless-rf-tag)# 24ghz-rf-policy rfprof24_1`	Attaches an IEEE 802.11b RF policy to the RF tag. To configure a dot11a policy, use the **5ghz-rf-policy** command.
Step 4	**description** *policy-description* **Example:** `Device(config-wireless-rf-tag)# description Test`	Adds a description for the RF tag.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config-wireless-rf-tag)# end`	Exits configuration mode and returns to privileged EXEC mode.
Step 6	**show wireless tag rf summary** **Example:** `Device# show wireless tag rf summary`	Displays the available RF tags.
Step 7	**show wireless tag rf detailed** *rf-tag* **Example:** `Device# show wireless tag rf detailed rftag1`	Displays detailed information of a particular RF tag.



CHAPTER 4

BIOS Protection

- BIOS Protection on the Controller, on page 45
- BIOS or ROMMON Upgrade with BIOS Protection, on page 45
- Upgrading BIOS, on page 46

BIOS Protection on the Controller

BIOS Protection enables you to protect and securely update BIOS flash for Intel-based platforms. If BIOS Protection is not used, the flash utility that stores the BIOS for an Intel platform is not write-protected. As a result, when BIOS updates are applied, malicious code also makes its way through.

By default, BIOS Protection works by bundling the flash containing the BIOS image, and by accepting updates only through the BIOS capsules that enable writing on the BIOS Flash.

BIOS or ROMMON Upgrade with BIOS Protection

To upgrade BIOS or ROMMON use the BIOS Protection feature as follows:

1. The new BIOS image capsule bundled together with the ROMMON binary is inserted into the media of the Cisco device by the ROMMON upgrade scripts.
2. The Cisco device is then reset for the new BIOS/ROMMON upgrade to take place.
3. On reset, the original BIOS detects the updated capsule and determines if the updated BIOS is available.
4. The original BIOS then verifies the digital signature of the BIOS capsule. If the signature is valid, the original BIOS will remove write-protection from the flash utility and update the SPI flash with the new BIOS image. If the BIOS capsule is invalid, the SPI flash is not updated.
5. After the new BIOS/ROMMON image is written to the SPI flash, the required regions of the SPI flash are once again write-protected.
6. After the card is reset, the updated BIOS is rebooted.
7. The capsule is deleted by BIOS.

Upgrading BIOS

Procedure

Use the **upgrade rom-monitor filename** command to update the BIOS capsule.

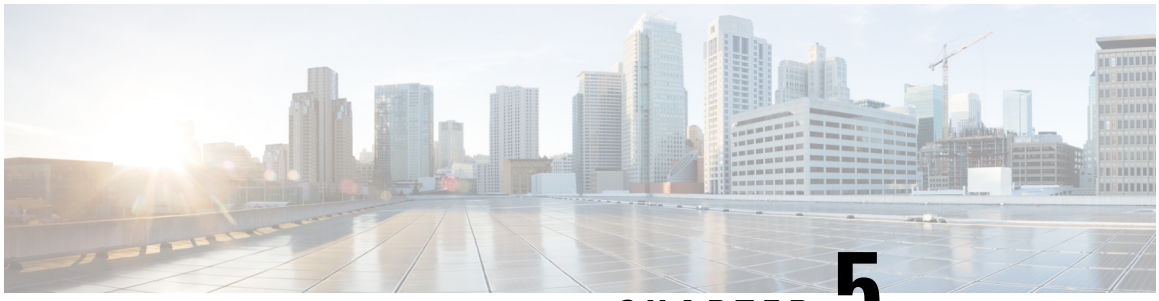
Example:

```
upgrade rom-monitor filename bootflash:capsule.pkg <slot>
```

Example

The following example shows you how to verify a BIOS Protection upgrade:

```
Device# upgrade rom-monitor filename bootflash:qwlc-rommon-capsule-p106.pkg all
Verifying the code signature of the ROMMON package...
Chassis model AIR-CT5540-K9 has a single rom-monitor.

Upgrade rom-monitor

Target copying rom-monitor image file

Secure update of the ROMMON image will occur after a reload.

8388608+0 records in
8388608+0 records out
8388608 bytes (8.4 MB, 8.0 MiB) copied, 11.9671 s, 701 kB/s
131072+0 records in
131072+0 records out
131072 bytes (131 kB, 128 KiB) copied, 0.414327 s, 316 kB/s
Copying ROMMON environment
8388608+0 records in
8388608+0 records out
8388608 bytes (8.4 MB, 8.0 MiB) copied, 31.1199 s, 270 kB/s
131072+0 records in
131072+0 records out
131072 bytes (131 kB, 128 KiB) copied, 2.44015 s, 53.7 kB/s
131072+0 records in
131072+0 records out
131072 bytes (131 kB, 128 KiB) copied, 2.43394 s, 53.9 kB/s
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the RP.
Device#reload
```



CHAPTER 5

Smart Licensing

- Information About Cisco Smart Licensing, on page 47
- Creating a Smart Account, on page 49
- Using Smart Licensing, on page 50
- Reregister a License (GUI), on page 50
- Using Specified License Reservation (SLR), on page 50
- Enabling Smart Software Licensing, on page 51
- Enabling Smart Call Home Reporting, on page 52
- Configuring AIR License Level (GUI), on page 52
- Configuring AIR License Level (CLI), on page 53
- Configuring AIR Network Essentials License Level, on page 53
- Configuring AIR Network Advantage License Level , on page 54
- Verifying Smart Licensing Configurations, on page 54

Information About Cisco Smart Licensing

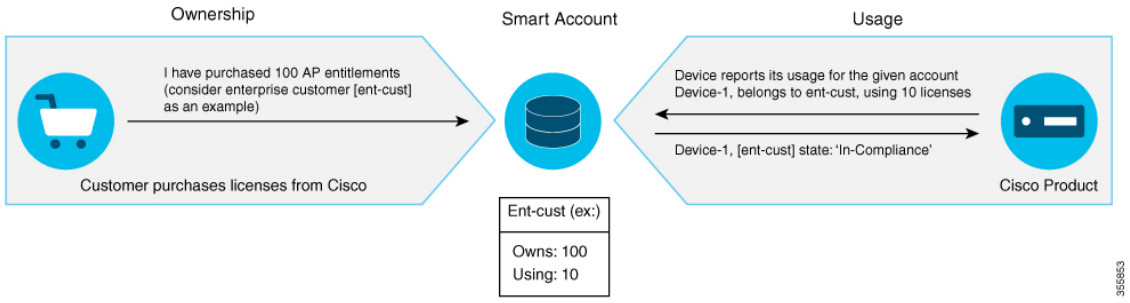
Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- Easy Activation: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- Unified Management: My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- License Flexibility: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (software.cisco.com).

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

Figure 2: Relationship Between Ownership, Smart Account, and Usage



Note As a prerequisite, register your controller with the satellite SSM (VM on customer premises) or CSSM (Cisco Cloud) using the Smart Call Home HTTPS server.

Once your product is registered in CSSM, you will be able to view the license usage using your Smart Account or Virtual Account for every eight hours.

Note

- Smart Licensing registration is lost when the device switches from controller to autonomous mode and back. In such instances, you should re-register the controller to CSSM to restore licenses authorization.
- After adding new license in the Cisco Smart Software Manager (CSSM) for customer virtual account, run the **license smart renew auth** command on the controller to get the license status changed from Out OF Compliance to Authorised.

Access points support the following AIR licensing levels:

- AIR Network Essential (AIR-NE)
- AIR Network Advantage (AIR-NA)
- AIR DNA Essential (AIR-DNA-E)
- AIR DNA Advantage (AIR-DNA-A)

Note The *AIR-DNA-A* and *AIR-DNA-E* are the available license levels on the controller.

The AIR-DNA-A is the default mode.

You can configure as *AIR-DNA-A* or *AIR-DNA-E* license level and on term expiry, you can move to the Network Advantage or Network Essentials license level, if you do not want to renew the DNA license.

Smart Licensing Reservation Types

License reservation is a mechanism to reserve node locked licenses and install them on the controller.

The following are the license reservation types:

- Permanent License Reservation (PLR)—All licenses are reserved.
- Specified License Reservation (SLR)—Only specific licenses are reserved. Supports term licenses.

The controller supports four different entitlement registration or reporting on Smart Licensing or service reservation. Every connecting AP requires a Cisco DNA Center License to leverage the unique value properties of the controller.

Note The controller boots up with *AIR-DNA-A* as the default. Any change in the license level requires a reboot.

Entitlement Reporting

Entitlement reporting is nothing but reporting the number of access points on the controller to the Cisco Smart Software Manager (CSSM).

The entitlement reporting is based on the configured AIR license level on the controller.

Note Two types of entitlement reporting occurs when you are in *AIR-DNA-E* and *AIR-DNA-A* levels. For instance, if your controller reports 100 APs as count, your entitlement reporting displays *100 AIR-NE* and *100 AIR-DNA-E*. Similarly, it also displays *100 AIR-NA* and *100 AIR-DNA-A* to CSSM.

Creating a Smart Account

Procedure

Step 1 Navigate to the Cisco Software Central web page:

https://software.cisco.com/#

The Cisco Software Central page is displayed.

Step 2 From the **Important News** pop-up window, click **Get a Smart Account**.

(Or)

From the **Administration** area, click **Request a Smart Account**.

Follow the process to create a Smart Account.

Note You need to have a Smart Account to use Smart Licensing.

Using Smart Licensing

Before you begin

Follow the procedure given below to cover the high-level steps on how to use smart licensing:

Procedure

Step 1 Configure your device for smart licensing.

Step 2 Login to **CSSM** customer **Smart Account** > **Virtual Account** to generate a token.

Step 3 Execute the following command on your device:

```
Device# license smart register idtoken <token-id>
```

Note You can get the *token-id* from the CSSM web portal.

Note You can use the **license smart register idtoken** *token-id* **force** command to register the device again even if the same device was registered with CSSM earlier.

Reregister a License (GUI)

Procedure

Step 1 Choose **Administration** > **Licensing**.

Step 2 In the **Registration Status** field, click **Reregister** link. The **Registration** dialog box is displayed.

Step 3 Select the **Register this product instance if it is already registered** check box to forcefully register the product.

Step 4 Click **Finish**.

Using Specified License Reservation (SLR)

Procedure

Step 1 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 2 **license smart reservation**

Example:

```
Device(config)# license smart reservation
```

Enables specified license reservation mode on the controller.

Step 3 **license smart reservation request local**

Example:

```
Device(config)# license smart reservation request local
```

Generates a request code.

Note Enter this request code in the Cisco Smart Software Manager portal:

```
CB-ZL-AIR-9500C-K9:9J4FVHMBXCO-BjSeUVwmn-D8
```

Step 4 **end**

Example:

```
Device(config)# end
```

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

Enabling Smart Software Licensing

Procedure

Step 1 Navigate to the Cisco Software Central web page using the following link:

https://software.cisco.com/#

The Cisco Software Central page is displayed.

Step 2 From the **License** tab, click **Smart Software Licensing**.

The Smart Software Licensing page is displayed.

Step 3 Click the **Inventory** tab to view **Virtual Account: Accounting** page details.

Step 4 Click **New Token** to register the product instances to this virtual account.

The Create Registration Token page is displayed.

Step 5 In the **Description** field, enter a description for the ID token.

Step 6 Check the **Allow export-controlled functionality on the products registered with this token** checkbox to enable export-controlled functionality.

Step 7 Click **Create Token**.

Note Licenses cannot be purchased with the wireless controller. All licenses can be purchased with access points.

Enabling Smart Call Home Reporting

Procedure

Step 1 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 2 **call-home reporting contact-email-addr** *email-address* **http-proxy** *proxy-server port-number*

Example:

```
Device(config)# call-home reporting contact-email-addr sample@cisco.com http-proxy 120.20.2.2
 5
```

Enables Call Home reporting.

- *port-number*—The valid range is from 1 to 65535.

Step 3 **end**

Example:

```
Device(config)# end
```

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

For more information on Smart Call Home, see:

https://www.cisco.com/c/en/us/td/docs/switches/lan/smart_call_home/book/SCH31_Ch3.html

Configuring AIR License Level (GUI)

Procedure

Step 1 Choose **Administration** > **Licensing**.

Step 2 Click **Change Wireless License Level**. The **Change Wireless License Level** dialog box is displayed.

Step 3 Select the License Level using the drop-downs.

Step 4 After changing the **New Level** values, click **Save & Reload** (Or) **Save without Reload**. Alternatively, you can click **Reload** to reload the device. During this time, you will lose network connectivity to the device. If you wish to continue, click **Yes**.

Step 5 Click refresh icon to refresh the device.

Configuring AIR License Level (CLI)

Procedure

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

Step 2	**license air level** {**air-network-advantage** | **air-network-essentials**}
	Example:
	`Device(config)# license air level air-network-advantage`
	`Device(config)# license air level air-network-essentials`
		Configures AIR license level.
		• air-network-advantage—Is the AIR network advantage license level.
		• air-network-essentials—Is the AIR network essential license level.

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

Configuring AIR Network Essentials License Level

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**license air level network-essentials addon air-dna-essentials** **Example:** `Device(config)# license air level network-essentials addon air-dna-essentials`	Configures AIR network essentials license level.

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

Configuring AIR Network Advantage License Level

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**license air level air-network-advantage addon air-dna-advantage** **Example:** `Device(config)# license air level air-network-advantage addon air-dna-advantage`	Configures AIR network advantage license level.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Smart Licensing Configurations

To verify the smart licensing status and license usage, use the following command:

```
Device# show license all
Smart Licensing Status
======================
Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 73 days, 1 hours, 33 minutes, 8 seconds

Utility:
Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
```

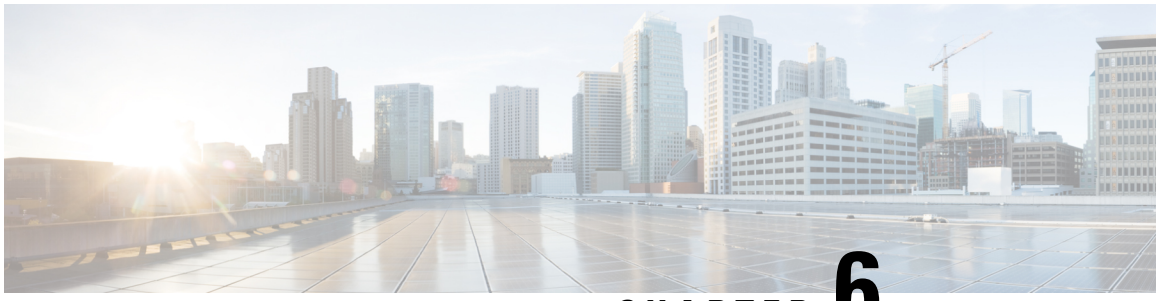
```
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

License Usage
==============
(AIR_network_essential):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE

Product Information
===================
UDI: PID:L-AIR-9500C-K9,SN:9J4FVHMBXCO

Agent Version
=============
Smart Agent for Licensing: 4.5.3_rel/43
Component Versions: SA:(1_3_dev)1.0.15, SI:(dev22)1.2.1, CH:(rel5)1.0.3, PK:(dev18)1.0.3

Reservation Info
================
License reservation: DISABLED
```

To verify the smart licensing status, use the following command:

```
Device# show license status
Tue Oct 02 07:34:36.023 IST
Smart Licensing is ENABLED
  Initial Registration: SUCCEEDED on Mon Oct 01 2018 21:55:46 IST
  Last Renewal Attempt: None
  Registration Expires: Sun Dec 29 2018 11:49:40 IST
License Authorization:
  Status: AUTHORIZED on Mon Oct 01 2018 21:55:46 IST
  Last Communication Attempt: SUCCEEDED on Mon Oct 01 2018 21:55:46 IST
  Next Communication Attempt: Thu Nov 02 2018 21:56:10 IST
    Communication Deadline: Sun Dec 29 2018 11:49:16 IST
```

To verify the air license level and smart licensing status, use the following command:

```
Device# show version
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Advantage

Smart Licensing Status: UNREGISTERED/No Licenses in Use
```



CHAPTER 6

Best Practices

- Introduction, on page 57

Introduction

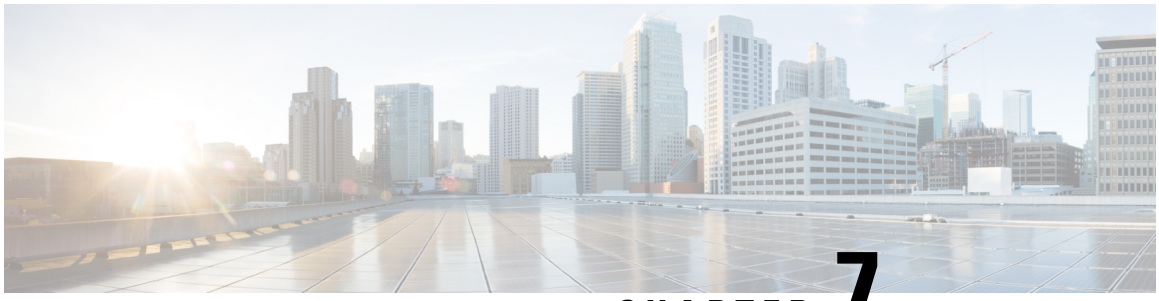
This chapter covers the best practices recommended for configuring a typical Cisco Catalyst 9800 Series wireless infrastructure. The objective is to provide common settings that you can apply to most wireless network implementations. However, not all networks are the same. Therefore, some of the tips might not be applicable to your installation. Always verify them before you perform any changes on a live network.

For more information, see Cisco Catalyst 9800 Series Configuration Best Practices guide.

PART II

Lightweight Access Points

- Country Codes, on page 61
- Sniffer Mode, on page 67
- Monitor Mode, on page 73
- Sensor Mode, on page 75
- AP Priority, on page 79
- FlexConnect, on page 81
- Data DTLS, on page 123
- Converting Autonomous Access Points to Lightweight Mode, on page 127
- AP Crash File Upload, on page 141
- Rogue per AP, on page 143
- Access Point Plug-n-Play, on page 153
- 802.11 Parameters for Cisco Access Points, on page 155
- 802.1x Support, on page 171
- CAPWAP Link Aggregation Support, on page 179
- DHCP and NAT Functionality on Root Access Point, on page 185
- Configuring Bi-Directional Rate Limiting Support with AAA Override, on page 187



CHAPTER 7

Country Codes

- Information About Country Codes, on page 61
- Prerequisites for Configuring Country Codes, on page 61
- Configuring Country Codes (GUI), on page 62
- Configuring Country Codes (CLI), on page 62
- Configuration Examples for Configuring Country Codes, on page 64

Information About Country Codes

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

Information About Japanese Country Codes

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

- J2: Allows only -P radios to join the controller
- J4: Allows 2.4G JPQU and 5G PQU to join the controller.

Prerequisites for Configuring Country Codes

- Generally, you should configure one country code per device; you configure one code that matches the physical location of the device and its access points. You can configure up to 200 country codes per device. This multiple-country support enables you to manage access points in various countries from a single device.
- When the multiple-country feature is used, all the devices that are going to join the same RF group must be configured with the same set of countries, configured in the same order.
- Access points are capable of using all the available legal frequencies. However, access points are assigned to the frequencies that are supported in their relevant domains.

- The country list configured on the RF group leader determines which channels the members will operate on. This list is independent of which countries have been configured on the RF group members.
- For devices in the Japan regulatory domain, you should have one or more Japan country codes (JP, J2, or J3) configured on your device at the time you last booted your device.
- For devices in the Japan regulatory domain, you should have one or more Japan country codes (J2, or J4) configured on your device at the time you last booted your device.
- For devices in the Japan regulatory domain, you must have at least one access point with a -J regulatory domain joined to your device.
- You cannot delete any country code using the configuration command **wireless country country-code** if the specified country was configured using the **ap country list** command and vice-versa.

Configuring Country Codes (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **Country**.

Step 2 On the **Country** page, select the check box for each country where your access points are installed. If you selected more than one check box, a message is displayed indicating that RRM channels and power levels are limited to common channels and power levels.

Step 3 Click **Apply**.

Configuring Country Codes (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**show wireless country supported** **Example:** `Device# show wireless country supported`	Displays a list of all the available country codes.
Step 3	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 4	**ap dot11** { **24ghz** | **5ghz** } **shutdown** **Example:** `Device(config)# ap dot11 5ghz shutdown`	Disables the 802.11b/g network, if you use 24ghz. Disables the 802.11a network, if you use 5ghz.
Step 5	**ap country** *country_code* **Example:** `Device(config)# ap country IN`	Configures country code on the controller, so that access points joining controller matches the country code and its corresponding regulatory domain codes for the AP. **Note** More than one country code can be configured.
Step 6	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 7	**show wireless country configured** **Example:** `Device# show wireless country configured`	Displays the configured countries.
Step 8	**show wireless country channels** **Example:** `Device# show wireless country channels`	Displays the list of available channels for the country codes configured on your device. **Note** Perform Steps 9 through 17 only if you have configured multiple country codes in Step 6.
Step 9	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 10	**no ap dot11** { **24ghz** | **5ghz** } **shutdown** **Example:** `Device(config)# no ap dot11 5ghz shutdown`	Enables the 802.11b/g network, if you use 24ghz. Enables the 802.11a network, if you use 5ghz.
Step 11	**ap name** *cisco-ap* **shutdown** **Example:** `Device# ap name AP02 shutdown`	Disables the access point. **Note** Ensure that you disable only the access point for which you are configuring country codes.
Step 12	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 13	**ap name** *cisco-ap* **country** *country_code* **Example:** `Device# ap name AP02 country US`	Assigns each access point with a country code from the controller country code list. **Note** • Ensure that the country code that you choose is compatible with the regulatory domain of at least one of the access point's radios. • Disable the access point before changing country code.
Step 14	**ap name** *cisco-ap* **no shutdown** **Example:** `Device# ap name AP02 no shutdown`	Enables the access point.

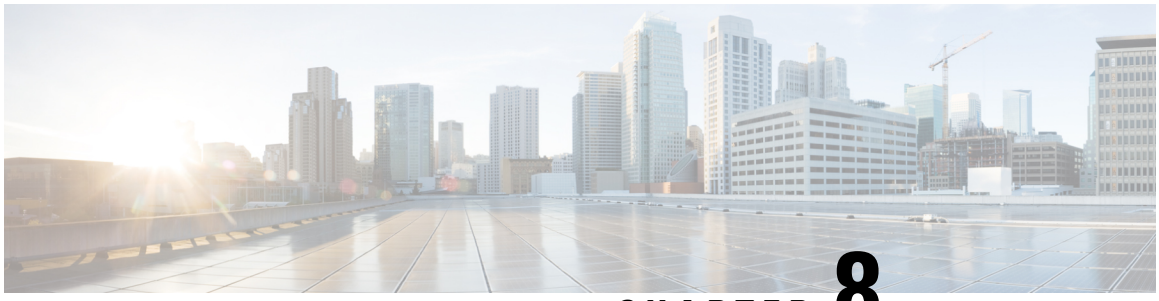
Configuration Examples for Configuring Country Codes

Viewing Channel List for Country Codes

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

```
Device# show wireless country channels

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

```
US (-A ,-AB )     : * * * * * * * * * * * * * * * * * * * * A * * * * * A
Auto-RF           : . . . . . . . . . . . . . . . . . . . . . . . . . . .
```



CHAPTER 8

Sniffer Mode

- Information about Sniffer, on page 67
- Prerequisites for Sniffer, on page 67
- Restrictions on Sniffer, on page 68
- How to Configure Sniffer, on page 68
- Verifying Sniffer Configurations, on page 70
- Examples for Sniffer Configurations and Monitoring, on page 70

Information about Sniffer

The controller enables you to configure an access point as a network “sniffer”, which captures and forwards all the packets on a particular channel to a remote machine that runs packet analyzer software. These packets contain information on time stamps, signal strength, packet sizes, and so on.

Sniffers allow you to monitor and record network activity, and detect problems.

The packet analyser machine configured receives the 802.11 traffic encapsulated using the Airopeek protocol from the controller management IP address with source port UDP/5555 and destination UDP/5000.

You must use **Clear** in AP mode to return the AP back to client-serving mode, for example the local mode or flexconnect mode depending on the remote site tag configuration.

Prerequisites for Sniffer

To perform 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 Sniffer

- 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..
- Sniffer mode is not supported when the controller L3 interface is the Wireless Management Interface (WMI).

How to Configure Sniffer

Configuring an Access Point as Sniffer (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 On the **General** tab, update the name of the AP. The AP name can be ASCII characters from 33 to 126, without leading and trailing spaces.

Step 3 Specify the physical location where the AP is present.

Step 4 Choose the **Admin Status** as **Enabled** if the AP is to be in enabled state.

Step 5 Choose the mode for the AP as *Sniffer*.

Step 6 In the **Tags** section, specify the appropriate policy, site, and RF tags that you created on the **Configuration** > **Tags & Profiles** > **Tags** page.

Note If the AP is in sniffer mode, you do not want to assign any tag.

Step 7 Click **Update & Apply to Device**.

Step 8 Choose the mode for the AP as **Clear** to return the AP back to the client-serving mode depending on the remote site tag configuration.

Configuring an Access Point as Sniffer (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device>enable`	Enables privileged EXEC mode.
Step 2	**ap name** *ap-name* **mode sniffer** **Example:** `Device# ap name access1 mode sniffer`	Configures the access point as a sniffer. Where, *ap-name* is the name of the Cisco lightweight access point. Use the **no** form of this command to disable the access point as a sniffer.

Enabling or Disabling Sniffing on the Access Point (GUI)

Before you begin

Change the access point AP mode to sniffer mode.

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 On the **Access Points** page, click the AP name from the 5 GHz or 2.4 GHz list.

Step 3 In the **Edit Radios** > **Configure** > **Sniffer Channel Assignment** section, check the **Sniffer Channel Assignment** checkbox to enable.

Uncheck the checkbox to disable sniffing on the access point.

Step 4 From the **Sniff Channel** drop-down list, select the channel.

Step 5 Enter the IP address in the **Sniffer IP** field.

Step 6 Click **Update & Apply to Device**.

Enabling or Disabling Sniffing on the Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 {24ghz | 5ghz | 6ghz} slot 3 sniff** *channel server-ip-address* **Example:** `Device# ap name access1 dot11 6ghz slot 3 sniff 1 9.9.48.5`	Enables sniffing on the access point. • *channel* is the valid channel to be sniffed. For 802.11a, the range is 36 to 165. For 802.11b, the range is 1 to 14. • *server-ip-address* is the IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark software.
Step 3	**ap name** *ap-name* **dot11 {24ghz | 5ghz | 6ghz} slot 3 no sniff** *channel server-ip-address* **Example:** `Device#ap name access1 dot11 6ghz slot 3 sniff 1 9.9.48.5`	Disables sniffing on the access point.

Verifying Sniffer Configurations

Table 2: Commands for verifying sniffer configurations

Commands	Description
show ap name *ap-name* **config dot11** {**24ghz** | **5ghz** | **dual-band**}	Displays the sniffing details.
show ap name *ap-name* **config slot** *slot-ID*	Displays the sniffing configuration details. *slot-ID* ranges from 0 to 3. All access points have slot 0 and 1.

Examples for Sniffer Configurations and Monitoring

This example shows how to configure an access point as Sniffer:

```
Device# ap name access1 mode sniffer
```

This example shows how to enable sniffing on the access point:

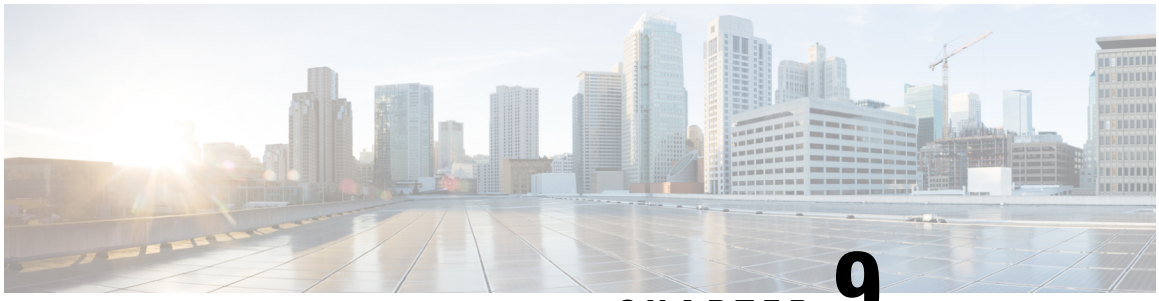
```
Device# ap name access1 sniff dot11b 1 9.9.48.5
```

This example shows how to disable sniffing on the access point:

```
Device# ap name access1 no sniff dot11b
```

This example shows how to display the sniffing configuration details:

```
Device# show ap name access1 config dot11 24ghz
Device# show ap name access1 config slot 0
```



CHAPTER 9

Monitor Mode

- Introduction to Monitor Mode, on page 73
- Enable Monitor Mode (GUI), on page 73
- Enable Monitor Mode (CLI), on page 74

Introduction to Monitor Mode

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/x 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).

Note You can move an AP to a particular mode (sensor mode to local mode or flex mode) using the site tag with the corresponding mode. If the AP is not tagged to any mode, it will fall back to the mode specified in the default site tag.

You must use clear in AP mode to return the AP back to client-serving mode, for example the local mode or flexconnect mode depending on the remote site tag configuration.

Enable Monitor Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Access Points** page, expand the **All Access Points** section and click the name of the AP to edit.

Step 3 In the **Edit AP** page, click the **General** tab and from the **AP Mode** drop-down list, choose **Monitor**.

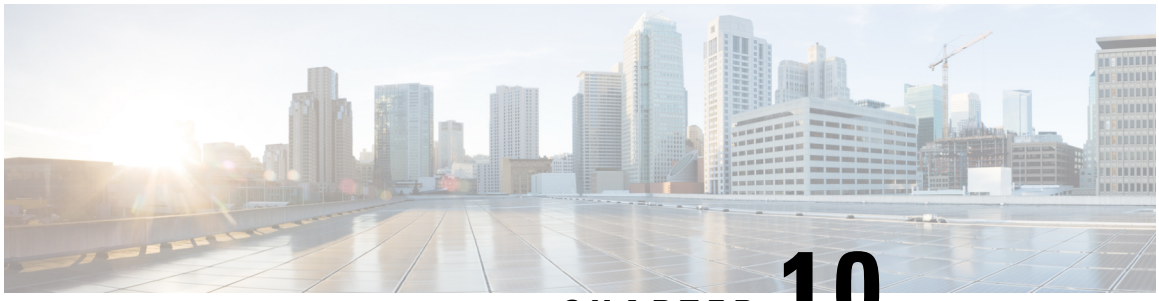
Step 4 Click **Update & Apply to Device**.

Step 5 Choose the mode for the AP as **clear** to return the AP back to the client-serving mode depending on the remote site tag configuration.

Enable Monitor Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **mode monitor** **Example:** `Device# ap name 3602a mode monitor`	Enables monitor mode for the access point.
Step 2	**ap name** *ap-name* **monitor tracking-opt** **Example:** `Device# ap name 3602a monitor tracking-opt`	Configures the access point to scan only the Dynamic Channel Assignment (DCA) channels supported by its country of operation.
Step 3	**ap name** *ap-name* **monitor-mode dot11b fast-channel** [*first-channel second-channel third-channel fourth-channel*] **Example:** `Device# ap name 3602a monitor dot11b 1 2 3 4`	Chooses up to four specific 802.11b channels to be scanned by the access point. In the United States, you can assign any value from 1 to 11 (inclusive) to the channel variable. Other countries support additional channels. You must assign at least one channel. **Note** Use the **show ap dot11 24ghz channel** command to see the available channels.
Step 4	**show ap dot11 {24ghz | 5ghz} channel** **Example:** `Device# show ap dot11 5ghz channel`	Shows configuration and statistics of 802.11a channel assignment.



CHAPTER 10

Sensor Mode

- Introduction to Sensor Mode, on page 75
- Enabling Sensor Mode, on page 75
- Verifying Sensor Mode Configuration, on page 78

Introduction to Sensor Mode

As these wireless networks grow especially in remote facilities where IT professionals may not always be on site, it becomes even more important to be able to quickly identify and resolve potential connectivity issues ideally before the users complain or notice connectivity degradation.

To address these issues, Cisco introduced a Wireless Service Assurance and a new AP mode called **sensor** mode. For more information, see Cisco Aironet Sensor Deployment Guide.

You must use **Clear** in AP mode to return the AP back to client-serving mode, for example the local mode or flexconnect mode depending on the remote site tag configuration.

Enabling Sensor Mode

Procedure

	Command or Action	Purpose

Step 1	**ap name** *ap-name* **mode sensor**
	
	Example:
	`Device# ap name AP4001.7A39.2E12 mode sensor`
		Enables sensor mode for the access point
		
		Sensor mode APs do not support the following per-AP configurations:
		
		`ap name <ap-name> [no] shutdown`
		`ap name <ap-name> dot11 24ghz SI`
		`ap name <ap-name> dot11 24ghz antenna ext-ant-gain <ext-ant-gain-number>`
		`ap name <ap-name> dot11 24ghz antenna selection [external | internal]`
		`ap name <ap-name> dot11 24ghz beamforming`
		`ap name <ap-name> dot11 24ghz channel [<channel-number> | auto]`
		`ap name <ap-name> dot11 24ghz cleanair`
		`ap name <ap-name> dot11 24ghz dot11n`

	Command or Action	Purpose
		antenna [A | B | C | D] ap name <ap-name> dot11 24ghz shutdown ap name <ap-name> dot11 24ghz txpower [<transmit-power-level> | auto] ap name <ap-name> dot11 24ghz slot <slot-number> SI ap name <ap-name> dot11 24ghz slot <slot-number> antenna ext-ant-gain <ext-ant-gain-number> ap name <ap-name> dot11 24ghz slot <slot-number> antenna selection [external | internal] ap name <ap-name> dot11 24ghz slot <slot-number> beamforming ap name <ap-name> dot11 24ghz slot <slot-number> channel [<channel-number> | auto] ap name <ap-name> dot11 24ghz slot <slot-number> cleanair ap name <ap-name> dot11 24ghz slot <slot-number> dot11n antenna [A | B | C | D] ap name <ap-name> dot11 24ghz slot <slot-number> shutdown ap name <ap-name> dot11 24ghz slot <slot-number> txpower [<trasnmit-power-level> | auto] ap name <ap-name> dot11 5ghz txpower [<transmit-power-level> | auto] ap name <ap-name> dot11 5ghz SI ap name <ap-name> dot11 5ghz antenna ext-ant-gain <ext-ant-gain> ap name <ap-name> dot11 5ghz antenna mode [omni | sectorA | sectorB] ap name <ap-name> dot11 5ghz antenna selection [external | internal] ap name <ap-name> dot11 5ghz beamforming ap name <ap-name> dot11 5ghz channel <channel-number> ap name <ap-name> dot11 5ghz channel auto ap name <ap-name> dot11 5ghz channel width [160 MHz | 20 MHz | 40 MHz | 80 MHz | 80+80 MHz] ap name <ap-name> dot11 5ghz cleanair ap name <ap-name> dot11 5ghz dot11n antenna [A | B | C | D | E | F | G | H] ap name <ap-name> dot11 5ghz rrm channel <channel-number> ap name <ap-name> dot11 5ghz secondary-80 <channel-number> ap name <ap-name> dot11 5ghz shutdown ap name <ap-name> dot11 5ghz slot <slot-number> SI ap name <ap-name> dot11 5ghz slot <slot-number> antenna ext-ant-gain <ext-ant-gain-number> ap name <ap-name> dot11 5ghz slot <slot-number> antenna mode [omni | sectorA | sectorB] ap name <ap-name> dot11 5ghz slot <slot-number> antenna selection [external | internal]

	Command or Action	Purpose
		ap name <ap-name> dot11 5ghz slot <slot-number> beamforming ap name <ap-name> dot11 5ghz slot <slot-number> channel <channel-number> ap name <ap-name> dot11 5ghz slot <slot-number> channel auto ap name <ap-name> dot11 5ghz slot <slot-number> channel width [160 MHz | 20 MHz | 40 MHz | 80 MHz] ap name <ap-name> dot11 5ghz slot <slot-number> cleanair ap name <ap-name> dot11 5ghz slot <slot-number> dot11n antenna [A | B | C | D | E | F | G | H] ap name <ap-name> dot11 5ghz slot <slot-number> rrm channel <channel-number> ap name <ap-name> dot11 5ghz slot <slot-number> shutdown ap name <ap-name> dot11 5ghz slot <slot-number> txpower [<transmit-power-level> | auto] ap name <ap-name> dot11 dual-band channel <channel-number> ap name <ap-name> dot11 dual-band channel auto ap name <ap-name> dot11 dual-band channel width [160W | 20W | 40W | 80W] ap name <ap-name> dot11 dual-band txpower [<transmit-power-level> | auto] ap name <ap-name> dot11 dual-band antenna ext-ant-gain <ext-ant-gain-number> ap name <ap-name> dot11 dual-band band [24ghz | 5ghz] ap name <ap-name> dot11 dual-band role {auto | manual [client-serving | monitor]} ap name <ap-name> dot11 dual-band cleanair ap name <ap-name> dot11 dual-band cleanair band [24Ghz | 5Ghz] ap name <ap-name> dot11 dual-band dot11n antenna [A | B | C | D] ap name <ap-name> dot11 dual-band shutdown ap name <ap-name> dot11 dual-band slot <slot-number> antenna ext-ant-gain <ext-ant-gain-number> ap name <ap-name> dot11 dual-band slot <slot-number> band [24ghz | 5ghz] ap name <ap-name> dot11 dual-band slot <slot-number> channel <channel-number> ap name <ap-name> dot11 dual-band slot <slot-number> channel auto ap name <ap-name> dot11 dual-band slot <slot-number> channel width [160 MHz | 20 MHz | 40 MHz | 80 MHz] ap name <ap-name> dot11 dual-band slot <slot-number> cleanair ap name <ap-name> dot11 dual-band slot <slot-number> cleanair band [24Ghz | 5Ghz]

	Command or Action	Purpose
		ap name <ap-name> dot11 dual-band slot <slot-number> dot11n antenna [A | B | C | D] ap name <ap-name> dot11 dual-band slot <slot-number> role {auto | manual [client-serving | monitor]} ap name <ap-name> dot11 dual-band slot <slot-number> shutdown ap name <ap-name> dot11 dual-band slot <slot-number> txpower [<transmit-power-level> | auto]

Verifying Sensor Mode Configuration

Use the following **show** command to verify the mode of the AP:

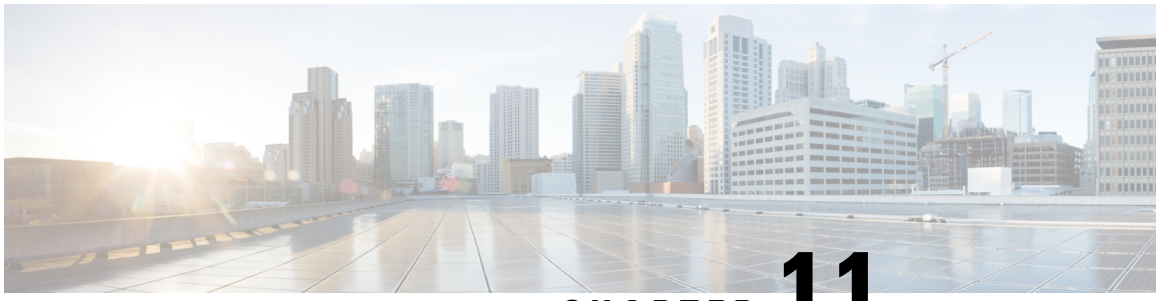
```
Device# show ap dot11 dual-band summary
AP Name          Mac Address    Slot Admin   State Oper State Width Txpwr Mode Subband
channel
-------------------------------------------------------------------------------------
AP4001.7A39.2E12 7070.8b24.1ba0  0   Enabled  N/A   NA   N/A   Sensor All (Sensor)
```

Use the following **show** command to verify Txpower, Channel width, Oper state and "(Sensor)" under Channel for an AP in Sensor mode:

```
Device# show ap dot11 24ghz summary
AP Name          Mac Address    Slot  Admin   State  Oper  State Width Txpwr Channel
-------------------------------------------------------------------------------------
AP4001.7A39.2E12 7070.8b24.1ba0 0    Enabled   N/A   N/A    N/A (Sensor)
AP-SIDD-3702I    80e0.1d6a.3520 0    Enabled   Down   20   *1/8 (22 dBm)(11)
```

Use the following **show** command to verify Txpower, Channel width, Oper state and "(Sensor)" under Channel for an AP in Sensor mode:

```
Device# show ap dot11 5ghz summary
AP Name          Mac Address    Slot  Admin   State  Oper  State Width Txpwr Channel
-------------------------------------------------------------------------------------
AP4001.7A39.2E12 7070.8b24.1ba0  1   Enabled   N/A   N/A   N/A   (Sensor)
AP-SIDD-3702I    80e0.1d6a.3520  1   Enabled   Down  40    1/6   (17 dBm) (100,104)*
```



CHAPTER 11

AP Priority

- Failover Priority for Access Points, on page 79
- Setting AP Priority (GUI), on page 79
- Setting AP Priority, on page 80

Failover Priority for Access Points

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

The following are some guidelines for configuring failover priority for access points:

- You can configure your wireless network so that the backup 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 associations requests to controller than the avaiable AP capacity on the controller.
- AP priority is checked while connecting to the controller when the controller is in full scale or the primary controller fails, the APs fallback to the secondary controller.
- 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.

Setting AP Priority (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 Click the Access Point.

Step 3 In the **Edit AP** dialog box, go to **High Availability** tab.

Step 4 Choose the priority from the **AP failover priority** drop-down list.

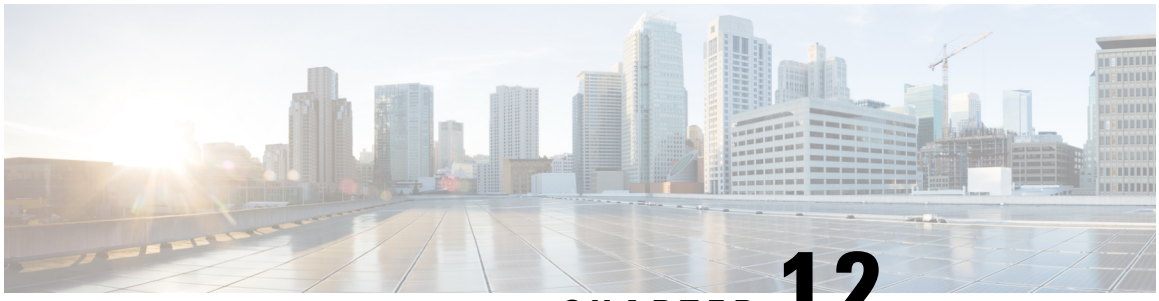
Step 5 Click **Update and Apply to Device**.

Setting AP Priority

Note Priority of access points ranges from 1 to 4, with 4 being the highest.

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **priority** *priority* **Example:** `Device# ap name AP44d3.ca52.48b5 priority 1`	Specifies the priority of an access point.
Step 2	**show ap config general** **Example:** `Device# show ap config general`	Displays common information for all access points.
Step 3	**show ap name** *ap-name* **config general** **Example:** `Device# show ap name AP44d3.ca52.48b5 config general`	Displays the configuration of a particular access point.



CHAPTER 12

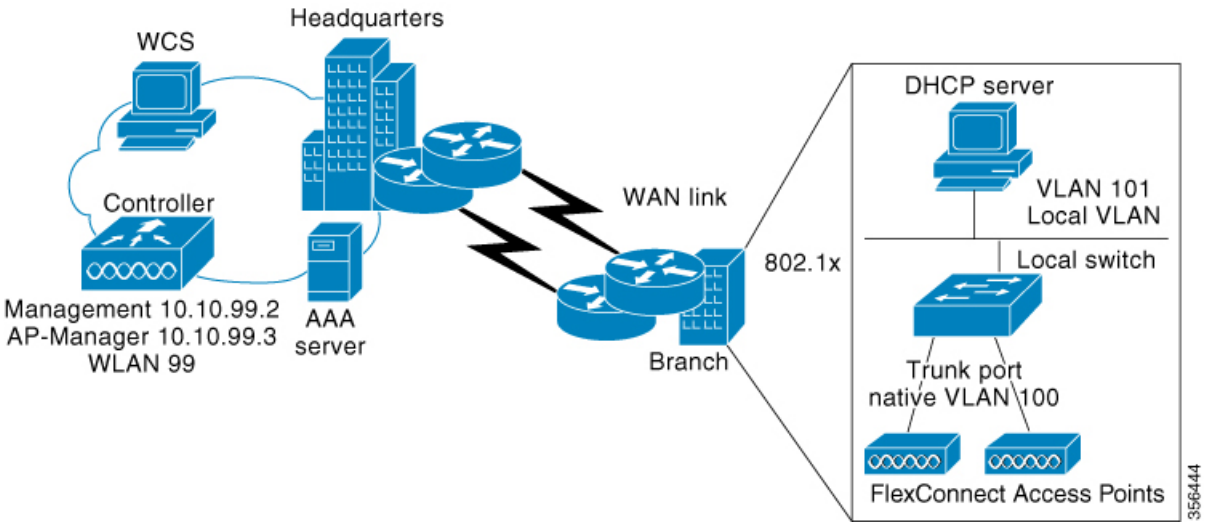
FlexConnect

- Information About FlexConnect, on page 81
- Guidelines and Restrictions for FlexConnect, on page 85
- Configuring a Site Tag, on page 88
- Configuring a Policy Tag (CLI), on page 89
- Attaching a Policy Tag and a Site Tag to an Access Point (GUI), on page 90
- Attaching Policy Tag and Site Tag to an AP (CLI), on page 91
- Linking an ACL Policy to the Defined ACL (GUI), on page 92
- Applying ACLs on FlexConnect, on page 92
- Configuring FlexConnect, on page 93
- Flex AP Local Authentication (GUI), on page 99
- Flex AP Local Authentication (CLI), on page 100
- Flex AP Local Authentication with External Radius Server, on page 102
- Configuration Example: FlexConnect with Central and Local Authentication , on page 105
- NAT-PAT for FlexConnect, on page 105
- Split Tunneling for FlexConnect, on page 109
- VLAN-based Central Switching for FlexConnect, on page 116
- OfficeExtend Access Points for FlexConnect, on page 118
- Proxy ARP, on page 121

Information About FlexConnect

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 also 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. FlexConnect access points support multiple SSIDs. In the connected mode, the FlexConnect access point can also perform local authentication.

Figure 3: 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 the 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 is 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 or new configured values only after the session timer expires.

The controller can send multicast packets in the form of unicast or multicast packets to an access point. In FlexConnect mode, an access point can receive only multicast packets.

In Cisco Catalyst 9800 Series Wireless Controller, you can define a flex connect site. A flex connect site can have a flex connect profile associate with it. You can have a maximum of 100 access points for each flex connect site.

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 or PAT boundary, except when you want true multicast to operate for all centrally switched WLANs.

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 an IPv4 operation. FlexConnect supports Client Mobility for a group of up to 100 access points.

An access point does not have to reboot when moving from local mode to FlexConnect mode and vice-versa.

FlexConnect Authentication

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 Aironet 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.

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:

Note For the FlexConnect local switching, central authentication deployments, whenever passive client is enabled, the IP Learn timeout is disabled by default.

- central authentication, central switching—In this state, the controller handles client authentication, and all client data is tunneled back to the controller. This state is valid only in connected mode.
- central authentication, local switching—In this state, the controller handles client authentication, and the FlexConnect access point switches data packets locally. After the client authenticates successfully, the controller sends a configuration command with a new payload to instruct the FlexConnect access point to start switching data packets locally. This message is sent per client. This state is applicable only in connected mode.
- 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. This 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.

Guidelines and Restrictions for FlexConnect

- 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.

This guideline is specific to Cisco Wave 1 APs, and not for Cisco Wave 2 APs or 11AX APs.

- FlexConnect mode can support only 16 VLANs per AP.
- You can deploy a FlexConnect access point with either a static IP address or a DHCP address. In the context 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 4 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 scenarios where you cannot achieve the 300-ms round-trip latency, 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. After the access point moves, the access point's radio is also reset.
- When multiple APs come from standalone mode to connected mode on flexconnect and all the APs send the client entry in hybrid-REAP payload to the controller. In this scenario, the controller sends disassociation messages to the WLAN client. However, the WLAN client comes back successfully and joins the controller.
- When APs are in standalone mode, if a client roams to another AP, the source AP cannot determine whether the client has roamed or is just idle. So, the client entry at source AP will not be deleted until idle timeout.
- 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 the secondary or backup controller must be the same.
- A newly connected access point cannot be booted in FlexConnect mode.
- 802.11r fast transition roaming is not supported on APs operating in local authentication.
- 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 you duplicate the SSID of the FlexConnect access point and its index number on both controllers.
- 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 the time of initialization, a few syslog packets from the access point are tagged with VLAN ID 1.
- 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 Cisco ISE.
- FlexConnect does not display any IPv6 client addresses in the Client Detail window.

- FlexConnect access points with locally switched WLANs cannot perform IP source guard and prevent ARP spoofing. For centrally switched WLANs, the wireless controller performs IP source guard and ARP spoofing.
- To prevent ARP spoofing attacks in FlexConnect APs with local switching, we recommend that you use ARP inspection.
- Passive client feature is not supported on FlexConnect local switching mode.
- When you enable local switching on policy profile for FlexConnect APs, the APs perform local switching. However, for the APs in local mode, central switching is performed.

  In a scenario where the roaming of a client between FlexConnect mode AP and Local mode AP is not supported, the client may not get the 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.

  FlexConnect local switching is not supported on Cisco Aironet Cisco 1810T and 1815T (Teleworker) Access Points.
- Cisco Centralized Key Management (CCKM) is not supported in FlexConnect standalone mode. Hence, CCKM enabled client will not be able to connect when AP is in FlexConnect standalone mode.
- For Wi-Fi Protected Access Version 2 (WPA2) in FlexConnect standalone mode or local authentication in connected mode or Cisco Centralized Key Management 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 Cisco Centralized Key Management 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 Cisco Centralized Key Management fast-roaming in connected mode.
- Only 802.11r fast-transition roaming is supported on the Cisco Aironet 1830 Series and 1850 Series APs.
- AVC on locally switched WLANs is supported on second-generation APs.
- Local authentication fallback is not supported when a user is not available in the external RADIUS server.
- For WLANs configured for FlexConnect APs in local switching and local authentication, synchronization of dot11 client information is supported.
- DNS override is not supported on the Cisco Aironet 1830 Series and 1850 Series APs.
- The Cisco Aironet 1830 Series and 1850 Series APs do not support IPv6. However, a wireless client can pass IPv6 traffic across these APs.
- VLAN group is not supported in Flex mode under flex-profile.
- Configuring maximum number of allowed media streams on individual client or radio is not supported in FlexConnect mode.
- The WLAN client association limit will not work when the AP is in FlexConnect mode (connected or standalone) and is performing local switching and local authentication.
- A local switching client on FlexConnect mode will not get IP address for RLAN profile on the Cisco Aironet 1810 Series AP.
- Standard ACL is not supported on FlexConnect AP mode.

- IPv6 RADIUS Server is not configurable for FlexConnect APs. Only IPv4 configuration is supported.
- Using custom VLANs under the policy profile of the FlexConnect locally switched WLANs stops the SSID broadcast. In such scenarios, run the **shut** and **no shut** commands on the policy profile to start the SSID broadcast.

  SSIDs are broadcasted when you:

  - Perform VLAN name to id mapping under FlexConnect profile and map the custom VLAN name under the policy profile.
  - Use VLAN id or standard VLAN name, for example, VLANxxxx.

- In the FlexConnect mode, NetFlow has a performance degradation impact on the Cisco Internetwork Operating System (IOS) AP models, especially on 2700, 3700, and 1700.
- From Cisco IOS XE Amsterdam 17.1.1 release onwards, the police rate per client in the flex connect APs in the controller, is represented as **rate_out** for Ingress (input) and **rate_in** for Egress (output). To verify police rate on the flex AP, use the **show rate-limit client** command.
- Cisco Wave 2 and Catalyst Wi-Fi6 APs in FlexConnect local switching mode do not support Layer2(PSK, 802.1X) + Layer3(LWA, CWA, redirection-based posturing) + Dynamic AAA override + NAC.
- Network access control (NAC) is not supported in FlexConnect local authentication.
- Multicast traffic on an AAA overridden VLAN is not supported. Using this configuration may result in potential traffic leaks between VLANs.

Configuring a Site Tag

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site default-site-tag`	Configures site tag and enters site tag configuration mode.
Step 3	**flex-profile** *flex-profile-name* **Example:** `Device(config-site-tag)# flex-profile rr-xyz-flex-profile`	Maps a flex profile to a site tag.
Step 4	**ap-profile** *ap-profile* **Example:**	Assigns an AP profile to the wireless site.

	Command or Action	Purpose
	`Device(config-site-tag)# ap-profile xyz-ap-profile`	
Step 5	**description** *site-tag-name* **Example:** `Device(config-site-tag)# description "default site tag"`	Adds a description for the site tag.
Step 6	**no local-site** **Example:** `Device(config-site-tag)# no local-site`	Moves the access point to FlexConnect mode.
Step 7	**end** **Example:** `Device(config-site-tag)# end`	Saves the configuration, exits the configuration mode, and returns to privileged EXEC mode.
Step 8	**show wireless tag site summary** **Example:** `Device# show wireless tag site summary`	(Optional) Displays the summary of site tags.

Configuring a Policy Tag (CLI)

Follow the procedure given below to configure a policy tag:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wireless tag policy** *policy-tag-name* **Example:** `Device(config-policy-tag)# wireless tag policy default-policy-tag`	Configures policy tag and enters policy tag configuration mode. **Note** When performing LWA, the clients connected to a controller gets disconnected intermittently before session timeout.

	Command or Action	Purpose
Step 4	**description** *description* **Example:** `Device(config-policy-tag)# description "default-policy-tag"`	Adds a description to a policy tag.
Step 5	**remote-lan** *name* **policy** *profile-policy-name* {**ext-module**| **port-id** } **Example:** `Device(config-policy-tag)# remote-lan rr-xyz-rlan-aa policy rr-xyz-rlan-policy1 port-id 2`	Maps a remote-LAN profile to a policy profile.
Step 6	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan rr-xyz-wlan-aa policy rr-xyz-policy-1`	Maps a policy profile to a WLAN profile.
Step 7	**end** **Example:** `Device(config-policy-tag)# end`	Exits policy tag configuration mode, and returns to privileged EXEC mode.
Step 8	**show wireless tag policy summary** **Example:** `Device# show wireless tag policy summary`	(Optional) Displays the configured policy tags. **Note** To view detailed information about a policy tag, use the **show wireless tag policy detailed** *policy-tag-name* command.

Attaching a Policy Tag and a Site Tag to an Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 Click the **Access Point** name.

Step 3 Go to the **Tags** section.

Step 4 Choose the **Policy Tag** from the **Policy** drop-down list.

Step 5 Choose the **Site Tag** from the **Site** drop-down list.

Step 6 Click **Update and Apply to Device**.

Attaching Policy Tag and Site Tag to an AP (CLI)

Follow the procedure given below to attach a policy tag and a site tag to an AP:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures a Cisco AP and enters AP profile configuration mode. **Note** The *mac-address* should be a wired mac address.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag rr-xyz-policy-tag`	Maps a policy tag to the AP.
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag rr-xyz-site`	Maps a site tag to the AP.
Step 5	**rf-tag** *rf-tag-name* **Example:** `Device(config-ap-tag)# rf-tag rf-tag1`	Associates the RF tag.
Step 6	**end** **Example:** `Device(config-ap-tag)# end`	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.
Step 7	**show ap tag summary** **Example:** `Device# show ap tag summary`	(Optional) Displays AP details and the tags associated to it.
Step 8	**show ap name** <*ap-name*> **tag info** **Example:** `Device# show ap name ap-name tag info`	(Optional) Displays the AP name with tag information.
Step 9	**show ap name** <*ap-name*> **tag detail** **Example:**	(Optional) Displays the AP name with tag detals.

	Command or Action	Purpose
	`Device# show ap name ap-name tag detail`	

Linking an ACL Policy to the Defined ACL (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** of the Flex Profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 In the **Policy ACL** tab, click **Add**.

Step 5 Select the ACL from the **ACL Name** drop-down list and click **Save**.

Step 6 Click **Apply to Device**.

Applying ACLs on FlexConnect

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex Flex-profile-1`	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	**acl-policy** *acl-policy-name* **Example:** `Device(config-wireless-flex-profile)# acl-policy ACL1`	Configures an ACL policy. Access control lists (ACLs) perform packet filtering to control the movement of packets through a network.
Step 4	**exit** **Example:** `Device(config-wireless-flex-profile-acl)# exit`	Returns to wireless flex profile configuration mode.

	Command or Action	Purpose
Step 5	**native-vlan-id** **Example:** `Device(config-wireless-flex-profile)# native-vlan-id 25`	Configures native vlan-id information.
Step 6	**vlan** *vlan-name* **Example:** `Device(config-wireless-flex-profile)# vlan-name VLAN0169`	Configures a VLAN.
Step 7	**acl** *acl-name* **Example:** `Device(config-wireless-flex-profile-vlan)# acl ACL1`	Configures an ACL for the interface.
Step 8	**vlan-id***vlan-id* **Example:** `Device(config-wireless-flex-profile-vlan)# vlan-id 169`	Configures VLAN information.

Configuring FlexConnect

Configuring a Switch at a Remote Site

Procedure

Step 1 Attach the access point, which will be enabled for FlexConnect, to a trunk or access port on the switch.

Note The sample configuration in this procedure shows the FlexConnect access point connected to a trunk port on the switch.

Step 2 The following example configuration shows you how to configure a switch to support a FlexConnect access point.

In this sample configuration, the FlexConnect access point is connected to the trunk interface FastEthernet 1/0/2 with native VLAN 100. The access point needs IP connectivity on the native VLAN. The remote site has local servers or resources on VLAN 101. A DHCP pool is created in the local switch for both the VLANs in the switch. The first DHCP pool (NATIVE) is used by the FlexConnect access point, and the second DHCP pool (LOCAL-SWITCH) is used by the clients when they associate to a WLAN that is locally switched.

```
.
.
.
ip dhcp pool NATIVE
   network 209.165.200.224 255.255.255.224
```

```
   default-router 209.165.200.225
   dns-server 192.168.100.167
!
ip dhcp pool LOCAL-SWITCH
   network 209.165.201.224 255.255.255.224
   default-router 209.165.201.225
   dns-server 192.168.100.167
!
interface Gig1/0/1
 description Uplink port
 no switchport
 ip address 209.165.202.225 255.255.255.224
!
interface Gig1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 101
 switchport mode trunk
!
interface Vlan100
 ip address 209.165.200.225 255.255.255.224
!
interface Vlan101
 ip address 209.165.201.225 255.255.255.224
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 3: WLAN Scenarios

WLAN	Security	Authentication	Switching	Interface Mapping (GUEST VLAN)
Employee	WPA1+WPA2	Central	Central	Management (centrally switched GUEST VLAN)
Employee-local	WPA1+WPA2 (PSK)	Local	Local	101 (locally switched GUEST VLAN)
Guest-central	Web authentication	Central	Central	Management (centrally switched GUEST VLAN)

WLAN	Security	Authentication	Switching	Interface Mapping (GUEST VLAN)
Employee-local-auth	WPA1+WPA2	Local	Local	101 (locally switched VLAN)

Configuring Local Switching in FlexConnect Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, click the name of a policy profile to edit it or click **Add** to create a new one.

Step 3 In the **Add/Edit Policy Profile** window that is displayed, uncheck the **Central Switching** and the **Central Association** check boxes.

Step 4 Click **Update & Apply to Device**.

Configuring Local Switching in FlexConnect Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**no central switching** **Example:** `Device(config-wireless-policy)# no central switching`	Configures the WLAN for local switching.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Central Switching in FlexConnect Mode (GUI)

Before you begin

Ensure that the policy profile is configured. If the policy profile is not configured, see *Configuring a Policy Profile (GUI)* section.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, select a policy.

Step 3 In the **Edit Policy Profile** window, in General Tab, use the slider to enable or disable **Central Switching**.

Step 4 Click **Update & Apply to Device**.

Configuring Central Switching in FlexConnect Mode

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures the WLAN for central switching.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring an Access Point for FlexConnect

For more information, see *Configuring a Site Tag (CLI)* topic in New Configuration Model chapter.

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

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 In the **Policy Profile** page, select a policy profile name. The **Edit Policy Profile** window is displayed.

Step 3 In the General tab, deselect **Central Authentication** check box.

Step 4 Click **Update & Apply to Device**.

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**no central authentication** **Example:** `Device(config-wireless-policy)# no central authentication`	Configures the WLAN for local authentication.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Connecting Client Devices to WLANs

Follow the instructions for your client device to create profiles to connect to the WLANs you created, as specified in the Configuring the Controller for FlexConnect, on page 94 .

In the example scenarios (see Configuring the Controller for FlexConnect, on page 94), there are three profiles on the client:

1. To connect to the *employee* WLAN, create a client profile that uses WPA or WPA2 with PEAP-MSCHAPV2 authentication. After the client is authenticated, the client is allotted an IP address by the management VLAN of the controller .

2. To connect to the *local-employee* WLAN, create a client profile that uses WPA or WPA2 authentication. After the client is authenticated, the client is allotted an IP address by VLAN 101 on the local switch.
3. To connect to the *guest-central* WLAN, create a client profile that uses open authentication. After the client is authenticated, the client is allocatted an IP address by VLAN 101 on the network local to the access point. After the client connects, a local user can enter any HTTP address in the web browser. The user is automatically directed to the controller to complete the web authentication process. When the web login window appears, the user should enter the username and password.

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.

Configuring FlexConnect Ethernet Fallback

Before you begin

This feature is not applicable to APs with multiple ports.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex test`	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	**fallback-radio-shut** **Example:** `Device(config-wireless-flex-profile)# fallback-radio-shut`	Enables radio interface shutdown.
Step 4	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**show wireless profile flex detailed** *flex-profile-name* **Example:** `Device# show wireless profile flex detailed test`	(Optional) Displays detailed information about the selected profile.

Flex AP Local Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 In the **Flex** page, click the name of the **Flex Profile** or click **Add** to create a new one.

Step 3 In the **Add/Edit Flex Profle** window that is displayed, click the **Local Authentication** tab.

When local authentication and association is enabled in Access Point with Flex mode, the following occurs:

- AP handles the authentication.
- AP handles the rejection of client joins (in Mobility).

Note The controller does not increment statistics when AP rejects client association.

Step 4 Choose the server group from the **RADIUS Server Group** drop-down list.

Step 5 Use the **Local Accounting Radius Server Group** drop down to select the RADIUS server group.

Step 6 Check the **Local Client Roaming** check box to enable client roaming.

Step 7 Choose the profile from the **EAP Fast Profile** drop-down list.

Step 8 Choose to enable or disable the following:

- LEAP: Lightweight Extensible Authentication Protocol (LEAP) is an 802.1X authentication type for wireless LANs and supports strong mutual authentication between the client and a RADIUS server using a logon password as the shared secret. It provides dynamic per-user, per-session encryption keys.
- PEAP: Protected Extensible Authentication Protocol (PEAP) is a protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel.
- TLS: Transport Layer Security (TLS) is a cryptographic protocol that provide communications security over a computer network.
- RADIUS: Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.

Step 9 In the **Users** section, click **Add**.

Step 10 Enter username and password details and click **Save**.

Step 11 Click **Save & Apply to Device**.

Flex AP Local Authentication (CLI)

Note The Cisco Catalyst 9800 Series Wireless Controller + FlexConnect local authentication + AP acting as RADIUS are not supported on Cisco COS and IOS APs.

Procedure

	Command or Action	Purpose
Step 1	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Creates a AAA authentication model.
Step 2	**aaa session-id common** **Example:** `Device(config)# aaa session-id common`	Ensures that all the session IDs information that is sent out from the RADIUS group for a given call are identical.
Step 3	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Enables system authorization control for the RADIUS group.
Step 4	**eap profile** *name* **Example:** `Device(config)# eap profile aplocal-test`	Creates an EAP profile.
Step 5	**method fast** **Example:** `Device(config-eap-profile)# method fast`	Configures the FAST method on the profile.
Step 6	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to configuration mode.
Step 7	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Configures the flex policy.
Step 8	**local-auth ap eap-fast** *name* **Example:**	Configures EAP-FAST profile details.

	Command or Action	Purpose
	`Device(config-wireless-flex-profile)# local-auth ap eap-fast aplocal-test`	
Step 9	**local-auth ap leap** **Example:** `Device(config-wireless-flex-profile)# local-auth ap leap`	Configures the LEAP method.
Step 10	**local-auth ap peap** **Example:** `Device(config-wireless-flex-profile)# local-auth ap peap`	Configures the PEAP method.
Step 11	**local-auth ap username** *username* **Example:** `Device(config-wireless-flex-profile)# local-auth ap username test1 test1`	Configures username and password.
Step 12	**local-auth ap username** *username password* **Example:** `Device(config-wireless-flex-profile)# local-auth ap username test2 test2`	Configures another username and password.
Step 13	**exit** **Example:** `Device(config-wireless-flex-profile)# exit`	Returns to configuration mode.
Step 14	**wireless profile policy** *policy-profile* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures profile policy.
Step 15	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables the policy profile.
Step 16	**no central authentication** **Example:** `Device(config)# no central authentication`	Disables central (controller) authentication.
Step 17	**vlan-id** *vlan-id* **Example:** `Device(config)# vlan-id 54`	Configures VLAN name or VLAN ID.

	Command or Action	Purpose
Step 18	**no shutdown** **Example:** `Device(config)# no shutdown`	Enables the configuration.

Flex AP Local Authentication with External Radius Server

In this mode, an access point handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode.

Procedure

	Command or Action	Purpose
Step 1	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Creates a AAA authentication model.
Step 2	**aaa session-id common** **Example:** `Device(config)# aaa session-id common`	Ensures that all the session ID's information that is sent out, from the RADIUS group for a given call are identical.
Step 3	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Enables the system authorization control for the RADIUS group.
Step 4	**radius server** *server-name* **Example:** `Device(config)# radius server Test-SERVER1`	Specifies the RADIUS server name. **Note** To authenticate clients with freeradius over RADSEC, you should generate an RSA key longer than 1024 bit. Use the **crypto key generate rsa general-keys exportable label** *name* command to achieve this. Do not configure **key-wrap** option under the radius server and radius server group, as it may lead to clients getting stuck in authentication state.
Step 5	**address {ipv4 | ipv6}** *ip address* {**auth-port** *port-number* | **acct-port** *port-number* } **Example:**	Specifies the primary RADIUS server parameters.

	Command or Action	Purpose
	`Device(config-radius-server)# address ipv4 124.3.50.62 auth-port 1112 acct-port 1113` `Device(config-radius-server)# address ipv6 2001:DB8:0:20::15 auth-port 1812 acct-port 1813`	
Step 6	**key** *string* **Example:** `Device(config-radius-server)# key test123`	Specifies the authentication and encryption key used between the device and the RADIUS daemon running on the RADIUS server. **Note** The maximum number of characters allowed for the shared secret is 63.
Step 7	**radius server** *server-name* **Example:** `Device(config)# radius server Test-SERVER2`	Specifies the RADIUS server name.

Step 8	**address {ipv4 | ipv6}** *ip address* {**auth-port** *port-number* | **acct-port** *port-number* }
	Example:
	`Device(config-radius-server)# address ipv4 124.3.52.62 auth-port 1112 acct-port 1113`
	`Device(config-radius-server)# address ipv6 2001:DB8:0:21::15 auth-port 1812 acct-port 1813`
		Specifies the secondary RADIUS server parameters.

Step 9	**key** *string* **Example:** `Device(config-radius-server)# key test113`	Specifies the authentication and encryption key used between the device and the RADIUS daemon running on the RADIUS server.
Step 10	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to configuration mode.
Step 11	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius aaa_group_name`	Creates a RADIUS server group identification.
Step 12	**radius server** *server-name* **Example:** `Device(config)# radius server Test-SERVER1`	Specifies the RADIUS server name.

	Command or Action	Purpose
Step 13	**radius server** *server-name* **Example:** `Device(config-radius-server)# radius server Test-SERVER2`	Specifies the RADIUS server name.
Step 14	**exit** **Example:** `Device(config-radius-server)# exit`	Exit from RADIUS server configuration mode.
Step 15	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Creates a new flex policy.
Step 16	**local-auth radius-server-group** *server-group* **Example:** `Device(config-wireless-flex-profile)# local-auth radius-server-group aaa_group_name`	Configures the authentication server group name.
Step 17	**exit** **Example:** `Device(config-wireless-flex-profile)# exit`	Returns to configuration mode.
Step 18	**wireless profile policy** *policy-profile* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures a WLAN policy profile.
Step 19	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables a policy profile.
Step 20	**no central authentication** **Example:** `Device(config-wireless-policy)# no central authentication`	Disables central (controller) authentication.
Step 21	**vlan-id** *vlan-id* **Example:** `Device(config-wireless-policy)# vlan-id 54`	Configures a VLAN name or VLAN Id.
Step 22	**no shutdown** **Example:**	Enables the configuration.

	Command or Action	Purpose
	`Device(config-wireless-policy)# no shutdown`	

Configuration Example: FlexConnect with Central and Local Authentication

To see configuration example on how to configure a controller for FlexConnect central and local authentication, see the FlexConnect Configuration with Central and Local Authentication on Catalyst 9800 Wireless Controllers document.

NAT-PAT for FlexConnect

If you want to use a central DHCP server to service clients across remote sites, NAT-PAT should be enabled.

An AP translates the traffic coming from a client and replaces the client's IP address with its own IP address.

Note You must enable local switching, central DHCP, and DHCP required using the (**ipv4 dhcp required**) command to enable NAT and PAT.

Configuring NAT-PAT for a WLAN or a Remote LAN

Creating a WLAN

Follow the steps given here to create a WLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-demo 1 ssid-demo`	Enters the WLAN configuration sub-mode. • *wlan-name*—Enter the profile name. The range is from 1 to 32 alphanumeric characters. • *wlan-id*—Enter the WLAN ID. The range is from 1 to 512. • *SSID-name*—Enter the Service Set Identifier (SSID) for this WLAN. If the

	Command or Action	Purpose
		SSID is not specified, the WLAN profile name is set as the SSID. **Note** If you have already configured WLAN, enter *wlan wlan-name* command.
Step 3	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Shut down the WLAN.
Step 4	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Wireless Profile Policy and NAT-PAT (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.
Step 2 Click **Add**.
Step 3 In the **General** tab, enter the **Name** of the policy.
Step 4 Disable the **Central Switching** toggle button.
Step 5 Enable the **Central DHCP** toggle button.
Step 6 Enable the **Flex NAT/PAT** toggle button.
Step 7 In the **Advanced** tab, under the **DHCP** Settings, check the **IPv4 DHCP Required** check box.
Step 8 Click **Apply to Device**.

Configuring a Wireless Profile Policy and NAT-PAT

Follow the procedure given below to configure a wireless profile policy and NAT-PAT:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:**	Configures the policy profile for NAT.

	Command or Action	Purpose
	`Device(config)# wireless profile policy nat-enabled-policy`	
Step 3	**no central switching** **Example:** `Device(config-wireless-policy)# no central switching`	Configures the WLAN for local switching.
Step 4	**ipv4 dhcp required** **Example:** `Device(config-wireless-policy)# ipv4 dhcp required`	Configures the DHCP parameters for WLAN.
Step 5	**central dhcp** **Example:** `Device(config-wireless-policy)# central dhcp`	Configures the central DHCP for locally switched clients.
Step 6	**flex nat-pat** **Example:** `Device(config-wireless-policy)# flex nat-pat`	Enables NAT-PAT.
Step 7	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables policy profile.
Step 8	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Mapping a WLAN to a Policy Profile

Follow the procedure given below to map a WLAN to a policy profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config)# wireless tag policy demo-tag`	Configures a policy tag and enters policy tag configuration mode.

	Command or Action	Purpose
Step 3	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan wlan-demo policy nat-enabled-policy`	Maps a policy profile to a WLAN profile.
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Site Tag

Follow the procedure given below to configure a site tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site flex-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**no local-site** **Example:** `Device(config-site-tag)# no local-site`	Moves an access point to FlexConnect mode.
Step 4	**end** **Example:** `Device(config-site-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Attaching a Policy Tag and a Site Tag to an Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.
Step 2 Click the **Access Point** name.
Step 3 Go to the **Tags** section.
Step 4 Choose the **Policy Tag** from the **Policy** drop-down list.
Step 5 Choose the **Site Tag** from the **Site** drop-down list.

Step 6 Click **Update and Apply to Device**.

Attaching a Policy Tag and a Site Tag to an Access Point

Follow the procedure given below to attach a policy tag and a site tag to an access point:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures Cisco APs and enters ap-tag configuration mode.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag demo-tag`	Maps a policy tag to the AP.
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag flex-site`	Maps a site tag to the AP.
Step 5	**end** **Example:** `Device(config-ap-tag)# end`	Returns to privileged EXEC mode.

Split Tunneling for FlexConnect

If a client that connects over a WAN link that is associated with a centrally switched WLAN has to send traffic to a device present in the local site, this traffic should be sent over CAPWAP to the controller, and the same traffic is sent back to the local site either over CAPWAP or with the help of some off-band connectivity.

This process consumes WAN link bandwidth unnecessarily. To avoid this, 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 policy profile using the (**ipv4 dhcp required**) command. This ensures that the client that is associating with the split WLAN does DHCP.

Note Apple iOS clients need option 6 (DNS) to be set in DHCP offer for split tunneling to work.

Note

- FlexConnect split tunneling (vlan-based central switching for flexconnect) on auto-anchor deployment is not supported.
- Split tunneling does not work on RLAN clients. When the **split-tunnel** option is enabled on RLAN, traffic denied by the split tunnel ACL is not translated based on the IP address, instead the traffic is sent back to the controller through CAPWAP.
- URL filter must not be configured with wildcard URLs such as * and *.*

Configuring Split Tunneling for a WLAN or Remote LAN

Defining an Access Control List for Split Tunneling (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **ACL**.

Step 2 Click **Add**.

Step 3 In the **Add ACL Setup** dialog box, enter the **ACL Name**.

Step 4 Choose the ACL type from the **ACL Type** drop-down list.

Step 5 Under the **Rules** settings, enter the **Sequence** number and choose the **Action** as either **permit** or **deny**.

Step 6 Choose the required source type from the **Source Type** drop-down list.

a) If you choose the source type as **Host**, then you must enter the **Host Name/IP**.

b) If you choose the source type as **Network**, then you must specify the **Source IP** address and **Source Wildcard** mask.

Step 7 Check the **Log** check box if you want the logs.

Step 8 Click **Add**.

Step 9 Add the rest of the rules and click **Apply to Device**.

Defining an Access Control List for Split Tunneling

Follow the procedure given below to define an Access Control List (ACL) for split tunneling:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended** *name* **Example:** `Device(config)# ip access-list extended split_mac_acl`	Defines an extended IPv4 access list using a name, and enters access-list configuration mode.
Step 3	**deny ip any host** *hostname* **Example:** `Device(config-ext-nacl)# deny ip any host 9.9.2.21`	Allows the traffic to switch centrally.
Step 4	**permit ip any any** **Example:** `Device(config-ext-nacl)# permit ip any any`	Allows the traffic to switch locally.
Step 5	**end** **Example:** `Device(config-ext-nacl)# end`	Exits configuration mode and returns to privileged EXEC mode.

Linking an ACL Policy to the Defined ACL

Follow the procedure given below to link an ACL policy to the defined ACL:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex flex-profile`	Configures the Flex profile and enters flex profile configuration mode.
Step 3	**acl-policy** *acl policy name* **Example:** `Device(config-wireless-flex-profile)# acl-policy split_mac_acl`	Configures an ACL policy for the defined ACL.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Creating a WLAN

Follow the procedure given below to create a WLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-demo 1 ssid-demo`	Specifies the WLAN name and ID: • *wlan-name*—Enter the profile name. The range is from 1 to 32 alphanumeric characters. • *wlan-id*—Enter the WLAN ID. The range is from 1 to 512. • *SSID-name*—Enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.
Step 3	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 4	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Wireless Profile Policy and a Split MAC ACL Name (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** of the policy.

Step 4 Enable the **Central Switching** toggle button.

Step 5 Enable the **Central DHCP** toggle button.

Step 6 In the **Advanced** tab, under the **DHCP** settings, check the **IPv4 DHCP Required** check box and enter the **DHCP Server IP Address**.

Step 7 Under the **WLAN Flex Policy** setttings, choose the split MAC ACL from the **Split MAC ACL** drop-down list.

Step 8 Click **Apply to Device**.

Configuring a Wireless Profile Policy and a Split MAC ACL Name

Follow the procedure given below to configure a wireless profile policy and a split MAC ACL name:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy split-tunnel-enabled-policy`	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 3	**flex split-mac-acl** *split-mac-acl-name* **Example:** `Device(config-wireless-policy)# flex split-mac-acl split_mac_acl`	Configures a split MAC ACL name. **Note** You should use the same ACL name for linking the flex and the policy profile.
Step 4	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures WLAN for central switching.
Step 5	**central dhcp** **Example:** `Device(config-wireless-policy)# central dhcp`	Enables central DHCP for centrally switched clients.
Step 6	**ipv4 dhcp required** **Example:** `Device(config-wireless-policy)# ipv4 dhcp required`	Configures the DHCP parameters for a WLAN.
Step 7	**ipv4 dhcp server** *ip_address* **Example:**	Configures the override IP address of the DHCP server.

	Command or Action	Purpose
	`Device(config-wireless-policy)# ipv4 dhcp server 9.1.0.100`	
Step 8	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables a policy profile.

Mapping a WLAN to a Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.
Step 2 Click **Add**.
Step 3 Enter the **Name** of the Tag Policy.
Step 4 Under **WLAN-POLICY Maps** tab, click **Add** .
Step 5 Choose the WLAN Profile from the **WLAN Profile** drop-down list.
Step 6 Choose the Policy Profile from the **Policy Profile** drop-down list.
Step 7 Click the **Tick** Icon .
Step 8 Click **Apply to Device**.

Mapping WLAN to a Policy Profile

Follow the procedure given below to map WLAN to a policy profile.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config)# wireless tag policy split-tunnel-enabled-tag`	Configures a policy tag and enters policy tag configuration mode.
Step 3	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan wlan-demo policy split-tunnel-enabled-policy`	Maps a policy profile to a WLAN profile.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Site Tag

Follow the procedure given below to configure a site tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site flex-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**no local-site** **Example:** `Device(config-site-tag)# no local-site`	**Local site** is not configured on the site tag.
Step 4	**flex-profile** *flex-profile-name* **Example:** `Device(config-site-tag)# flex-profile flex-profile`	Configures a flex profile.
Step 5	**end** **Example:** `Device(config-site-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Attaching a Policy Tag and Site Tag to an Access Point

Follow the procedure given below to attach a policy tag and site tag to an access point.

Procedure

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

	Command or Action	Purpose
Step 2	**ap** *ethernet-mac-address* **Example:** `Device(config)# ap 188b.9dbe.6eac`	Configures an AP and enters ap tag configuration mode.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag split-tunnel-enabled-tag`	Maps a policy tag to an AP.
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag flex-site`	Maps a site tag to an AP.
Step 5	**end** **Example:** `Device(config-ap-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

VLAN-based Central Switching for FlexConnect

In FlexConnect local switching, if the VLAN definition is not available in an access point, the corresponding client does not pass traffic. This scenario is applicable when the AAA server returns the VLAN as part of client authentication.

When a WLAN is locally switched in flex and a VLAN is configured on the AP side, the traffic is switched locally. When a VLAN is not defined in an AP, the VLAN drops the packet.

When VLAN-based central switching is enabled, the corresponding AP tunnels the traffic back to the controller. The controller then forwards the traffic to its corresponding VLAN.

Note

- For VLAN-based central switching, ensure that VLAN is defined on the controller.
- VLAN-based central switching is not supported by mac filter.
- For local switching, ensure that VLAN is defined on the policy profile and FlexConnect profile.
- VLAN-based central switching with central web authentication enabled in Flex profile is not supported.

Configuring VLAN-based Central Switching (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the name of the policy profile.

Step 3 In the **Edit Policy Profile** window, perform these tasks:

a) Set **Central Switching** to **Disabled** state.
b) Set **Central DHCP** to **Disabled** state.
c) Set **Central Authentication** to **Enabled** state.

Step 4 Click the **Advanced** tab.

Step 5 Under **AAA Policy**, check the **Allow AAA Override** check box to enable AAA override.

Step 6 Under **WLAN Flex Policy**, check the **VLAN Central Switching** check box, to enable VLAN-based central switching on the policy profile.

Step 7 Click **Update & Apply to Device**.

Configuring VLAN-based Central Switching (CLI)

Follow the procedure given below to configure VLAN-based central switching.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures a wireless policy profile.
Step 3	**no central switching** **Example:** `Device(config-wireless-policy)# no central switching`	Configures a WLAN for local switching.
Step 4	**no central dhcp** **Example:** `Device(config-wireless-policy)# no central dhcp`	Configures local DHCP mode, where the DHCP is performed in an AP.
Step 5	**central authentication** **Example:** `Device(config-wireless-policy)# central authentication`	Configures a WLAN for central authentication.
Step 6	**aaa-override** **Example:**	Configures AAA policy override.

	Command or Action	Purpose
	`Device(config-wireless-policy)# aaa-override`	
Step 7	**flex vlan-central-switching** **Example:** `Device(config-wireless-policy)# flex vlan-central-switching`	Configures VLAN-based central switching.
Step 8	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.
Step 9	**show wireless profile policy detailed** *default-policy-profile* **Example:** `Device# show wireless profile policy detailed default-policy-profile`	(Optional) Displays detailed information of the policy profile.

OfficeExtend Access Points for FlexConnect

A Cisco OfficeExtend access point (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. A 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 an access point and the controller ensures that all communications have the highest level of security.

Note Preconfigure the controller IP for a zero-touch deployment with OEAP. All other home users can use the same access point to connect for home use by configuring the local SSID from AP.

Note In releases prior to Cisco IOS XE Amsterdam 17.3.2, when an AP is converted to OEAP, the local DHCP server on the AP is enabled by default. If the DHCP server on home router has a similar configuration, a network conflict occurs and AP will not be able to join back to the controller. In such a scenario, we recommend that you change the default DHCP server on the Cisco AP using OEAP GUI.

Note In Cisco OfficeExtend access point (Cisco OEAP), if the OEAP local DHCP server is enabled and the user configures DNS IP from OEAP GUI, the wireless and wired clients connected to Cisco OEAP will receive that IP as DNS server IP in DHCP ACK.

Configuring OfficeExtend Access Points

Follow the procedure given below to configure OfficeExtend access points.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex test`	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	**office-extend** **Example:** `Device(config-wireless-flex-profile)# office-extend`	Enables the OfficeExtend AP mode for a flexconnect AP.
Step 4	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits configuration mode and returns to privileged EXEC mode. **Note** After creating a flex profile, ensure that OEAP is in flex connect mode and mapped to its corresponding site tag. OfficeExtend is disabled by default. To clear the access point's configuration and return it to the factory-defaults, use the **clear ap config** *cisco-ap* command.

Disabling OfficeExtend Access Point

Follow the procedure given below to disable an OfficeExtend access point.

Procedure

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

	Command or Action	Purpose
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex test`	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	**no office-extend** **Example:** `Device(config-wireless-flex-profile)# no office-extend`	Disables OfficeExtend AP mode for a flexconnect AP.
Step 4	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Clearing Personal SSID from an OfficeExtend Access Point

To clear the personal SSID from an access point, run the following command:

ap name *Cisco_AP* **clear-personal-ssid**

Example: Viewing OfficeExtend Configuration

This example displays an OfficeExtend configuration:

```
Device# show ap config general

Cisco AP Name   : ap_name
=================================================

Cisco AP Identifier                              : 70db.986d.a860
Country Code                                     : Multiple Countries : US,IN
Regulatory Domain Allowed by Country             : 802.11bg:-A   802.11a:-ABDN
AP Country Code                                  : US  - United States
AP Regulatory Domain
  Slot 0                                         : -A
  Slot 1                                         : -D
MAC Address                                      : 002c.c899.7b84
IP Address Configuration                         : DHCP
IP Address                                       : 9.9.48.51
IP Netmask                                       : 255.255.255.0
Gateway IP Address                               : 9.9.48.1
CAPWAP Path MTU                                  : 1485
Telnet State                                     : Disabled
SSH State                                        : Disabled
Jumbo MTU Status                                 : Disabled
Cisco AP Location                                : default location
Site Tag Name                                    : flex-site
RF Tag Name                                      : default-rf-tag
Policy Tag Name                                  : split-tunnel-enabled-tag
AP join Profile                                  : default-ap-profile
Primary Cisco Controller Name                    : uname-controller
Primary Cisco Controller IP Address              : 9.9.48.34
```

```
Secondary Cisco Controller Name                 : uname-controller1
Secondary Cisco Controller IP Address           : 0.0.0.0
Tertiary Cisco Controller Name                  : uname-ewlc2
Tertiary Cisco Controller IP Address            : 0.0.0.0
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : FlexConnect
AP Submode                                      : Not Configured
Office Extend Mode                              : Enabled
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : information
Software Version                                : 16.8.1.1
Boot Version                                    : 1.1.2.4
Mini IOS Version                                : 0.0.0.0
Stats Reporting Period                          : 0
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : PoE/Full Power (normal mode)
```

Proxy ARP

Proxy address resolution protocol (ARP) is the most common method for learning about MAC address through a proxy device. Enabling Proxy ARP known as ARP caching in Cisco Catalyst 9800 Series Wireless Controller means that the AP owning client is the destination of the ARP request, replies on behalf of that client and therefore does not send the ARP request to the client over the air. Access points not owning the destination client and receiving an ARP request through their wired connection will drop the ARP request. When the ARP caching is disabled, the APs bridge the ARP requests from wired-to-wireless and vice-versa increasing the air time usage and broadcasts over wireless.

The AP acts as an ARP proxy to respond to ARP requests on behalf of the wireless clients.

Enabling Proxy ARP for FlexConnect APs (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** of the Flex Profile and check the **ARP Caching** check box. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

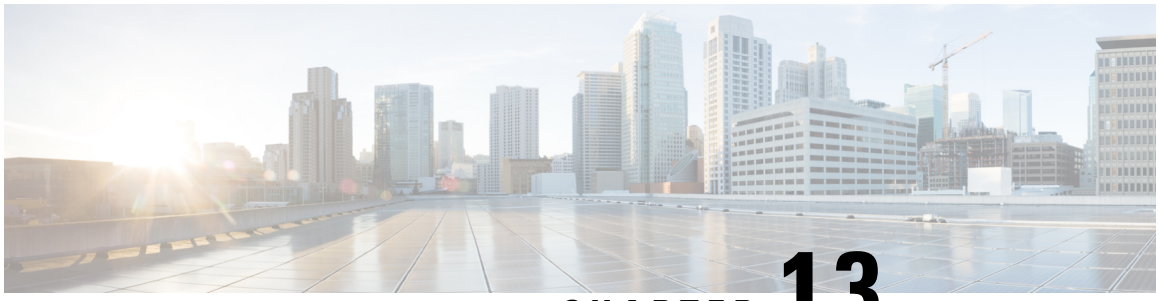
Step 4 Click **Apply to Device**.

Enabling Proxy ARP for FlexConnect APs

Follow the procedure given below to configure proxy ARP for FlexConnect APs.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-policy* **Example:** `Device(config)# wireless profile flex flex-test`	Configures WLAN policy profile and enters wireless flex profile configuration mode.
Step 3	**arp-caching** **Example:** `Device(config-wireless-flex-profile)# arp-caching`	Enables ARP caching. **Note** Use the **no arp-caching** command to disable ARP caching.
Step 4	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config | section wireless profile flex** **Example:** `Device# show running-config | section wireless profile flex`	Displays ARP configuration information.
Step 6	**show wireless profile flex detailed** *flex-profile-name* **Example:** `Device# show wireless profile flex detailed flex-test`	(Optional) Displays detailed information of the flex profile.
Step 7	**show arp summary** **Example:** `Device# show arp summary`	(Optional) Displays ARP summary.



CHAPTER 13

Data DTLS

- Information About Data Datagram Transport Layer Security, on page 123
- Configuring Data DTLS (GUI), on page 123
- Configuring Data DTLS (CLI), on page 124

Information About Data Datagram Transport Layer Security

Data Datagram Transport Layer Security (DTLS) enables you to encrypt CAPWAP data packets that are sent between an access point and the controller using DTLS, which is a standards-track IETF protocol that can encrypt both control and data packets based on TLS. CAPWAP control packets are management packets that are 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.

If an access point supports Data DTLS, it enables data DTLS after receiving the new configuration from the controller . The access point performs a DTLS handshake on port 5247 and after successfully establishing the DTLS session. All the data traffic (from the access point to the controller and the controller to the access point) is encrypted.

Note The throughput is affected for some APs that have data encryption enabled.

Note If the AP's DHCP lease time is less and the DHCP pool is small, access point join failure or failure in establishing the Data Datagram Transport Layer Security (DTLS) session may occur. In such scenarios, associate the AP with a named site-tag and increase the DHCP lease time for at least 8 days.

Configuring Data DTLS (GUI)

Follow the procedure to enable DTLS data encryption for the access points on the controller :

Procedure

Step 1 Click **Configuration** > **Tags and Profile** > **AP Join**.

Step 2 Click **Add** to create a new **AP Join Profile** or click an existing profile to edit it.

Step 3 Click **CAPWAP** > **Advanced**.

Step 4 Check **Enable Data Encryption** check box to enable Datagram Transport Layer Security (DTLS) data encryption.

Step 5 Click **Update & Apply to Device**.

Configuring Data DTLS (CLI)

Follow the procedure given below to enable DTLS data encryption for the access points on the controller :

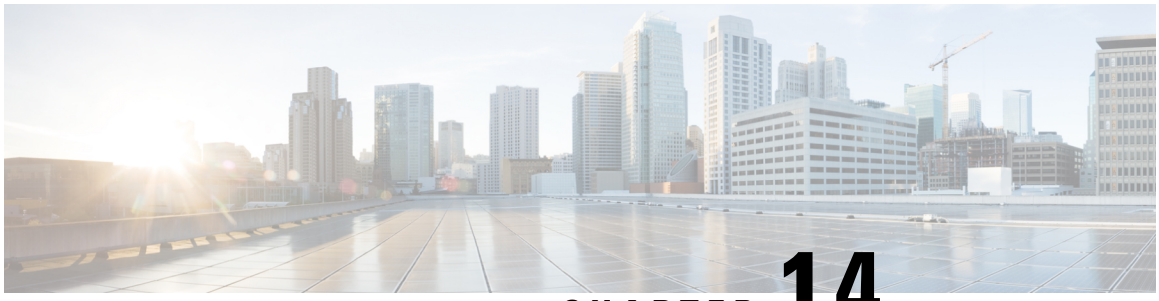
Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile test-ap-profile`	Configures an AP profile and enters AP profile configuration mode. **Note** You can use the default AP profile (default-ap-profile) or create a named AP profile, as shown in the example.

Step 3	**link-encryption**
	Example:
	`Device(config-ap-profile)# link-encryption`
		Enables link encryption based on the profile. Answer yes, when the system prompts you with this message:
		Note If you set stats-timer as as zero (0) under the AP profile, then the AP will not send the link encryption statistics.
		`Enabling link-encryption will reboot the APs with link-encryption.`
		`Are you sure you want to continue? (y/n)[y]:`

Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**show wireless dtls connections** **Example:** `Device# show wireless dtls connections`	(Optional) Displays the DTLS session established for the AP that has joined this controller.
Step 6	**show ap link-encryption** **Example:** `Device# show ap link-encryption`	(Optional) Displays the link encryption-related statistics (whether link encryption is enabled or disabled) counter received from the AP.



CHAPTER 14

Converting Autonomous Access Points to Lightweight Mode

- Guidelines for Converting Autonomous Access Points to Lightweight Mode, on page 127
- Information About Autonomous Access Points Converted to Lightweight Mode, on page 128
- How to Convert a Lightweight Access Point Back to an Autonomous Access Point, on page 130
- Authorizing Access Points, on page 131
- Disabling the Reset Button on Converted Access Points (CLI), on page 134
- Monitoring the AP Crash Log Information, on page 134
- How to Configure a Static IP Address on an Access Point, on page 135
- Configuring a Static IP Address on an Access Point (GUI), on page 136
- Recovering the Access Point Using the TFTP Recovery Procedure, on page 137
- Configuration Examples for Converting Autonomous Access Points to Lightweight Mode, on page 137
- AP MAC Authorization, on page 138
- Ethernet VLAN Tagging on Access Points, on page 139

Guidelines for Converting Autonomous Access Points to Lightweight Mode

- Access points that are converted to lightweight mode do not support Wireless Domain Services (WDS). Converted access points communicate only with Cisco wireless LAN devices and cannot communicate with WDS devices. However, the device provides functionality that is equivalent to WDS when an access point is associated to it.
- All Cisco lightweight access points support 16 Basic Service Set Identifiers (BSSIDs) per radio and a total of 16 wireless LANs per access point. When a converted access point is associated to a device, only wireless LANs with IDs 1 through 16 are pushed to the access point, unless the access point is a member of an access point group.
- Access points that are converted to lightweight mode must get an IP address and discover the device using DHCP, DNS, or IP subnet broadcast.

Information About Autonomous Access Points Converted to Lightweight Mode

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

Note Autonomous mode is supported only on the following APs:

- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 3700 Series Access Points

Reverting from Lightweight Mode to Autonomous Mode

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

Using DHCP Option 43 and DHCP Option 60

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

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

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

Note Ensure that the device IP address that you obtain from the DHCP server is a unicast IP address. Do not configure the device IP address as a multicast address when configuring DHCP option 43.

Restrictions for DHCP Option 60

- Cisco Wave2 APs support strings with length up to 256 characters only.

Note When the string length exceeds the limit, the default value is sent during the DHCP discover process.

How Converted Access Points Send Crash Information to the Device

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

Uploading Memory Core Dumps from Converted Access Points

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

Displaying MAC Addresses for Converted 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 page, the device lists converted access points by the radio MAC address.

Configuring a Static IP Address for a Lightweight Access Point

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

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

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

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

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

Procedure

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

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

Procedure

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

Step 2 Make sure that the PC contains the access point image file in the TFTP server folder and that the TFTP server is activated.

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

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

Step 5 Disconnect power from the access point.

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

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

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

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

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

Authorizing Access Points

The following sections describe the various ways in which access points can be authorized:

Authorizing Access Points Using Local Database (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ap auth-list ap-policy authorize-ap** **Example:** `Device(config)# ap auth-list ap-policy authorize-ap`	Configures an access point authorization policy.
Step 4	**username** *user_name* **mac** [**aaa attribute list** *list_name*] **Example:** `Device(config)# username abcdabcdabcd mac aaa attribute list attrlist`	(Optional) Configures the MAC address of an access point locally. **Note** Configure the MAC address for local authentication and AP local authorization using the following command: `username abcdabcdabcd mac`
Step 5	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables new access control commands and functions.
Step 6	**aaa authorization credential-download** {*auth_list* | **default**} **local** **Example:**	Downloads EAP credentials from the local server.

	Command or Action	Purpose
	`Device(config)# aaa authorization credential-download auth_download local`	
Step 7	**aaa attribute list** *list* **Example:** `Device(config)# aaa attribute list alist`	(Optional) Configures AAA attribute list definitions.
Step 8	**aaa session-id common** **Example:** `Device(config)# aaa session-id common`	Configures the AAA common session ID.
Step 9	**aaa local authentication default authorization default** **Example:** `Device(config)# aaa local authentication default authorization default`	(Optional) Configures the local authentication method list.
Step 10	**end**	Saves the configuration and exits the configuration mode and returns to privileged EXEC mode.
Step 11	**show ap name** *Cisco_AP* **config general** **Example:** `Device# show ap name AP01 config general`	Displays the configuration information that corresponds to a specific access point.

Authorizing Access Points Using RADIUS Server (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server ise`	Enters the RADIUS server configuration mode.

	Command or Action	Purpose
Step 4	**address** {**ipv4** | **ipv6**} *radius-server-ipv4-address-or-name* **auth-port** *udp-port-auth-server* **acct-port** *udp-port-acct-server* **Example:** `Device(config-radius-server)# address ipv4 224.0.0.1 auth-port 1645 acct-port 1646`	Configures the RADIUS server along with other server parameters.
Step 5	**key** *0 cisco* **Example:** `Device(config-radius-server)# key 0 cisco`	Sets a clear text encryption key for the RADIUS authentication server.
Step 6	**exit** **Example:** `Device(config-radius-server)# exit`	Reverts to the Privileged EXEC mode.
Step 7	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius ise-group`	Configures RADIUS server group definition.
Step 8	**server name** *ise* **Example:** `Device(config-sg-radius)# server name ise`	Configures the RADIUS server name.
Step 9	**ip radius source-interface** *vlan* **Example:** `Device(config-sg-radius)# ip radius source-interface vlan`	(Optional) Configures interface for source address in RADIUS packets.
Step 10	**exit** **Example:** `Device(cconfig-sg-radius)# exit`	Reverts to the Privileged EXEC mode.
Step 11	**aaa authorization network default group** *default-server-group* **local** **Example:** `Device(config)# aaa authorization network default group ise-group local`	Sets the authorization method to local.
Step 12	**aaa authorization credential-download default group** *default-server-group* **local** **Example:**	Configures local database to download EAP credentials from local, RADIUS, or LDAP server.

	Command or Action	Purpose
	`Device(config)# aaa authorization credential-download default group ise-group local`	

Disabling the Reset Button on Converted Access Points (CLI)

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

Procedure

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

Monitoring the AP Crash Log Information

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

Procedure

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

How to Configure a Static IP Address on an Access Point

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *Cisco_AP* **static-ip ip-address** *static_ap_address* **netmask** *static_ip_netmask* **gateway** *static_ip_gateway* **Example:** `Device# ap name AP03 static-ip ip-address 9.9.9.16 netmask 255.255.0.0 gateway 9.9.9.2`	Configures a static IP address on the access point. This command contains the following keywords and arguments: • **ip-address**— Specifies the Cisco access point static IP address. • *ip-address*— Cisco access point static IP address. • **netmask**—Specifies the Cisco access point static IP netmask. • *netmask*— Cisco access point static IP netmask. • **gateway**—Specifies the Cisco access point gateway. • *gateway*— IP address of the Cisco access point gateway. The access point reboots and rejoins the device, and the static IP address that you specify is pushed to the access point. After the static IP address has been sent to the access point, you

	Command or Action	Purpose
		can configure the DNS server IP address and domain name. You must perform Steps 3 and Step 4 after the access points reboot.
Step 3	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 4	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 5	**ap static-ip name-server** *nameserver_ip_address* **Example:** `Device(config)# ap static-ip name-server 10.10.10.205`	Configures a DNS server so that a specific access point or all access points can discover the device using DNS resolution. **Note** To undo the DNS server configuration, enter the **no ap static-ip name-server** *nameserver_ip_address* command.
Step 6	**ap static-ip domain** *static_ip_domain* **Example:** `Device(config)# ap static-ip domain domain1`	Configures the domain to which a specific access point or all access points belong. **Note** To undo the domain name configuration, enter the **no ap static-ip domain** *static_ip_domain* command.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 8	**show ap name** *Cisco_AP* **config general** **Example:** `Device# show ap name AP03 config general`	Displays the IP address configuration for the access point.

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

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 On the **All Access Points** section, click on an **AP Name**.

Step 3 In the **Edit AP** window that is displayed, go to the **IP Config** section.

Step 4 Select the **Static IP (IPv4/IPv6)** check box. This activates the static IP details pane.

Step 5 Enter the **Static IP**, **Netmask**, **Gateway**, and **DNS IP Address**.

Step 6 Click **Update & Apply to Device**.

Recovering the Access Point Using the TFTP Recovery Procedure

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 device to download the oversized access point image and complete the upgrade procedure.

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

Configuration Examples for Converting Autonomous Access Points to Lightweight Mode

Example: Displaying the IP Address Configuration for Access Points

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

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

Example: Displaying Access Point Crash File Information

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

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

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

AP MAC Authorization

The AP Authentication Policy feature ensures that only authorized APs can associate with a controller. To authorize an AP, the Ethernet MAC address of the AP must be registered. This can be done locally on the controller or on an external RADIUS server.

Configuring AP MAC Authorization (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**[no] ap auth-list ap-policy authorize-ap** *profile-name* **Example:** `Device(config)# ap auth-list ap-policy authorize-ap`	Configures AP authorization policy.
Step 3	**end** **Example:** `Device(config)# end`	Exits the configuration mode and returns to privileged EXEC mode.
Step 4	**show ap auth-list** *value-in-dBm* **Example:** `Device# show ap auth-list`	Shows the status of AP MAC authorization.

Example

1. Local database configuration:

   ```
   Device(config)# aaa authorization network default local
   Device(config)# aaa authorization credential-download default local
   ```

2. Username configuration:

   ```
   Device(config)# username abcdabcdabcd mac
   ```

   Username is the Ethernet MAC address of the AP, which is to be authorized before the AP associates with the controller. The Ethernet MAC address of the AP must be in the following format:

```
username <abcdabcdabcd> mac
```

Use the **show ap summary** command to get the Ethernet MAC address of the AP.

Ethernet VLAN Tagging on Access Points

Information About Ethernet VLAN Tagging on 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.

Configuring Ethernet VLAN Tagging on Access Points (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points** and expand the **All Access Points** section.

Step 2 To enable VLAN tagging for all access points associated with the controller, select **Set VLAN Tag** from the **Select an Action**drop-down list.

Step 3 In the **Configure VLAN Tag** window enter the VLAN Tag ID to enable VLAN tagging of both CAPWAP control and data packets on the Access Point and click **Apply to Device** for the configuration to take effect. If you do not want all devices to be tagged, select the **Remove Current VLAN Tag** and click **Apply to Device.**

Step 4 Alternatively, if you want to configure VLAN tagging on individual Access Points, click the name of the AP go to **Edit** > **Advanced** and select the **VLAN Tag** to enable the VLAN tagging on the AP.

Step 5 Click **Update & Apply to Device**.

Configuring Ethernet VLAN Tagging on Access Points (CLI)

Follow the procedure given below to configure Ethernet VLAN tagging on APs.

Before you begin

- VLAN tagging is not supported on MAPs that are in bridge mode. The feature is automatically disabled when the APs are set to bridge mode.
- If VLAN tagging is enabled, flex native VLAN ID cannot be configured for an AP.
- APs in flexconnect standalone mode (with VLAN tag enabled) may reload at every 10 minutes, if the APs fail to discover the wireless controller during failover.

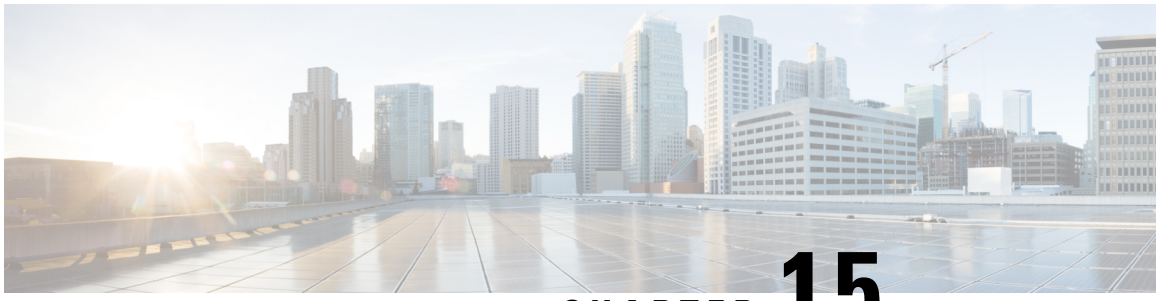
Procedure

	Command or Action	Purpose

Step 1	**ap name** *ap-name* **vlan-tag** *vlan-id*
	Example:
	`Device# ap name AP1 vlan-tag 12`
	`Device# ap name AP1 no vlan-tag`
		Configures VLAN tagging for a non-bridge AP. Use the **no** form of this command to disable the configuration.

Step 2	**ap vlan-tag** *vlan-id*
	Example:
	`Device# ap vlan-tag 1000`
	`Device# ap no vlan-tag`
		Configure VLAN tagging for all nonbridge APs. Use the **no** form of this command to disable the configuration.

Step 3	**show ap config general** **Example:** `Device# show ap config general`	(Optional) Shows the common information of all the APs.



CHAPTER 15

AP Crash File Upload

- AP Crash File Upload, on page 141
- Configuring AP Crash File Upload (CLI), on page 142

AP Crash File Upload

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

Note The system does not generate reports in case of a reload.

During a process crash, the following are collected locally from the device:

- Full process core
- Trace logs
- Cisco IOS syslogs (not guaranteed in case of nonactive crashes)
- System process information
- Bootup logs
- Reload logs
- Certain types of proc information

All this information is stored in separate files, which are then archived and compressed into one bundle. This makes it convenient to get a crash snapshot in one place, and can be then moved off the box for analysis. This report is generated before the device goes down to ROMMON/bootloader.

Note Except for the full core and tracelogs, everything else is a text file.

Configuring AP Crash File Upload (CLI)

Procedure

Step 1 **enable**

Enters privileged EXEC mode.

Step 2 **ap name** *ap-name* **crash-file get-crash-data**

Collects AP crash information. The crash file is uploaded automatically after the AP reloads to ready state. Therefore, this command does not have to be manually executed.

Step 3 **ap name** *ap-name* **crash-file get-radio-core-dump slot** {**0** | **1**}

Collects the AP core dump file for slot 0 or slot 1.

Step 4 **ap name** *ap-name* **core-dump** *tftp-ip crash-file* **uncompress**

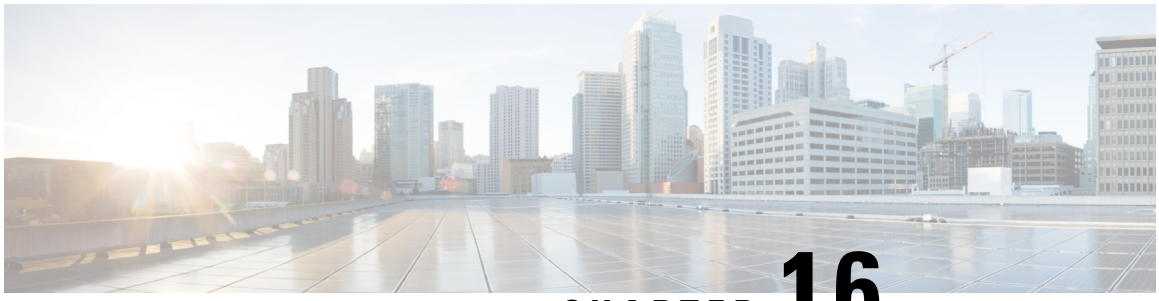
Uploads the AP crash coredump file to the given TFTP location.

Step 5 **show ap crash-file**

Displays the AP crash file, as well as the radio crash file.

Step 6 **dir bootflash**

Displays the crash file in bootflash with .crash extension.



CHAPTER 16

Rogue per AP

- Rogue per AP, on page 143
- Enabling Rogue Detection, on page 144

Rogue per AP

Rogue detection is configured per AP or for a group of APs. The rogue AP detection is configured under the AP profile. The rogue AP detection configuration enabled by default and is part of the default AP profile.

The following commands are deprecated from this release:

- **wireless wps rogue detection enable**
- **wireless wps rogue detection report-interval** *interval*
- **wireless wps rogue detection min-rssi** *rssi*
- **wireless wps rogue detection min-transient-time** *transtime*
- **wireless wps rogue detection containment flex-connect**
- **wireless wps rogue detection containment auto-rate**

Enabling Rogue Detection

The following are the high-level steps to enable rogue detection:

- Configure an AP Profile
- Define a Wireless Site Tag and Assign the AP Profile
- Associate the Wireless Site Tag to an AP

Note The controller may not report the original min-rssi value due to conversions made by the AP and the controller. Hence, the reported min-rssi may be different from the original value.

Enabling Rogue Detection

Configuring an AP Profile (GUI)

Before you begin

The default AP join profile values will have the global AP parameters and the AP group parameters. The AP join profile contains attributes that are specific to AP, such as CAPWAP, IPv4/IPv6, UDP Lite, High Availability, retransmit configuration parameters, global AP failover, Hyperlocation configuration parameters, Telnet/SSH, 11u parameters, and so on.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join Profile** page, click **Add**.

The **Add AP Join Profile** page is displayed.

Step 3 In the **General** tab, enter a name and description for the AP join profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Check the **LED State** check box to set the LED state of all APs connected to the device to blink so that the APs are easily located.

Step 5 In the **Client** tab and **Statistics Timer** section, enter the time in seconds that the AP sends its 802.11 statistics to the controller.

Step 6 In the **TCP MSS Configuration** section, check the **Adjust MSS Enable** check box to enter value for Adjust MSS. You can enter or update the maximum segment size (MSS) for transient packets that traverse a router. TCP MSS adjustment enables the configuration of the maximum segment size (MSS) for transient packets that traverse a router, specifically TCP segments with the SYN bit set.

In a CAPWAP environment, a lightweight access point discovers a device by using CAPWAP discovery mechanisms, and then sends a CAPWAP join request to the device. The device sends a CAPWAP join response to the access point that allows the access point to join the device.

When the access point joins the device, the device manages its configuration, firmware, control transactions, and data transactions.

Step 7 In the **CAPWAP** tab, you can configure the following:

- High Availability

  You can configure primary and secondary backup controllers for all access points (which are used if primary, secondary, or tertiary controllers are not responsive) in this order: primary, secondary, tertiary, primary backup, and secondary backup. In addition, you can configure 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.

a) In the **High Availability** tab, enter the time (in seconds) in the **Fast Heartbeat Timeout** field to configure the heartbeat timer for all access points. Specifying a small heartbeat interval reduces the amount of time it takes to detect device failure.
b) In the **Heartbeat Timeout** field, enter the time (in seconds) to configure the heartbeat timer for all access points. Specifying a small heartbeat interval reduces the amount of time it takes to detect device failure.
c) In the **Discovery Timeout** field, enter a value between 1 and 10 seconds (inclusive) to configure the AP discovery request timer.
d) In the **Primary Discovery Timeout** field, enter a value between 30 and 3000 seconds (inclusive) to configure the access point primary discovery request timer.
e) In the **Primed Join Timeout** field, enter a value between 120 and 43200 seconds (inclusive) to configure the access point primed join timeout.
f) In the **Retransmit Timers Count** field, enter the number of times that you want the AP to retransmit the request to the device and vice-versa. Valid range is between 3 and 8.
g) In the **Retransmit Timers Interval** field, enter the time duration between retransmission of requests. Valid range is between 2 and 5.
h) Check the **Enable Fallback** check box to enable fallback.
i) Enter the **Primary Controller** name and IP address.
j) Enter the **Secondary Controller** name and IP address.
k) Click **Save & Apply to Device**.

Note The primary and secondary settings in the AP join profile are not used for AP fallback. This means that the AP will not actively probe for those controllers (which are a part of the AP join profile), when it has joined one of them.

This setting is used only when the AP loses its connection with the controller, and then prioritizes which other controller it should join. These controllers have a priority of 4 and 5, following APs in the **High Availability** tab of the AP page.

The APs that are added as the primary, secondary, and tertiary APs in the **High Availability** tab of the AP configuration page, are actively probed and are used for the AP fallback option.

- Advanced

a) In the **Advanced** tab, check the **Enable VLAN Tagging** check box to enable VLAN tagging.
b) Check the **Enable Data Encryption** check box to enable Datagram Transport Layer Security (DTLS) data encryption.
c) Check the **Enable Jumbo MTU** to enable big maximum transmission unit (MTU). MTU is the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are divided into smaller packets before transmission. Jumbo frames are frames that are bigger than the standard Ethernet frame size, which is 1518 bytes (including Layer 2 (L2) header and FCS). The definition of frame size is vendor-dependent, as these are not part of the IEEE standard.
d) Use the **Link Latency** drop-down list to select the link latency. Link latency monitors the round-trip time of the CAPWAP heartbeat packets (echo request and response) from the AP to the controller and back.
e) From the **Preferred Mode** drop-down list, choose the mode.
f) Click **Save & Apply to Device**.

Step 8 In the **AP** tab, you can configure the following:

- General

a) In the **General** tab, check the **Switch Flag** check box to enable switches.

b) Check the **Power Injector State** check box if power injector is being used. Power Injector increases wireless LAN deployment flexibility of APs by providing an alternative powering option to local power, inline power-capable multiport switches, and multiport power patch panels.

Power Injector Selection parameter enables you to protect your switch port from an accidental overload if the power injector is inadvertently bypassed.

c) From the **Power Injector Type** drop-down list, choose power injector type from the following options:

- 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.

d) In the **Injector Switch MAC** field, enter the MAC address of the switch.
e) From the **EAP Type** drop-down list, choose the EAP type as *EAP-FAST*, *EAP-TLS*, or *EAP-PEAP*.
f) From the **AP Authorization Type** drop-down list, choose the type as either *CAPWAP DTLS* + or *CAPWAP DTLS*.
g) In the **Client Statistics Reporting Interval** section, enter the interval for 5 GHz and 2.4 GHz radios in seconds.
h) Check the **Enable** check box to enable extended module.
i) From the **Profile Name** drop-down list, choose a profile name for mesh.
j) Click **Save & Apply to Device**.

- Hyperlocation: Cisco Hyperlocation is a location solution that allows to track the location of wireless clients with the accuracy of one meter. Selecting this option disables all other fields in the screen, except NTP Server.

a) In the **Hyperlocation** tab, check the **Enable Hyperlocation** check box.
b) Enter the **Detection Threshold** value to filter out packets with low RSSI. The valid range is –100 dBm to –50 dBm.
c) Enter the **Trigger Threshold** value to set the number of scan cycles before sending a BAR to clients. The valid range is 0 to 99.
d) Enter the **Reset Threshold** value to reset value in scan cycles after trigger. The valid range is 0 to 99.
e) Enter the **NTP Server** IP address.
f) Click **Save & Apply to Device**.

- BLE: If your APs are Bluetooth Low Energy (BLE) enabled, they can transmit beacon messages that are packets of data or attributes transmitted over a low energy link. These BLE beacons are frequently used for health monitoring, proximity detection, asset tracking, and in-store navigation. For each AP, you can customize BLE Beacon settings configured globally for all APs.

a) In the **BLE** tab, enter a value in the **Beacon Interval** field to indicate how often you want your APs to send out beacon advertisements to nearby devices. The range is from 1 to 10, with a default of 1.
b) In the **Advertised Attenuation Level** field, enter the attenuation level. The range is from 40 to 100, with a default of 59.
c) Click **Save & Apply to Device**.

- Packet Capture: Packet Capture feature allows to capture the packets on the AP for the wireless client troubleshooting. The packet capture operation is performed on the AP by the radio drivers on the current channel on which it is operational, based on the specified packet capture filter.

a) In the **Packet Capture** tab, choose an **AP Packet Capture Profile** from the drop-down list.
b) You can also create a new profile by clicking the + sign.
c) Enter a name and description for the AP packet capture profile.
d) Enter the **Buffer Size**.
e) Enter the **Duration**.
f) Enter the **Truncate Length** information.
g) In the **Server IP** field, enter the IP address of the TFTP server.
h) In the **File Path** field, enter the directory path.
i) Enter the username and password details.
j) From the **Password Type** drop-down list, choose the type.
k) In the **Packet Classifiers** section, use the option to select or enter the packets to be captured.
l) Click **Save**.
m) Click **Save & Apply to Device**.

Step 9 In the **Management** tab, you can configure the following:

- Device

a) In the **Device** tab, enter the **IPv4/IPv6 Address** of the TFTP server, **TFTP Downgrade** section.
b) In the **Image File Name** field, enter the name of the software image file.
c) From the **Facility Value** drop-down list, choose the appropriate facility.
d) Enter the IPv4 or IPv6 address of the host.
e) Choose the appropriate **Log Trap Value**.
f) Enable Telnet and/or SSH configuration, if required.
g) Enable core dump, if required.
h) Click **Save & Apply to Device**.

- User

a) In the **User** tab, enter username and password details.
b) Choose the appropriate password type.
c) In the **Secret** field, enter a custom secret code.
d) Choose the appropriate secret type.
e) Choose the appropriate encryption type.
f) Click **Save & Apply to Device**.

- Credentials

a) In the **Credentials** tab, enter local username and password details.
b) Choose the appropriate local password type.
c) Enter 802.1x username and password details.
d) Choose the appropriate 802.1x password type.
e) Enter the time in seconds after which the session should expire.
f) Enable local credentials and/or 802.1x credentials as required.
g) Click **Save & Apply to Device**.

- CDP Interface

a) In the **CDP Interface** tab, enable the CDP state, if required.
b) Click **Save & Apply to Device**.

Step 10 In the **Rogue AP** tab, check the **Rogue Detection** check box to enable rogue detection.

Step 11 In the **Rogue Detection Minimum RSSI** field, enter the RSSI value.

This field specifies the minimum RSSI value for which a Rogue AP should be reported. All Rogue APs with RSSI lower than what is configured will not be reported to controller.

Step 12 In the **Rogue Detection Transient Interval** field, enter the transient interval value.

This field indicates how long the Rogue AP should be seen before reporting the controller.

Step 13 In the **Rogue Detection Report Interval** field, enter the report interval value.

This field indicates the frequency (in seconds) of Rogue reports sent from AP to controller.

Step 14 Check the **Rogue Containment Automatic Rate Selection** check box to enable rogue containment automatic rate selection.

Here, the AP selects the best rate for the target Rogue, based on its RSSI.

Step 15 Check the **Auto Containment on FlexConnect Standalone** check box to enable the feature.

Here, the AP will continue containment in case it moves to flexconnect standalone mode.

Step 16 Click **Save & Apply to Device**.

Configure an AP Profile

Follow the procedure given below to configure an AP profile:

Procedure

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

	Command or Action	Purpose
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters the ap profile configuration mode.
Step 3	**description** *ap-profile-name* **Example:** `Device(config-ap-profile)# description "xyz ap profile"`	Adds a description for the ap profile.
Step 4	**rogue detection enable** **Example:** `Device(config-ap-profile)# rogue detection enable`	Enables rogue detection for individual access points. Rogue detection is enabled by default. Use this command if rogue detection is disabled.
Step 5	**rogue detection report-interval** *interval* **Example:** `Device(config-ap-profile)# rogue detection report-interval 12`	Specifies the time interval, in seconds, at which APs should send the rogue detection report to the controller . The default value for *interval* is 10.
Step 6	**rogue detection min-rssi** *rssi* **Example:** `Device(config-ap-profile)# rogue detection min-rssi -128`	Specifies the minimum RSSI value that rogues should have for APs to detect them. The minimum RSSI value is –128.
Step 7	**rogue detection min-transient-time** *transtime* **Example:** `Device(config-ap-profile)# rogue detection min-transient-time 120`	Specifies the time interval at which rogues have to be consistently scanned for by APs after the first time the rogues are scanned. The lowest value for minimum transient time is 0.
Step 8	**rogue detection containment flex-connect** **Example:** `Device(config-ap-profile)# rogue detection containment flex-connect`	Sets the auto containment options for standalone FlexConnect access points. By default, this option is disabled.
Step 9	**rogue detection containment auto-rate** **Example:** `Device(config-ap-profile)# rogue detection containment auto-rate`	Sets the auto rate for containment of rogues. By default, auto-rate is disabled.

Define a Wireless Site Tag and Assign an AP Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 On the **Tags** page, click the **Site** tab and click **Add**.

Step 3 In the **Add Site Tag** window, enter the name in the **name** field.

Step 4 Choose the AP profile from the **AP Join Profile** drop-down list.

Step 5 Click **Save & Apply to Device**.

Define a Wireless Site Tag and Assign an AP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless tag site***site-tag* **Example:** `Device(config)# wireless tag site default-site-tag`	Enters the wireless site tag configuration mode.
Step 3	**ap-profile** *ap-profile* **Example:** `Device(config-site-tag)# ap-profile xyz-ap-profile`	Assigns an AP profile to the wireless site.
Step 4	**exit** **Example:** `Device(config-site-tag)# exit`	Returns to the global configuration mode.

Associating Wireless Tag to an AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 Click **AP** tab to configure the following:

- Tag Source

- Static
- Filter

Step 3 In the **Static** tab, click **Add** to perform the following:

a) Enter a MAC address.
b) Choose the appropriate **Policy Tag Name**, **Site Tag Name**, and **RF Tag Name**.
c) Click **Save & Apply to Device**.

Step 4 In the **Filter** tab, click **Add** to perform the following:

a) Enter a rule and AP name.
b) Use the slider to enable **Active**.
c) Enter the priority. The valid range is from 0 to 127.
d) Choose the appropriate **Policy Tag Name**, **Site Tag Name**, and **RF Tag Name**.
e) Click **Save & Apply to Device**.

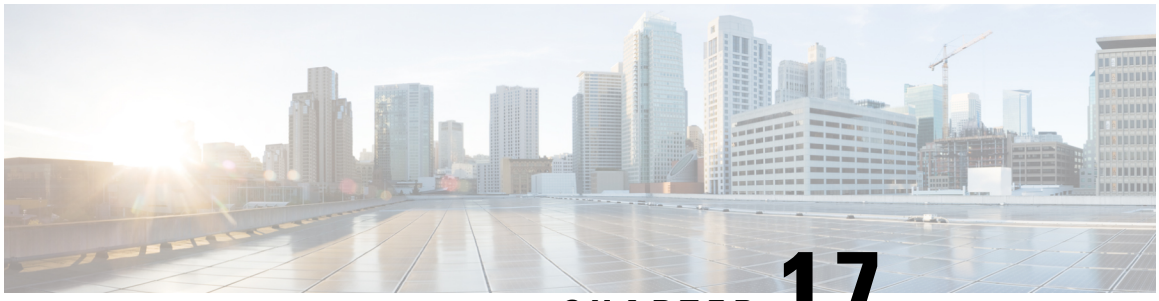
Associate Wireless Tag to an AP (CLI)

Follw the procedure given below to apply the rogue configuration defined under ap profile to the AP.

Note If the AP is not explicitly associated to a non-default site tag, it will be associated to default-site-tag and resultantly the default-ap-profile rogue configuration will be used.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures Cisco APs and enters the ap configuration mode.
Step 3	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag sitetag1`	Maps a wireless site tag to the AP.



CHAPTER 17

Access Point Plug-n-Play

- Overview of Access Point Plug-n-Play, on page 153
- Provisioning AP from PnP Server, on page 153
- Verifying AP Tag Configuration, on page 154

Overview of Access Point Plug-n-Play

The Plug and Play (PnP) server provides staging parameters to an access point (AP) before it joins a controller. Using this staging configuration, the AP receives the runtime configuration when it joins the controller.

The AP PnP feature enables the PnP server to provide all tag-related information, as part of the preconfigured information to the AP and in turn, to the controller.

You can upload configuration in PNP server in either *TXT* or *JSON* format and also add the AP details. The AP details are then mapped with the details in the *TXT* or *JSON* configuration file. While provisioning AP from PnP server, the AP acquires this configuration details. Based on the configuration details, the AP then joins the corresponding controller with the tag details.

Provisioning AP from PnP Server

You can provision AP from PnP Server in either ways:

- Configure DHCP server or switch with *Option 43*. For example, you can refer to the following code sample:

```
ip dhcp pool vlan10
 network 9.10.10.0 255.255.255.0
 default-router 9.10.10.1
  option 43 ascii 5A1D;B2;K4;|9.10.60.5;J80
```

- Configure DHCP server with DNS. For example, you can refer to the following code sample:

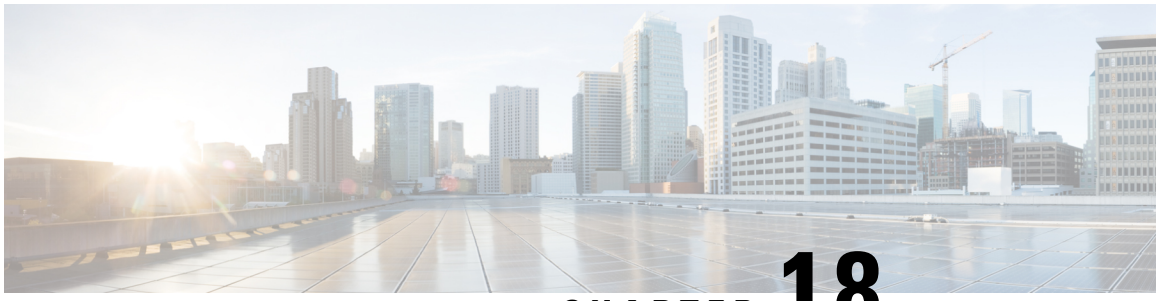
```
ip dhcp pool vlan10
 network 9.10.10.0 255.255.255.0
 default-router 9.10.10.1
 dns-server 9.8.65.5
 domain-name dns.com
```

Verifying AP Tag Configuration

The following example shows how to verify the AP tag configuration:

```
Device# show ap tag summary
Number of APs: 5


AP Name                 AP Mac           Site Tag Name           Policy Tag Name
RF Tag Name             Misconfigured    Tag Source

-------------------------------------------------------------------------------------

APd42c.4482.6102        d42c.4482.6102   default-site-tag        default-policy-tag
default-rf-tag          No               Default

AP00c1.64d8.6af0        00c1.64d8.6af0   named-site-tag          named-policy-tag
named-rf-tag            No               AP
```

Note The details in the second row reflect the tag source coming from a PNP server.



CHAPTER 18

802.11 Parameters for Cisco Access Points

- 2.4-GHz Radio Support, on page 155
- 5-GHz Radio Support, on page 157
- Information About Dual-Band Radio Support , on page 160
- Configuring Default XOR Radio Support, on page 161
- Configuring XOR Radio Support for the Specified Slot Number (GUI), on page 163
- Configuring XOR Radio Support for the Specified Slot Number, on page 163
- Receiver Only Dual-Band Radio Support, on page 165
- Configuring Client Steering (CLI), on page 167
- Verifying Cisco Access Points with Dual-Band Radios, on page 169

2.4-GHz Radio Support

Configuring 2.4-GHz Radio Support for the Specified Slot Number

Before you begin

Note The term *802.11b radio* or *2.4-GHz radio* will be used interchangeably.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 24ghz slot 0 SI** **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 SI`	Enables Spectrum Intelligence (SI) for the dedicated 2.4-GHz radio hosted on slot 0 for a specific access point. For more information, *Spectrum Intelligence* section in this guide.

	Command or Action	Purpose
		Here, **0** refers to the Slot ID.
Step 3	**ap name** *ap-name* **dot11 24ghz slot 0 antenna** {**ext-ant-gain** *antenna_gain_value* | **selection** [**internal** | **external**]} **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 antenna selection internal`	Configures 802.11b antenna hosted on slot 0 for a specific access point. • **ext-ant-gain**: Configures the 802.11b external antenna gain. *antenna_gain_value*- Refers to the external antenna gain value in multiples of .5 dBi units. The valid range is from 0 to 4294967295. • **selection**: Configures the 802.11b antenna selection (internal or external). **Note** • For APs supporting self-identifying antennas (SIA), the gain depends on the antenna, and not on the AP model. The gain is learned by the AP and there is no need for controller configuration. • For APs that do not support SIA, the APs send the antenna gain in the configuration payload, where the default antenna gain depends on the AP model. • Cisco Catalyst 9120E and 9130E APs support self-identifying antennas (SIA). Cisco Catalyst 9115E APs do not support SIA antennas. Although Cisco Catalyst 9115E APs work with SIA antennas, the APs do not auto-detect SIA antennas nor add the correct external gain.
Step 4	**ap name** *ap-name* **dot11 24ghz slot 0 beamforming** **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 beamforming`	Configures beamforming for the 2.4-GHz radio hosted on slot 0 for a specific access point.

	Command or Action	Purpose
Step 5	**ap name** *ap-name* **dot11 24ghz slot 0 channel** {*channel_number* | **auto**} **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 channel auto`	Configures advanced 802.11 channel assignment parameters for the 2.4-GHz radio hosted on slot 0 for a specific access point.
Step 6	**ap name** *ap-name* **dot11 24ghz slot 0 cleanair** **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 cleanair`	Enables CleanAir for 802.11b radio hosted on slot 0 for a specific access point.
Step 7	**ap name** *ap-name* **dot11 24ghz slot 0 dot11n antenna** {**A** | **B** | **C** | **D**} **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11n antenna A`	Configures 802.11n antenna for 2.4-GHz radio hosted on slot 0 for a specific access point. Here, **A**: Is the antenna port A. **B**: Is the antenna port B. **C**: Is the antenna port C. **D**: Is the antenna port D.
Step 8	**ap name** *ap-name* **dot11 24ghz slot 0 shutdown** **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 shutdown`	Disables 802.11b radio hosted on slot 0 for a specific access point.
Step 9	**ap name** *ap-name* **dot11 24ghz slot 0 txpower** {*tx_power_level* | **auto**} **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 txpower auto`	Configures transmit power level for 802.11b radio hosted on slot 0 for a specific access point. • *tx_power_level*: Is the transmit power level in dBm. The valid range is from 1 to 8. • **auto**: Enables auto-RF.

5-GHz Radio Support

Configuring 5-GHz Radio Support for the Specified Slot Number

Before you begin

Note The term *802.11a radio* or *5-GHz radio* will be used interchangeably in this document.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 5ghz slot 1 SI** **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 SI`	Enables Spectrum Intelligence (SI) for the dedicated 5-GHz radio hosted on slot 1 for a specific access point. Here, **1** refers to the Slot ID.
Step 3	**ap name** *ap-name* **dot11 5ghz slot 1 antenna ext-ant-gain** *antenna_gain_value* **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna ext-ant-gain`	Configures external antenna gain for 802.11a radios for a specific access point hosted on slot 1. *antenna_gain_value*—Refers to the external antenna gain value in multiples of .5 dBi units. The valid range is from 0 to 4294967295. **Note** • For APs supporting self-identifying antennas (SIA), the gain depends on the antenna, and not on the AP model. The gain is learned by the AP and there is no need for controller configuration. • For APs that do not support SIA, the APs send the antenna gain in the configuration payload, where the default antenna gain depends on the AP model. • Cisco Catalyst 9120E and 9130E APs support self-identifying antennas (SIA). Cisco Catalyst 9115E APs do not support SIA antennas. Although Cisco Catalyst 9115E APs work with SIA antennas, the APs do not auto-detect SIA antennas nor add the correct external gain.

	Command or Action	Purpose
Step 4	**ap name** *ap-name* **dot11 5ghz slot 1 antenna mode** [**omni** | **sectorA** | **sectorB**] **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna mode sectorA`	Configures the antenna mode for 802.11a radios for a specific access point hosted on slot 1.
Step 5	**ap name** *ap-name* **dot11 5ghz slot 1 antenna selection** [**internal** | **external**] **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna selection internal`	Configures the antenna selection for 802.11a radios for a specific access point hosted on slot 1.
Step 6	**ap name** *ap-name* **dot11 5ghz slot 1 beamforming** **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 beamforming`	Configures beamforming for the 5-GHz radio hosted on slot 1 for a specific access point.
Step 7	**ap name** *ap-name* **dot11 5ghz slot 1 channel** {*channel_number* | **auto** | **width** [**20** | **40** | **80** | **160**]} **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 channel auto`	Configures advanced 802.11 channel assignment parameters for the 5-GHz radio hosted on slot 1 for a specific access point. Here, *channel_number*- Refers to the channel number. The valid range is from 1 to 173.
Step 8	**ap name** *ap-name* **dot11 5ghz slot 1 cleanair** **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 cleanair`	Enables CleanAir for 802.11a radio hosted on slot 1 for a given or specific access point.
Step 9	**ap name** *ap-name* **dot11 5ghz slot 1 dot11n antenna** {**A** | **B** | **C** | **D**} **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 dot11n antenna A`	Configures 802.11n for 5-GHz radio hosted on slot 1 for a specific access point. Here, **A**- Is the antenna port A. **B**- Is the antenna port B. **C**- Is the antenna port C. **D**- Is the antenna port D.
Step 10	**ap name** *ap-name* **dot11 5ghz slot 1 rrm channel** *channel* **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 rrm channel 2`	Is another way of changing the channel hosted on slot 1 for a specific access point. Here, *channel*- Refers to the new channel created using 802.11h channel announcement. The valid range is from 1 to 173, provided 173 is

	Command or Action	Purpose
		a valid channel in the country where the access point is deployed.
Step 11	**ap name** *ap-name* **dot11 5ghz slot 1 shutdown** **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 shutdown`	Disables 802.11a radio hosted on slot 1 for a specific access point.
Step 12	**ap name** *ap-name* **dot11 5ghz slot 1 txpower** {*tx_power_level* | **auto**} **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 txpower auto`	Configures 802.11a radio hosted on slot 1 for a specific access point. • *tx_power_level*- Is the transmit power level in dBm. The valid range is from 1 to 8. • **auto**- Enables auto-RF.

Information About Dual-Band Radio Support

The Dual-Band (XOR) radio in Cisco 2800, 3800, 4800, and the 9120 series AP models offer the ability to serve 2.4–GHz or 5–GHz bands or passively monitor both the bands on the same AP. These APs can be configured to serve clients in 2.4–GHz and 5–GHz bands, or serially scan both 2.4–GHz and 5–GHz bands on the flexible radio while the main 5–GHz radio serves clients.

Cisco APs models up and through the Cisco 9120 APs are designed to support dual 5–GHz band operations with the *i* model supporting a dedicated Macro/Micro architecture and the *e* and *p* models supporting Macro/Macro. The Cisco 9130AXI APs and the Cisco 9136 APs support dual 5-GHz operations as Micro/Messo cell.

When a radio moves between bands (from 2.4-GHz to 5-GHz and vice versa), clients need to be steered to get an optimal distribution across radios. When an AP has two radios in the 5–GHz band, client steering algorithms contained in the Flexible Radio Assignment (FRA) algorithm are used to steer a client between the same band co-resident radios.

The XOR radio support can be steered manually or automatically:

- Manual steering of a band on a radio—The band on the XOR radio can only be changed manually.
- Automatic client and band steering on the radios is managed by the FRA feature that monitors and changes the band configurations as per site requirements.

Note RF measurement will not run when a static channel is configured on slot 1. Due to this, the dual band radio slot 0 will move only with 5–GHz radio and not to the monitor mode.

When slot 1 radio is disabled, RF measurement will not run, and the dual band radio slot 0 will be only on 2.4–GHz radio.

Configuring Default XOR Radio Support

Before you begin

Note The default radio points to the XOR radio hosted on slot 0.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 dual-band antenna ext-ant-gain** *antenna_gain_value* **Example:** `Device# ap name ap-name dot11 dual-band antenna ext-ant-gain 2`	Configures the 802.11 dual-band antenna on a specific Cisco access point. *antenna_gain_value*: The valid range is from 0 to 40.
Step 3	**ap name** *ap-name* **[no] dot11 dual-band shutdown** **Example:** `Device# ap name ap-name dot11 dual-band shutdown`	Shuts down the default dual-band radio on a specific Cisco access point. Use the **no** form of the command to enable the radio.
Step 4	**ap name** *ap-name* **dot11 dual-band role manual client-serving** **Example:** `Device# ap name ap-name dot11 dual-band role manual client-serving`	Switchs to client–serving mode on the Cisco access point.
Step 5	**ap name** *ap-name* **dot11 dual-band band 24ghz** **Example:** `Device# ap name ap-name dot11 dual-band band 24ghz`	Switchs to 2.4-GHz radio band.
Step 6	**ap name** *ap-name* **dot11 dual-band txpower** {*transmit_power_level* | **auto**} **Example:**	Configures the transmit power for the radio on a specific Cisco access point.

	Command or Action	Purpose
	`Device# ap name ap-name dot11 dual-band txpower 2`	**Note** When an FRA-capable radio (slot 0 on 9120 AP[for instance]) is set to Auto, you cannot configure static channel and Txpower on this radio. If you want to configure static channel and Txpower on this radio, you will need to change the radio role to Manual Client-Serving mode.
Step 7	**ap name** *ap-name* **dot11 dual-band channel** *channel-number* **Example:** `Device# ap name ap-name dot11 dual-band channel 2`	Enters the channel for the dual band. *channel-number*—The valid range is from 1 to 173.
Step 8	**ap name** *ap-name* **dot11 dual-band channel auto** **Example:** `Device# ap name ap-name dot11 dual-band channel auto`	Enables the auto channel assignment for the dual-band.
Step 9	**ap name** *ap-name* **dot11 dual-band channel width** {**20 MHz** | **40 MHz** | **80 MHz** | **160 MHz**} **Example:** `Device# ap name ap-name dot11 dual-band channel width 20 MHz`	Chooses the channel width for the dual band.
Step 10	**ap name** *ap-name* **dot11 dual-band cleanair** **Example:** `Device# ap name ap-name dot11 dual-band cleanair`	Enables the Cisco CleanAir feature on the dual-band radio.

Step 11	**ap name** *ap-name* **dot11 dual-band cleanair band** {**24 GHz | 5 GMHz**}
	Example:
	`Device# ap name ap-name dot11 dual-band cleanair band 5 GHz`
	`Device# ap name ap-name [no] dot11 dual-band cleanair band 5 GHz`
		Selects a band for the Cisco CleanAir feature.
		Use the **no** form of this command to disable the Cisco CleanAir feature.

Step 12	**ap name** *ap-name* **dot11 dual-band dot11n antenna** {**A | B | C | D**} **Example:**	Configures the 802.11n dual-band parameters for a specific access point.

	Command or Action	Purpose
	`Device# ap name ap-name dot11 dual-band dot11n antenna A`	
Step 13	**show ap name** *ap-name* **auto-rf dot11 dual-band** **Example:** `Device# show ap name ap-name auto-rf dot11 dual-band`	Displays the auto-RF information for the Cisco access point.
Step 14	**show ap name** *ap-name* **wlan dot11 dual-band** **Example:** `Device# show ap name ap-name wlan dot11 dual-band`	Displays the list of BSSIDs for the Cisco access point.

Configuring XOR Radio Support for the Specified Slot Number (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Dual-Band Radios** section, select the AP for which you want to configure dual-band radios.

The AP name, MAC address, CleanAir capability and slot information for the AP are displayed. If the Hyperlocation method is HALO, the antenna PID and antenna design information are also displayed.

Step 3 Click **Configure**.

Step 4 In the **General** tab, set the **Admin Status** as required.

Step 5 Set the **CleanAir Admin Status** field to Enable or Disable.

Step 6 Click **Update & Apply to Device**.

Configuring XOR Radio Support for the Specified Slot Number

Procedure

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

	Command or Action	Purpose
Step 2	**ap name** *ap-name* **dot11 dual-band slot 0 antenna ext-ant-gain** *external_antenna_gain_value* **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 antenna ext-ant-gain 2`	Configures dual-band antenna for the XOR radio hosted on slot 0 for a specific access point. *external_antenna_gain_value* - Is the external antenna gain value in multiples of .5 dBi unit. The valid range is from 0 to 40. **Note** • For APs supporting self-identifying antennas (SIA), the gain depends on the antenna, and not on the AP model. The gain is learned by the AP and there is no need for controller configuration. • For APs that do not support SIA, the APs send the antenna gain in the configuration payload, where the default antenna gain depends on the AP model.
Step 3	**ap name** *ap-name* **dot11 dual-band slot 0 band** {**24ghz** | **5ghz**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 band 24ghz`	Configures current band for the XOR radio hosted on slot 0 for a specific access point.
Step 4	**ap name** *ap-name* **dot11 dual-band slot 0 channel** {*channel_number* | **auto** | **width** [**160** | **20** | **40** | **80**]} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 channel 3`	Configures dual-band channel for the XOR radio hosted on slot 0 for a specific access point. *channel_number*- The valid range is from 1 to 165.
Step 5	**ap name** *ap-name* **dot11 dual-band slot 0 cleanair band** {**24Ghz** | **5Ghz**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 cleanair band 24Ghz`	Enables CleanAir features for dual-band radios hosted on slot 0 for a specific access point.
Step 6	**ap name** *ap-name* **dot11 dual-band slot 0 dot11n antenna** {**A** | **B** | **C** | **D**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 dot11n antenna A`	Configures 802.11n dual-band parameters hosted on slot 0 for a specific access point. Here, **A**- Enables antenna port A. **B**- Enables antenna port B.

	Command or Action	Purpose
		C- Enables antenna port C. **D**- Enables antenna port D.
Step 7	**ap name** *ap-name* **dot11 dual-band slot 0 role** {**auto** | **manual** [**client-serving** | **monitor**]} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 role auto`	Configures dual-band role for the XOR radio hosted on slot 0 for a specific access point. The following are the dual-band roles: • **auto**- Refers to the automatic radio role selection. • **manual**- Refers to the manual radio role selection.

Step 8	**ap name** *ap-name* **dot11 dual-band slot 0 shutdown**
	Example:
	`Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 shutdown`
	`Device# ap name AP-SIDD-A06 [no] dot11 dual-band slot 0 shutdown`
		Disables dual-band radio hosted on slot 0 for a specific access point.
		Use the **no** form of this command to enable the dual-band radio.

Step 9	**ap name** *ap-name* **dot11 dual-band slot 0 txpower** {*tx_power_level* | **auto**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 txpower 2`	Configures dual-band transmit power for XOR radio hosted on slot 0 for a specific access point. • *tx_power_level*- Is the transmit power level in dBm. The valid range is from 1 to 8. • **auto**- Enables auto-RF.

Receiver Only Dual-Band Radio Support

Information About Receiver Only Dual-Band Radio Support

This feature configures the dual-band Rx-only radio features for an access point with dual-band radios.

This dual-band Rx-only radio is dedicated for Analytics, Hyperlocation, Wireless Security Monitoring, and BLE AoA*.

This radio will always continue to serve in monitor mode, therefore, you will not be able to make any channel and *tx-rx* configurations on the 3rd radio.

Configuring Receiver Only Dual-Band Parameters for Access Points

Enabling CleanAir with Receiver Only Dual-Band Radio on a Cisco Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Dual-Band Radios** settings, click the AP for which you want to configure the dual-band radios.

Step 3 In the **General** tab, enable the **CleanAir** toggle button.

Step 4 Click **Update & Apply to Device**.

Enabling CleanAir with Receiver Only Dual-Band Radio on a Cisco Access Point

Procedure

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

Step 2	**ap name** *ap-name* **dot11 rx-dual-band slot 2 cleanair band** {**24Ghz** | **5Ghz**}
	Example:
	`Device# ap name AP-SIDD-A06 dot11 rx-dual-band slot 2 cleanair band 24Ghz`
	`Device# ap name AP-SIDD-A06 [no] dot11 rx-dual-band slot 2 cleanair band 24Ghz`
		Enables CleanAir with receiver only (Rx-only) dual-band radio on a specific access point.
		Here, 2 refers to the slot ID.
		Use the **no** form of this command to disable CleanAir.

Disabling Receiver Only Dual-Band Radio on a Cisco Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Dual-Band Radios** settings, click the AP for which you want to configure the dual-band radios.

Step 3 In the **General** tab, disable the **CleanAir Status** toggle button.

Step 4 Click **Update & Apply to Device**.

Disabling Receiver Only Dual-Band Radio on a Cisco Access Point

Procedure

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

Step 2	**ap name** *ap-name* **dot11 rx-dual-band slot 2 shutdown**
	Example:
	`Device# ap name AP-SIDD-A06 dot11 rx-dual-band slot 2 shutdown`
	`Device# ap name AP-SIDD-A06 [no] dot11 rx-dual-band slot 2 shutdown`
		Disables receiver only dual-band radio on a specific Cisco access point.
		Here, 2 refers to the slot ID.
		Use the **no** form of this command to enable receiver only dual-band radio.

Configuring Client Steering (CLI)

Before you begin

Enable Cisco CleanAir on the corresponding dual-band radio.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wireless macro-micro steering transition-threshold balancing-window** *number-of-clients(0-65535)* **Example:** `Device(config)# wireless macro-micro steering transition-threshold balancing-window 10`	Configures the micro-macro client load–balancing window for a set number of clients.
Step 4	**wireless macro-micro steering transition-threshold client count** *number-of-clients(0-65535)*	Configures the macro-micro client parameters for a minimum client count for transition.

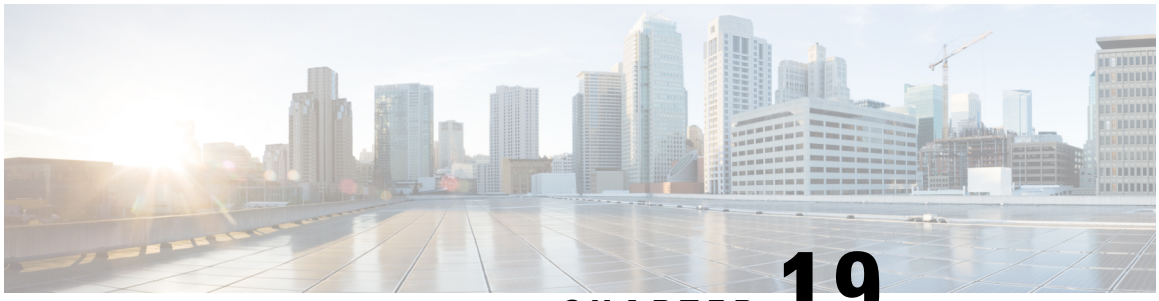
	Command or Action	Purpose
	Example: `Device(config)# wireless macro-micro steering transition-threshold client count 10`	
Step 5	**wireless macro-micro steering transition-threshold macro-to-micro** *RSSI-in-dBm(–128—0)* **Example:** `Device(config)# wireless macro-micro steering transition-threshold macro-to-micro -100`	Configures the macro–to–micro transition RSSI.
Step 6	**wireless macro-micro steering transition-threshold micro-to-macro** *RSSI-in-dBm(–128—0)* **Example:** `Device(config)# wireless macro-micro steering transition-threshold micro-to-macro -110`	Configures the micro–to–macro transition RSSI.
Step 7	**wireless macro-micro steering probe-suppression aggressiveness** *number-of-cycles(–128—0)* **Example:** `Device(config)# wireless macro-micro steering probe-suppression aggressiveness -110`	Configures the number of probe cycles to be suppressed.
Step 8	**wireless macro-micro steering probe-suppression hysteresis** *RSSI-in-dBm* **Example:** `Device(config)# wireless macro-micro steering probe-suppression hysteresis -5`	Configures the macro-to-micro probe in RSSI. The range is between –6 to –3.
Step 9	**wireless macro-micro steering probe-suppression probe-only** **Example:** `Device(config)# wireless macro-micro steering probe-suppression probe-only`	Enables probe suppression mode.
Step 10	**wireless macro-micro steering probe-suppression probe-auth** **Example:** `Device(config)# wireless macro-micro steering probe-suppression probe-auth`	Enables probe and single authentication suppression mode.

	Command or Action	Purpose
Step 11	**show wireless client steering** **Example:** `Device# show wireless client steering`	Displays the wireless client steering information.

Verifying Cisco Access Points with Dual-Band Radios

To verify the access points with dual-band radios, use the following command:

```
Device# show ap dot11 dual-band summary

AP Name Subband Radio      Mac   Status Channel Power Level Slot ID Mode
-------------------------------------------------------------------------------
4800   All 3890.a5e6.f360 Enabled (40)* *1/8     (22 dBm)      0   Sensor
4800   All 3890.a5e6.f360 Enabled N/A    N/A       2               Monitor
```



CHAPTER 19

802.1x Support

- Introduction to the 802.1X Authentication, on page 171
- Limitations of the 802.1X Authentication, on page 172
- Topology - Overview, on page 173
- Configuring 802.1X Authentication Type and LSC AP Authentication Type (GUI), on page 173
- Configuring 802.1X Authentication Type and LSC AP Authentication Type, on page 174
- Enabling 802.1X on the Switch Port, on page 176
- Verifying 802.1X on the Switch Port, on page 178
- Verifying the Authentication Type, on page 178

Introduction to the 802.1X Authentication

IEEE 802.1X port-based authentication is configure on a device to prevent unauthorized devices from gaining access to the network. The device can combine the function of a router, switch, and access point, depending on the fixed configuration. Any device connecting to a switch port where 802.1X authentication is enabled must go through relevant EAP authentication model to start exchanging traffic.

Currently, the Cisco Wave 2 and Wi-Fi 6 (802.11AX) APs support 802.1X authentication with switch port for EAP-FAST, EAP-TLS and EAP-PEAP methods. Now, you can enable configurations and provide credentials to the AP from the controller .

Note If the AP is dot1x EAP-FAST, when the AP reboots, it should perform an anonymous PAC provision. For performing PAC provision, the ADH cipher suites should be used to establish an authenticated tunnel. If the ADH cipher suites are not supported by radius servers, AP will fail to authenticate on reload.

EAP-FAST Protocol

In the EAP-FAST protocol developed by Cisco, in order to establish a secured TLS tunnel with RADIUS, the AP requires a strong shared key (PAC), either provided via in-band provisioning (in a secured channel) or via out-band provisioning (manual).

Note The EAP-FAST type configuration requires 802.1x credentials configuration for AP, since AP will use EAP-FAST with MSCHAP Version 2 method.

Note Local EAP is not supported on the Cisco 7925 phones.

Note In Cisco Wave 2 APs, for 802.1x authentication using EAP-FAST after PAC provisioning (caused by the initial connection or after AP reload), ensure that you configure the switch port to trigger re-authentication using one of the following commands: **authentication timer restart** *num* or **authentication timer reauthenticate** *num*.

EAP-TLS/EAP-PEAP Protocol

The EAP-TLS protocol or EAP-PEAP protocol provides certificate based mutual EAP authentication.

In EAP-TLS, both the server and the client side certificates are required, where the secured shared key is derived for the particular session to encrypt or decrypt data. Whereas, in EAP-PEAP, only the server side certificate is required, where the client authenticates using password based protocol in a secured channel.

Note The EAP-PEAP type configuration requires Dot1x credentials configuration for AP; and the AP also needs to go through LSC provisioning. AP uses the PEAP protocol with MSCHAP Version 2 method.

Limitations of the 802.1X Authentication

- 802.1X is not supported on dynamic ports or Ethernet Channel ports.
- 802.1X is not supported in a mesh AP scenario.
- There is no recovery from the controller on credential mismatch or the expiry/invalidity of the certificate on AP. The 802.1X authentication has to be disabled on the switch port to connect the AP back to fix the configurations.
- There are no certificate revocation checks implemented on the certificates installed in AP.
- Only one Locally Significant Certificates (LSC) can be provisioned on the AP and the same certificate must be used for CAPWAP DTLS session establishment with controller and the 802.1X authentication with the switch. If global LSC configuration on the controller is disabled; AP deletes LSC which is already provisioned.
- If clear configurations are applied on the AP, then the AP will lose the 802.1X EAP type configuration and the LSC certificates. AP should again go through staging process if 802.1X is required.

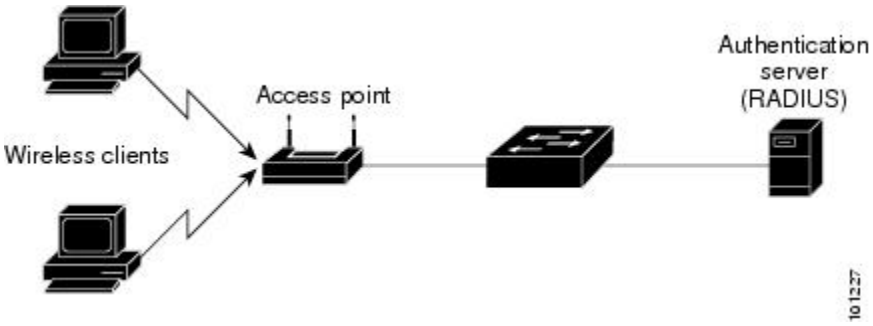
- 802.1X for trunk port APs on multi-host authentication mode is supported. Network Edge Authentication Topology (NEAT) is not supported on COS APs.

Topology - Overview

The 802.1X authentication events are as follows:

1. The AP acts as the 802.1X supplicant and is authenticated by the switch against the RADIUS server which supports EAP-FAST along with EAP-TLS and EAP-PEAP. When dot1x authentication is enabled on a switch port, the device connected to it authenticates itself to receive and forward data other than 802.1X traffic.
2. In order to authenticate with EAP-FAST method, the AP requires the credentials of the RADIUS server. It can be configured at the controller , from where it will be passed on to the AP via configuration update request. For, EAP-TLS or EAP-PEAP the APs use the certificates (device/ID and CA) made significant by the local CA server.

Figure 4: Figure: 1 Topology for 802.1X Authentication



Configuring 802.1X Authentication Type and LSC AP Authentication Type (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join Profile** page, click **Add**.

The **Add AP Join Profile** page is displayed.

Step 3 In the **AP** > **General** tab, navigate to the **AP EAP Auth Configuration** section.

Step 4 From the **EAP Type** drop-down list, choose the EAP type as *EAP-FAST*, *EAP-TLS*, or *EAP-PEAP* to configure the dot1x authentication type.

Step 5 From the **AP Authorization Type** drop-down list, choose the type as either CAPWAP DTLS + or CAPWAP DTLS.

Step 6 Click **Save & Apply to Device**.

Configuring 802.1X Authentication Type and LSC AP Authentication Type

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ap profile** *profile-name* **Example:** `Device(config)# ap profile new-profile`	Specify a profile name.
Step 4	**dot1x {max-sessions | username | eap-type | lsc-ap-auth-state}** **Example:** `Device(config-ap-profile)# dot1x eap-type`	Configures the dot1x authentication type. **max-sessions**: Configures the maximum 802.1X sessions initiated per AP. **username**: Configures the 802.1X username for all Aps. **eap-type:** Configures the dot1x authentication type with the switch port. **lsc-ap-auth-state**: Configures the LSC authentication state on the AP.
Step 5	**dot1x eap-type {EAP-FAST | EAP-TLS | EAP-PEAP}** **Example:** `Device(config-ap-profile)# dot1x eap-type`	Configures the dot1x authentication type: EAP-FAST, EAP-TLS, or EAP-PEAP.
Step 6	**dot1x lsc-ap-auth-state {CAPWAP-DTLS | Dot1x-port-auth | Both}** **Example:** `Device(config-ap-profile)#dot1x lsc-ap-auth-state Dot1x-port-auth`	Configures the LSC authentication state on the AP. **CAPWAP-DTLS**: Uses LSC only for CAPWAP DTLS. **Dot1x-port-auth**: Uses LSC only for dot1x authentication with port.

	Command or Action	Purpose
		Both: Uses LSC for both CAPWAP-DTLS and Dot1x authentication with port.
Step 7	**end** **Example:** `Device(config-ap-profile)# end`	Exits the AP profile configuration mode and enters privileged EXEC mode.

Configuring the 802.1X Username and Password (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.
Step 2 On the **AP Join** page, click the name of the AP Join profile or click **Add** to create a new one.
Step 3 Click the **Management** tab and then click the **Credentials** tab.
Step 4 Enter the local username and password details.
Step 5 Choose the appropriate local password type.
Step 6 Enter 802.1X username and password details.
Step 7 Choose the appropriate 802.1X password type.
Step 8 Enter the time in seconds after which the session should expire.
Step 9 Enable local credentials and/or 802.1X credentials as required.
Step 10 Click **Update & Apply to Device**.

Configuring the 802.1X Username and Password (CLI)

The following procedure configures the 802.1X password for all the APs:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ap profile** *profile-name* **Example:** `Device(config)# ap profile new-profile`	Specify a profile name.

	Command or Action	Purpose
Step 4	**dot1x {max-sessions | username | eap-type | lsc-ap-auth-state}** **Example:** `Device(config-ap-profile)# dot1x eap-type`	Configures the dot1x authentication type. **max-sessions**: Configures the maximum 802.1X sessions initiated per AP. **username**: Configures the 802.1X username for all Aps. **eap-type:** Configures the dot1x authentication type with the switch port. **lsc-ap-auth-state**: Configures the LSC authentication state on the AP.
Step 5	**dot1x username** <username> **password {0 | 8}** <password> **Example:** `Device(config-ap-profile)#dot1x username username password 0 password`	Configures the dot1x password for all the APs. 0: Specifies an unencrypted password will follow. 8: Specifies an AES encrypted password will follow.

Enabling 802.1X on the Switch Port

The following procedure enables 802.1X on the switch port:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**aaa authentication dot1x {default | listname} method1[method2...]** **Example:** `Device(config)# aaa authentication dot1x default group radius`	Creates a series of authentication methods that are used to determine user privilege to access the privileged command level so that the device can communicate with the AAA server.

	Command or Action	Purpose
Step 5	**aaa authourization network group** **Example:** `aaa authourization network group`	Enables AAA authorization for network services on 802.1X.
Step 6	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication.
Step 7	**interface type slot/port** **Example:** `Device(config)# interface fastethernet2/1`	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
Step 8	**authentication port-control {auto | force-authorized | force-unauthorized}** **Example:** `Device(config-if)# authentication port-control auto`	Enables 802.1X port-based authentication on the interface. **auto**—Enables IEEE 802.1X authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The Device requests the identity of the supplicant and begins relaying authentication messages between the supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the Device by using the supplicant MAC address. **force-authorized**-—Disables IEEE 802.1X authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1X-based authentication of the client. This is the default setting. **force-unauthorized**—Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. The Device cannot provide authentication services to the supplicant through the port.
Step 9	**dot1x pae [supplicant | authenticator | both]** **Example:** `Device(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters.

	Command or Action	Purpose
Step 10	**end** **Example:** `Device(config-if)# end`	Enters privileged EXEC mode.

Verifying 802.1X on the Switch Port

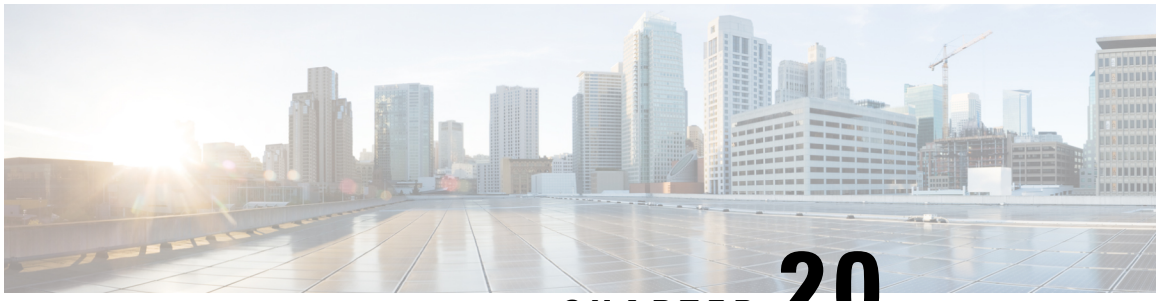
The following show command displays the authentication state of 802.1X on the switch port:

```
Device# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version      2
Dot1x Info for FastEthernet1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Device#
```

Verifying the Authentication Type

The following show command displays the authentication state of an AP profile:

```
Device#show ap profile <profile-name> detailed ?
  chassis  Chassis
  |        Output modifiers
  <cr>

Device#show ap profile <profile-name> detailed

  AP Profile Name        : default-ap-profile
  Description            : default ap profile
  …
  Dot1x EAP Method       : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
  LSC AP AUTH STATE      : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth
```



CHAPTER 20

CAPWAP Link Aggregation Support

- Information About CAPWAP LAG Support, on page 179
- Restrictions for CAPWAP LAG Support, on page 180
- Enabling CAPWAP LAG Support on Controller (GUI), on page 180
- Enabling CAPWAP LAG Support on Controller, on page 180
- Enabling CAPWAP LAG Globally on Controller, on page 181
- Disabling CAPWAP LAG Globally on Controller, on page 181
- Enabling CAPWAP LAG for an AP Profile (GUI), on page 181
- Enabling CAPWAP LAG for an AP Profile, on page 182
- Disabling CAPWAP LAG for an AP Profile, on page 182
- Disabling CAPWAP LAG Support on Controller , on page 183
- Verifying CAPWAP LAG Support Configurations, on page 183

Information About CAPWAP LAG Support

Link aggregation (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.

The CAPWAP LAG support feature is applicable for access points that support multiple ethernet ports for CAPWAP.

The 11AC APs with dual ethernet ports require the CAPWAP AP LAG support for data channel.

Cisco Aironet 1850, 2800, and 3800 Series APs' second Ethernet port is used as a link aggregation port, by default. It is possible to use this LAG port as an RLAN port when LAG is disabled.

The following APs use LAG port as an RLAN port:

- 1852E
- 1852I
- 2802E
- 2802I
- 3802E

- 3802I
- 3802P

Restrictions for CAPWAP LAG Support

- APs must be specifically enabled for CAPWAP AP LAG support.
- CAPWAP data does not support IPv6.
- Data DTLS must not be enabled when LAG is enabled.
- APs behind NAT and PAT are not supported.

Enabling CAPWAP LAG Support on Controller (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Wireless Global**.

Step 2 Check the **AP LAG Mode** check box.

Step 3 Click **Apply**.

Enabling CAPWAP LAG Support on Controller

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lag support** **Example:** `Device(config)# ap lag support`	Enables CAPWAP LAG support on the controller. **Note** After executing this command, you get to view the following warning statement: *Changing the lag support will cause all the APs to disconnect.* Thus, all APs with LAG capability reboots and joins the enabled CAPWAP LAG.

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

Enabling CAPWAP LAG Globally on Controller

If the CAPWAP LAG is enabled globally on the controller, the following occurs:

- AP joins the controller.
- AP exchanges its CAPWAP support.
- LAG mode starts, if LAG is enabled on AP.

Disabling CAPWAP LAG Globally on Controller

If the CAPWAP LAG is disabled globally on the controller, the following occurs:

- AP joins the controller.
- AP exchanges its CAPWAP support.
- AP LAG config is sent to AP, if LAG is already enabled on AP.
- AP reboots.
- AP joins back with the disabled LAG.

Enabling CAPWAP LAG for an AP Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 Click **Add**.

Step 3 Under the **General** tab, enter the **Name** of the AP Profile and check the **LAG Mode** check box to set the CAPWAP LAG for the AP profile.

Step 4 Click **Apply to Device**.

Enabling CAPWAP LAG for an AP Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode. **Note** When you delete a named profile, the APs associated with that profile will not revert to the default profile.
Step 3	**lag** **Example:** `Device(config-ap-profile)# lag`	Enables CAPWAP LAG for an AP profile.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Disabling CAPWAP LAG for an AP Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode. **Note** When you delete a named profile, the APs associated with that profile will not revert to the default profile.

	Command or Action	Purpose
Step 3	**no lag** **Example:** `Device(config-ap-profile)# no lag`	Disables CAPWAP LAG for an AP profile.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Disabling CAPWAP LAG Support on Controller

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**no ap lag support** **Example:** `Device(config)# no ap lag support`	Disables CAPWAP LAG support on the controller . **Note** All APs with LAG capability reboots and joins the disabled CAPWAP LAG.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode and returns to privileged EXEC mode.

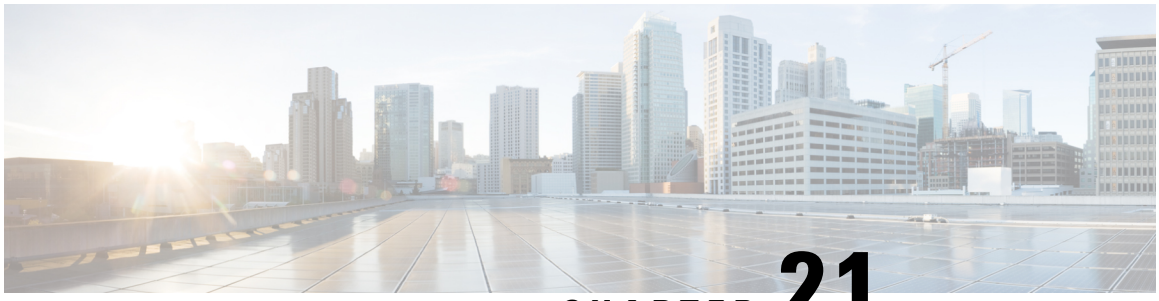
Verifying CAPWAP LAG Support Configurations

To verify the global LAG status for all Cisco APs, use the following command:

```
Device# show ap lag-mode
AP Lag-Mode Support Enabled
```

To verify the AP LAG configuration status, use the following command:

```
Device# show ap name <ap-name> config general
Cisco AP Identifier : 0008.3291.6360
Country Code : US
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-AB
AP Country Code : US - United States
::
AP Lag Configuration Status : Enabled/Disabled
Has AP negotiated lag based on AP capability and per AP config.
```



CHAPTER 21

DHCP and NAT Functionality on Root Access Point

- Information About DHCP and NAT Functionality on Root AP (RAP), on page 185
- Configuring DHCP Server on Root Access Point (RAP), on page 186
- Verifying DHCP Server for Root AP Configuration, on page 186

Information About DHCP and NAT Functionality on Root AP (RAP)

Note This feature is applicable for Cisco Aironet 1542 series outdoor access points only.

The access points associated to a mesh network can play one of the two roles:

- Root Access Point (RAP) - An access point can be a root access point for multiple mesh networks.
- Mesh Access Point (MAP) - An access point can be a mesh access point for only one single mesh network at a time.

DHCP and NAT Functionality on Root AP - IPv4 Scenario

This feature enables the controller to send a TLV to RAP when a new RAP joins the controller.

The following covers the workflow:

- Controller pushes TLV to RAP for enabling DHCP and NAT functionality.
- Client associates to an SSID.
- RAP executes DHCP funtionality to assign private IPv4 address to the client.
- RAP executes NAT functionality to get the private IPv4 address of the client and allow access to the network.

Configuring DHCP Server on Root Access Point (RAP)

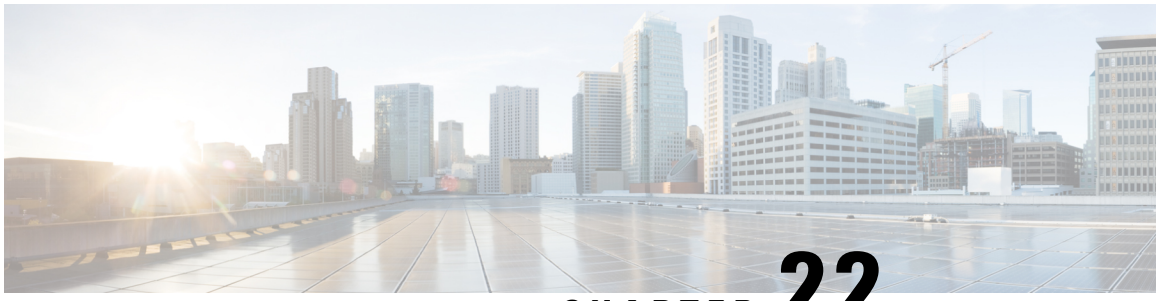
Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures an AP Profile.
Step 3	**dhcp-server** **Example:** `Device(config-ap-profile)# dhcp-server`	Configures DHCP server on the root access point.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Saves the configuration and exits configuration mode and returns to privileged **EXEC** mode.

Verifying DHCP Server for Root AP Configuration

To verify the DHCP server for root AP configuration, use the following command:

```
Device# show ap config general
Cisco AP Name   : AP4C77.6DF2.D588
================================================
<SNIP>
Dhcp Server                                     : Enabled
```



CHAPTER 22

Configuring Bi-Directional Rate Limiting Support with AAA Override

- Information About Bi-Directional Rate Limiting with AAA Override, on page 187
- Configuring Time of Day, on page 188
- Verifying Time of Day Configuration, on page 191

Information About Bi-Directional Rate Limiting with AAA Override

When a wireless client joins an access point, certain QoS policies get enforced on the access point. One such feature is the rate limiting for both upstream and downstream traffic at AP. The rate limiting feature when clubbed with AAA override supports specific set of policies based on the time of day and day of week. The AAA override then applies these policies coming from a RADIUS server to the access point.

Let's consider a use case of time of the day in conjunction with user role. Usually, the user role is used as an extra matching criteria along with the time of day. You can club the time of day usage with any matching criteria to get the desired result. The matching will be performed when the client joins the controller.

You can configure policies as two separate components:

- Defining policy attributes as service templates that are specific to clients joining the network and applying policy match criteria.
- Applying match criteria to the policy.

To configure Bi-Directional rate limiting, perform the following:

- Create a class map.

Note You can apply a service template using either a class map or parameter map.

- Create a policy map.
- Create a service template.

Note If class-map has to be used, associate the class-map to the policy-map and associate the service-template to the class-map.

- Associate the policy-map to the policy profile.

Configuring Time of Day

Creating a Class Map

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**class-map type control subscriber match-all** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-all match_tod`	Specifies the class map type and name.
Step 3	**match join-time-of-day** *start-time end-time* **Example:** `Device(config-filter-control-classmap)# match join-time-of-day 10:30 12:30`	Specifies a match to the time of day. Here, join time is considered for matching. For example, if the match filter is set from 11:00 am to 2:00 pm, a device joining at 10:59 am is not considered, even if it acquires credentials after 11:00 am. You should also disable AAA override for this command to work. Here, *start-time* and *end-time* specifies the 24-hour format.
Step 4	**match day** *day-of-week* **Example:** `Device(config-filter-control-classmap)# match day Mon`	Specifies a match to the day of week.
Step 5	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-filter-control-classmap)# end`	Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a Policy Map

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map type control subscriber** *policy-map-name* **Example:** `Device(config)# policy-map type control subscriber match_tod`	Specifies the policy map type.
Step 3	**event identity-update match-all** **Example:** `Device(config-event-control-policymap)# event identity-update match-all`	Specifies the match criteria to the policy map.

Step 4	*class-num* **class** *class-map-name*
	Example:
	`Device(config-class-control-policymap)# 1 class match_tod do-until-failure`
	Example:
	`Device(config-action-control-policymap)# 1 activate service-template match_tod`
	Example:
	`Device(config-action-control-policymap)# map attribute-to-service table param`
		Configures the local profiling policy class map number and specifies how to perform the action or activates the service template or maps an identity-update attribute to an auto-configured template.
		action-index **activate service-template** *service-template-name*
		The following example shows how a parameter map has to be applied (service template is already associated with the parameter map *param* while creating it):

Step 5	**end** **Example:** `Device(config-action-control-policymap)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 6	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 7	**wireless profile policy** *profile-policy*	Configures a wireless policy profile.

	Command or Action	Purpose
	Example: `Device(config)# wireless profile policy default-policy-profile`	**Caution** Do not configure **aaa-override** for native profiling under a named wireless profile policy.
Step 8	**description** *profile-policy-description* **Example:** `Device(config-wireless-policy)# description "default policy profile"`	Adds a description for the policy profile.
Step 9	**subscriber-policy-name** *policy-name* **Example:** `Device(config-wireless-policy)# subscriber-policy-name match_tod`	Configures the subscriber policy name.
Step 10	**vlan** *vlan-id* **Example:** `Device(config-wireless-policy)# vlan 59`	Configures a VLAN name or VLAN ID.
Step 11	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a Service Template

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**service-template** *service-template-name* **Example:** `Device(config)# service-template match_tod`	Enters service template configuration mode.
Step 3	**sgt** *sgt_value* **Example:** `Device(config-service-template)# sgt 100`	Configures SGT.
Step 4	**end** **Example:** `Device(config-service-template)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

	Command or Action	Purpose
		Note This way when a wireless client joins an access point on Monday (day of week), the client gets an SGT of 100 along with a VLAN.

Verifying Time of Day Configuration

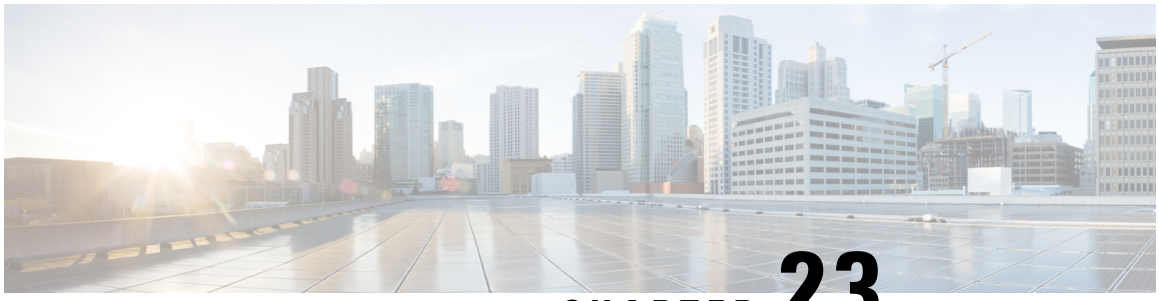
To view class map details for a class map name, use the following command:

```
Device# show class-map type control subscriber name test
Class-map               Action                        Exec  Hit  Miss  Comp
---------                ------                       ----  ---  ----   ---
match-any test     match day Monday                     0     0    0     0
match-any test     match join-time-of-day 8:00 18:00    0     0    0     0
Key:
  "Exec" - The number of times this line was executed
  "Hit"  - The number of times this line evaluated to TRUE
  "Miss" - The number of times this line evaluated to FALSE
  "Comp" - The number of times this line completed the execution of its
       condition without a need to continue on to the end
```

PART III

Radio Resource Management

- Radio Resource Management, on page 195
- Coverage Hole Detection, on page 227
- Optimized Roaming, on page 233
- Cisco Flexible Radio Assignment, on page 237
- XOR Radio Support, on page 243
- Cisco Receiver Start of Packet, on page 249
- Client Limit, on page 253
- IP Theft, on page 255
- Unscheduled Automatic Power Save Delivery, on page 261
- Enabling USB Port on Access Points, on page 263
- Dynamic Frequency Selection, on page 267



CHAPTER 23

Radio Resource Management

- Information About Radio Resource Management, on page 195
- Restrictions for Radio Resource Management, on page 203
- How to Configure RRM, on page 204
- Monitoring RRM Parameters and RF Group Status, on page 222
- Examples: RF Group Configuration, on page 223
- Information About ED-RRM, on page 223

Information About Radio Resource Management

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

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

RRM performs these functions:

- Radio resource monitoring
- Power control transmission
- Dynamic channel assignment
- Coverage hole detection and correction
- RF grouping

Note RRM grouping does not occur when an AP operates in a static channel that is not in the DCA channel list. The Neighbor Discovery Protocol (NDP) is sent only on DCA channels; therefore, when a radio operates on a non-DCA channel, it does not receive NDP on the channel.

Radio Resource Monitoring

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

Lightweight access points can scan all the valid channels for the country of operation as well as for channels available in other locations. The access points in local mode go *offchannel* for a period not greater than 70 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

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

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

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 Cisco Catalyst 9800 Series Wireless Controller into a single RF group enables the RRM algorithms to scale beyond the capabilities of a single Cisco Catalyst 9800 Series Wireless 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 controllers .

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

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

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

RF Group Leader

RF Group Leader can be configured in two ways as follows:

Note RF Group Leader is chosen on the basis of the controller with the greatest AP capacity (platform limit.) If multiple controllers have the same capacity, the leader is the one with the highest management IP address.

- 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.

If Dynamic Channel Assignment (DCA) needs to use the worst-performing radio as the single criterion for adopting a new channel plan, it can result in pinning or cascading problems.

The main cause of both pinning and cascading is that any potential channel plan changes are controlled by the RF circumstances of the worst-performing radio. The DCA algorithm does not do this; instead, it does the following:

- Multiple local searches: The DCA search algorithm performs multiple local searches initiated by different radios in the same DCA run rather than performing a single global search that is driven by a single radio. This change addresses both pinning and cascading, while maintaining the desired flexibility and adaptability of DCA and without jeopardizing stability.

- Multiple Channel Plan Change Initiators (CPCIs): Previously, the single worst radio was the sole initiator of a channel plan change. Now each radio in an RF group is evaluated and prioritized as a potential initiator. Intelligent randomization of the resulting list ensures that every radio is eventually evaluated, which eliminates the potential for pinning.
- Limiting the propagation of channel plan changes (Localization): For each CPCI radio, the DCA algorithm performs a local search for a better channel plan, but only the CPCI radio itself and its one-hop neighboring access points are actually allowed to change their current transmit channels. The impact of an access point triggering a channel plan change is felt only to within two RF hops from that access point, and the actual channel plan changes are confined to within a one-hop RF neighborhood. Because this limitation applies across all CPCI radios, cascading cannot occur.
- Non-RSSI-based cumulative cost metric: A cumulative cost metric measures how well an entire region, neighborhood, or network performs with respect to a given channel plan. The individual cost metrics of all the access points in that area are considered in order to provide an overall understanding of the channel plan's quality. These metrics ensure that the improvement or deterioration of each single radio is factored into any channel plan change. The objective is to prevent channel plan changes in which a single radio improves, but at the expense of multiple other radios experiencing a considerable performance decline.

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

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

RF Grouping Failure Reason Codes

RF Grouping failure reason codes and their explanations are listed below:

Table 4: RF Grouping Failure Reason Codes

Reason Code	Description
1	Maximum number (20) of controllers are already present in the group.
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.

Reason Code	Description
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.

Secure RF Groups

Secure RF groups enable to encrypt and secure RF grouping and RRM message exchanges over DTLS tunnel. During the DTLS handshake controllers authenticate each other with wireless management trust-point certificate.

Note If a controller has to be part of secure RF-group, that controller must be part of the same mobility group.

Transmit Power Control

The device dynamically controls access point transmit power based on the 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.

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.

Cisco APs support power level changes in 3 dB granularity. TPC Min and Max power settings allow for values in 1 dB increments. The resulting power level will be rounded to the nearest value supported in the allowed powers entry for the AP model and the current serving channel.

Each AP model has its own set of power levels localized for its regulatory country and region. Moreover, the power levels for the same AP model will vary based on the band and channel it is set to. For more information on Allowed Power Level vs. Actual power(in dBm), use the **show ap name <name> config slot <0|1|2|3>**

command to view the specific number of power levels, the range of power levels allowed, and the current power level setting on the AP.

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. Devices 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 device'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 device 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 device 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 device 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 device. Using the RRM algorithms, the device 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 device 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 device may choose to avoid this channel. In huge deployments in which all nonoverlapping channels are occupied, the device 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 device 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 device 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 DCA supports only 20-MHz channels in 2.4-GHz band.

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-device environment, the RRM startup mode is invoked after the device is upgraded and rebooted.
- In a multiple-device environment, the RRM startup mode is invoked after an RF Group leader is elected.
- You can trigger the RRM startup mode from the CLI.

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

Note DCA algorithm interval is set to 1 hour, but DCA algorithm always runs in default interval of 10 min, channel allocation occurs at 10-min intervals for the first 10 cycles, and channel changes occur as per the DCA algorithm every 10 min. After that the DCA algorithm goes back to the configured time interval. This is common for both DCA interval and anchor time because it follows the steady state.

Note If Dynamic Channel Assignment (DCA)/Transmit Power Control (TPC) is turned off on the RF group member, and auto is set on RF group leader, the channel or TX power on a member gets changed as per the algorithm that is run on the RF group leader.

Dynamic Bandwidth Selection

While upgrading from 11n to 11ac, the Dynamic Bandwidth Selection (DBS) algorithm provides a smooth transition for various configurations.

The following pointers describe the functionalities of DBS:

- It applies an additional layer of bias on top of those applied to the core DCA, for channel assignment in order to maximize the network throughput by dynamically varying the channel width.
- It fine tunes the channel allocations by constantly monitoring the channel and Base Station Subsystem (BSS) statistics.
- It evaluates the transient parameters, such as 11n or 11ac client mix, load, and traffic flow types.
- It reacts to the fast-changing statistics by varying the BSS channel width or adapting to the unique and new channel orientations through 11ac for selection between 40 MHz and 80 MHz bandwidths.

Coverage Hole Detection and Correction

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

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

Restrictions for Radio Resource Management

- The number of APs in a RF-group is limited to 3000.
- If an AP tries to join the RF-group that already holds the maximum number of APs it can support, the device rejects the application and throws an error.
- Disabling all data rates for default rf-profile or custom rf-profile, impacts ISSU upgrade and client join process after the software upgrade (ISSU or non-ISSU). To prevent this, you must enable at least one data rate (for example, **ap dot11 24 rate RATE_5_5M enable**) on the default rf-profile or custom rf-profile. We recommend that you enable the lowest data rate if efficiency is of prime concern.

How to Configure RRM

Configuring Neighbor Discovery Type (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 On the **Radio Resource Management** page, click either the **5 GHz Band** or the **2.4 GHz Band** tab.

Step 3 In the **General** tab under **Noise/Interference/Rogue/CleanAir# Monitoring Channels**, choose either **Transparent** or **Protected** from the **RRM Neighbor Discover Type** drop-down list.

Step 4 Click Apply to save your configuration.

Configuring Neighbor Discovery Type (CLI)

Procedure

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

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

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

Configuring RF Groups

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

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 In Auto mode , RF group leader will skip TPC and DCA for first three runs of grouping cycle in order to stabilize the RF-group

Configuring RF Group Selection Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 On the **RRM** page, click the relevant band's tab: either **5 GHz Band** or **2.4 GHz Band**.

Step 3 Click the **RF Grouping** tab.

Step 4 Choose the appropriate **Group Mode** from these options:

- Automatic: Sets the 802.11 RF group selection to automatic update mode
- Leader: Sets the 802.11 RF group selection to leader mode
- Off: Disables the 802.11 RF group selection

Step 5 Save the configuration.

Configuring RF Group Selection Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {24ghz | 5ghz} rrm group-mode**{**auto | leader | off**} **Example:** `Device(config)#ap dot11 24ghz rrm group-mode leader`	Configures RF group selection mode for 802.11 bands. • **auto**: Sets the 802.11 RF group selection to automatic update mode. • **leader**: Sets the 802.11 RF group selection to leader mode. • **off**: Disables the 802.11 RF group selection.

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

Configuring an RF Group Name (CLI)

Procedure

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

Configuring Members in an 802.11 Static RF Group (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 On the **RRM** page, click either the **5 GHz Band** or **2.4 GHz Band** tab.

Step 3 Click the **RF Grouping** tab.

Step 4 Choose the appropriate **Group Mode** from the following options:

- **Automatic(default)**: 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 if RF group members experience major changes).
- **Leader**: A device as an RF group leader, manually. In this mode, the leader and the members are manually configured and are therefore fixed. If the members are unable to join the RF group, the reason is indicated. The members' management IP addresses and system name are used to request the member to join the leader. The leader tries to establish a connection with a member every 1 minute if the member has not joined in the previous attempt.

- **Off**: No RF group is configured.

Step 5 Under **Group Members** section, click **Add**.

Step 6 In the **Add Static Member** window that is displayed, enter the controller name and the IPv4 or IPv6 address of the controller.

Step 7 Click **Save & Apply to Device**.

Configuring Members in an 802.11 Static RF Group (CLI)

Procedure

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

Configuring Transmit Power Control

Configuring Transmit Power (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 On the **5 GHz Band** or **2.4 GHz Band** tab, click the **TPC** tab.

Step 3 Choose of the following dynamic transmit power assignment modes:

- *Automatic*(default): The transmit power is periodically updated for all APs that permit this operation.
- *On Demand*: The transmit power is updated on demand. If you choose this option, you get to view the **Invoke Power Update Once**. Click **Invoke Power Update Once** to apply the RRM data successfully.
- *Fixed*: No dynamic transmit power assignments occur and values are set to their global default.

Step 4 Enter the maximum and minimum power level assignment on this radio. If you configure maximum transmit power, RRM does not allow any access point attached to the device to exceed this transmit power level

(whether the power is set by RRM TPC or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, then no access point would transmit above 11 dBm, unless the access point is configured manually. The range is –10 dBm to 30 dBm.

Step 5 In the **Power Threshold** field, enter the cutoff signal level used by RRM when determining whether to reduce an access point's power.

The default value for this parameter varies depending on the TPC version you choose. For TPCv1, the default value is –70 dBm, and for TPCv2, the default value is –67 dBm. The default value 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 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 might have difficulty processing a large number of BSSIDs or a high beacon rate and might exhibit problematic behavior with the default threshold.

Step 6 Click **Apply**.

Configuring the Tx-Power Control Threshold (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm tpc-threshold** *threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm tpc-threshold -60`	Configures the Tx-power control threshold used by RRM for auto power assignment. The range is from –80 to –50.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring the Tx-Power Level (CLI)

Procedure

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

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**ap dot11 {24ghz | 5ghz} rrm txpower** {*trans_power_level* | **auto** | **max** | **min** | **once**} **Example:** `Device(config)#ap dot11 24ghz rrm txpower auto`	Configures the 802.11 tx-power level • **trans_power_level**—Sets the transmit power level. • **auto**—Enables auto-RF. • **max**—Configures the maximum auto-RF tx-power. • **min**—Configures the minimum auto-RF tx-power. • **once**—Enables one-time auto-RF.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring 802.11 RRM Parameters

Configuring Advanced 802.11 Channel Assignment Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 In the **DCA** tab, choose a **Channel Assignment Mode** to specify the DCA mode:

- *Automatic*(default)—Causes the device to periodically evaluate and, if necessary, update the channel assignment for all joined APs.
- *Freeze*—Causes the device to evaluate and update the channel assignment for all joined APs. If you choose this option, you get to view the Invoke Channel Update Once. Click **Invoke Channel Update Once** to apply the RRM data successfully.
- *Off*—Turns off DCA and sets all AP 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.

Step 3 From the **Interval** drop-down list, choose the interval that tells how often the DCA algorithm is allowed to run. The default interval is 10 minutes.

Step 4 From the **AnchorTime** drop-down list, choose a number to specify the time of day when the DCA algorithm must 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 5 Check the **Avoid Foreign AP Interference** check box to cause the device's RRM algorithms to consider 802.11 traffic from foreign APs (those not included in your wireless network) when assigning channels to

lightweight APs, or uncheck it to disable this feature. For example, RRM may adjust the channel assignment to have access points avoid channels close to foreign APs. By default, this feature is in enabled state.

Step 6 Check the **Avoid Cisco AP Load** check box to cause the device's RRM algorithms to consider 802.11 traffic from Cisco lightweight APs in your wireless network when assigning channels. For example, RRM can assign better reuse patterns to access points that carry a heavier traffic load. By default, this feature is in disabled state.

Step 7 Check the **Avoid Non-802.11a Noise** check box to cause the device's RRM algorithms to consider noise (non-802.11 traffic) in the channel when assigning channels to lightweight APs. For example, RRM may have APs avoid channels with significant interference from non-AP sources, such as microwave ovens. By default, this feature is in enabled state.

Step 8 Check the **Avoid Persistent Non-WiFi Interference** check box to enable the device to take into account persistent non-Wi-Fi interference in DCA calculations. A persistent interfering device is any device from the following categories, which has been seen in the past 7 days - Microwave Oven, Video Camera, Canopy, WiMax Mobile, WiMax Fixed, Exalt Bridge. With **Avoid Persistent Non-WiFi Interference** enabled, if a Microwave Oven is detected, that interference from the Microwave Oven is taken into account in the DCA calculations for the next 7 days. After 7 days, if the interfering device is not detected anymore, it is no longer considered in the DCA calculations.

Step 9 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. The DCA threshold is 30 dB.
- *Medium* (default)—The DCA algorithm is moderately sensitive to environmental changes. The DCA threshold is 15 dB.
- *High* —The DCA algorithm is highly sensitive to environmental changes. The DCA threshold is 5 dB.

Step 10 Set the **Channel Width** as required. You can choose the RF channel width as 20 MHz, 40 MHz, 80 MHz, 160 MHz, or Best. This is applicable only for 802.11a/n/ac (5 GHZ) radio.

Step 11 The **Auto-RF Channel List** section shows the channels that are currently selected. To choose a channel, check the corresponding check box.

Step 12 In the **Event Driven RRM** section, check the **EDRRM** check box to run RRM when CleanAir-enabled AP detects a significant level of interference. If enabled, set the sensitivity threshold level at which the RRM is invoked, enter the custom threshold, and check the **Rogue Contribution** check box to enter the rogue duty-cycle.

Step 13 Click **Apply**.

Configuring Advanced 802.11 Channel Assignment Parameters (CLI)

Procedure

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

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

Step 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel dca** {**add** *channel-number* | **anchor-time** | **global** {**auto** | **once**} | **interval** | **min-metric** | **remove** *channel-number* | **sensitivity** {**high** | **low** | **medium**}}
	Example:
	`Device(config)#ap dot11 24ghz rrm channel dca interval 2`
		Configures Dynamic Channel Assignment (DCA) algorithm parameters for the 802.11 band.
		• **add** *channel-number*–Enter a channel number to be added to the DCA list. The range is between 1 to 14.
		• **anchor-time**–Configures the anchor time for the DCA. The range is between 0 and 23 hours.
		• **global**–Configures the DCA mode for all 802.11 Cisco APs.
		  • **auto**–Enables auto-RF.
		  • **once**–Enables auto-RF only once.
		• **interval**–Configures the DCA interval value. The values are 1, 2, 3, 4, 6, 8, 12 and 24 hours and the default value 0 denotes 10 minutes.
		• **min-metric**–Configures the DCA minimum RSSI energy metric. The range is between -100 and -60.
		• **remove** *channel-number*–Enter the channel number to be removed from the DCA list. The range is between 1 to 14.
		• **sensitivity**–Configures the DCA sensitivity level to changes in the environment.
		  • **high**–Specifies the most sensitivity.
		  • **low**–Specifies the least sensitivity.

	Command or Action	Purpose
		• **medium**–Specifies medium sensitivity.
Step 4	**ap dot11 5ghz rrm channel dca chan-width** {**20** | **40** | **80 | best** | **160 | best maximum** {**20** | **40** | **80** | **MAX**}} **Example:** `Device(config)#ap dot11 5ghz rrm channel dca chan-width best`	Configures the DCA channel bandwidth for all 802.11 radios in the 5-GHz band. Sets the channel bandwidth to 20 MHz, 40 MHz, 80 MHz, or Best; 20 MHz is the default value for channel bandwidth. 80 MHz is the default value for best. Set the channel bandwidth to best before configuring the constraints.
Step 5	**ap dot11 5ghz rrm channel dca chan-width width-max** {**WIDTH_20MHz** | **WIDTH_40MHz** | **WIDTH_80MHz** | **WIDTH_MAX**} **Example:** `Device(config)#ap dot11 5ghz rrm channel dca chan-width width-max WIDTH_80MHz`	Configures the maximum channel bandwidth that can be assigned to a channel. In this example, *WIDTH_80MHz* assigns the channel bandwidth to 20 MHz, 40 MHz, or 80 MHz but not greater than that.
Step 6	**ap dot11** {**24ghz** | **5ghz**} **rrm channel device** **Example:** `Device(config)#ap dot11 24ghz rrm channel device`	Configures the persistent non-Wi-Fi device avoidance in the 802.11 channel assignment.
Step 7	**ap dot11** {**24ghz** | **5ghz**} **rrm channel foreign** **Example:** `Device(config)#ap dot11 24ghz rrm channel foreign`	Configures the foreign AP 802.11 interference avoidance in the channel assignment.
Step 8	**ap dot11** {**24ghz** | **5ghz**} **rrm channel load** **Example:** `Device(config)#ap dot11 24ghz rrm channel load`	Configures the Cisco AP 802.11 load avoidance in the channel assignment.
Step 9	**ap dot11** {**24ghz** | **5ghz**} **rrm channel noise** **Example:** `Device(config)#ap dot11 24ghz rrm channel noise`	Configures the 802.11 noise avoidance in the channel assignment.

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

Configuring 802.11 Coverage Hole Detection (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM** to configure Radio Resource Management parameters for 802.11a/n/ac (5-GHz) and 802.11b/g/n (2.4-GHz) radios.

Step 2 On the**Radio Resource Management** page, click **Coverage** tab.

Step 3 To enable coverage hole detection, check the **Enable Coverage Hole Detection** check box.

Step 4 In the **Data Packet Count** field, enter the number of data packets.

Step 5 In the **Data Packet Percentage** field, enter the percentage of data packets.

Step 6 In the **Data RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 dBm to -90 dBm; the default value is –80 dBm.

Step 7 In the **Voice Packet Count** field, enter the number of voice data packets.

Step 8 In the **Voice Packet Percentage** field, enter the percentage of voice data packets.

Step 9 In the **Voice RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 dBm to -90 dBm; the default value is –80 dBm.

Step 10 In the **Minimum Failed Client per AP** field, enter the minimum number of clients on an AP with a signal-to-noise ratio (SNR) below the coverage threshold. Value ranges from 1 to 75 and the default value is 3.

Step 11 In the **Percent Coverage Exception Level per AP** field, enter the maximum desired percentage of clients on an access point's radio operating below the desired coverage threshold and click **Apply**. Value ranges from 0 to 100% and the default value is 25%.

Configuring 802.11 Coverage Hole Detection (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {24ghz | 5ghz} rrm coverage data**{**fail-percentage | packet-count | rssi-threshold**} **Example:**	Configures the 802.11 coverage hole detection for data packets. • **fail-percentage**: Configures the 802.11 coverage failure-rate threshold for uplink

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

Configuring 802.11 Event Logging (CLI)

Procedure

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

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

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

Configuring 802.11 Statistics Monitoring (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM** to configure Radio Resource Management parameters for 802.11a/n/ac (5 GHz) and 802.11b/g/n (2.4 GHz) radios.

Step 2 In the **Monitor Intervals(60 to 3600secs)** section, proceed as follows:

a) To configure the 802.11 noise measurement interval (channel scan interval), set the **AP Noise Interval**. The valid range is from 60 to 3600 seconds.

b) To configure the 802.11 signal measurement interval (neighbor packet frequency), set the **AP Signal Strength Interval**. The valid range is from 60 to 3600 seconds.

c) To configure the 802.11 coverage measurement interval, set the **AP Coverage Interval**. The valid range is from 60 to 3600 seconds.
d) To configure the 802.11 load measurement, set the **AP Load Interval**. The valid range is from 60 to 3600 seconds.

Step 3 Click **Apply**.

Configuring 802.11 Statistics Monitoring (CLI)

Procedure

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

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

Configuring the 802.11 Performance Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join** page, click the name of the profile or click **Add** to create a new one.

Step 3 In the **Add/Edit RF Profile** window, click the **RRM** tab.

Step 4 In the **General** tab that is displayed, enter the following parameters:

a) In the **Interference (%)** field, enter the threshold value for 802.11 foreign interference that ranges between 0 and 100 percent.

b) In the **Clients** field, enter the threshold value for 802.11 Cisco AP clients that range between 1 and 75 clients.

c) In the **Noise (dBm)** field, enter the threshold value for 802.11 foreign noise ranges between –127 and 0 dBm.

d) In the **Utilization(%)** field, enter the threshold value for 802.11 RF utilization that ranges between 0 to 100 percent.

Step 5 Click **Update & Apply to Device**.

Configuring the 802.11 Performance Profile (CLI)

Procedure

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

	Command or Action	Purpose
	`Device(config)#ap dot11 24ghz rrm profile clients 20`	
Step 3	**ap dot11** {**24ghz** | **5ghz**} **rrm profile foreign** *int_threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm profile foreign 50`	Sets the threshold value for 802.11 foreign interference that ranges between 0 and 100%.
Step 4	**ap dot11** {**24ghz** | **5ghz**} **rrm profile noise** *for_noise_threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm profile noise -65`	Sets the threshold value for 802.11 foreign noise ranges between –127 and 0 dBm.
Step 5	**ap dot11** {**24ghz** | **5ghz**} **rrm profile throughput** *throughput_threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm profile throughput 10000`	Sets the threshold value for 802.11 Cisco AP throughput that ranges between 1000 and 10000000 bytes per second.
Step 6	**ap dot11** {**24ghz** | **5ghz**} **rrm profile utilization** *rf_util_threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm profile utilization 75`	Sets the threshold value for 802.11 RF utilization that ranges between 0 to 100%.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring Advanced 802.11 RRM

Enabling Channel Assignment (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 In the **RRM** page, click the relevant band's tab: either **5 GHz Band** or **2.4 GHz Band**.

Step 3 Click the **DCA** tab

Step 4 In the **Dynamic Channel Assignment Algorithm** section, choose the appropriate **Channel Assignment Mode** from these options:

- Automatic: Sets the channel assignment to automatic.
- Freeze: Locks the channel assignment. Click **Invoke Channel Update Once** to refresh the assigned channels.

Step 5 Click **Apply**.

Enabling Channel Assignment (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel-update** **Example:** `Device# ap dot11 24ghz rrm channel-update`	Enables the 802.11 channel selection update for each of the Cisco access points. **Note** After you enable **ap dot11 {24ghz | 5ghz} rrm channel-update**, a token is assigned for channel assignment in the DCA algorithm.

Restarting DCA Operation

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm dca restart** **Example:** `Device# ap dot11 24ghz rrm dca restart`	Restarts the DCA cycle for 802.11 radio.

Updating Power Assignment Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 On the **Access Points** page, click the AP name from the 5GHz or 2.4 GHz list.

Step 3 In the **Edit Radios** > **Configure** > **Tx Power Level Assignment** section, choose **Custom** from the **Assignment Method** droup-down list.

Step 4 Choose the value for **Transmit Power** from the drop-down list.

Step 5 Click **Update & Apply to Device**.

Updating Power Assignment Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm txpower update** **Example:** `Device# ap dot11 24ghz rrm txpower update`	Updates the 802.11 transmit power for each of the Cisco access points.

Configuring Rogue Access Point Detection in RF Groups

Configuring Rogue Access Point Detection in RF Groups (CLI)

Before you begin

Ensure 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 controller have different names, false alarms will occur.

Procedure

	Command or Action	Purpose
Step 1	**ap name** *Cisco_AP* **mode** {**monitor** | **clear** | **sensor** | **sniffer**} **Example:** `Device# ap name ap1 mode clear`	Perform this step for every access point connected to the controller . Configures the following AP modes of operation: • **monitor**:Sets the AP mode to monitor mode. • **clear**: Resets AP mode to local or remote based on the site. • **sensor**: Sets the AP mode to sensor mode. • **sniffer**: Sets the AP mode to wireless sniffer mode.
Step 2	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 3	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 4	**wireless wps ap-authentication** **Example:** `Device (config)# wireless wps ap-authentication`	Enables rogue access point detection.
Step 5	**wireless wps ap-authentication threshold** *value* **Example:** `Device (config)# wireless wps ap-authentication threshold 50`	Specifies when a rogue access point alarm is generated. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period. The valid threshold range is from 1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value. **Note** Enable rogue access point detection and threshold value on every 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 controller with this feature disabled are reported as rogues.

Monitoring RRM Parameters and RF Group Status

Monitoring RRM Parameters

Table 5: Commands for monitoring Radio Resource Management

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

Verifying RF Group Status (CLI)

This section describes the new commands for RF group status.

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

Table 6: Verifying Aggressive Load Balancing Command

Command	Purpose

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

Examples: RF Group Configuration

This example shows how to configure RF group name:

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

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

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

Information About ED-RRM

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. Once a channel change occurs due to event-driven RRM, the channel is blocked list for three hours to avoid selection. 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.

Configuring ED-RRM on the Cisco Wireless LAN Controller (CLI)

Procedure

Step 1 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:

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event** —Configures CleanAir driven RRM parameters for the 802.11 Cisco lightweight access points.

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**low** | **medium** | **high** | **custom**}—Configures CleanAir driven RRM sensitivity for the 802.11 Cisco lightweight access points. Default selection is Medium.

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event custom-threshold** *custom-threshold-value*—Triggers the ED-RRM event at the set threshold value. The custom threshold values range from 1 to 99.

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contribution**—Enables rogue contribution.

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contribution duty-cycle** *thresholdvalue*—Configures threshold value for rogue contribution. The valid range is from 1 to 99, with 80 as the default.

Step 2 Save your changes by entering this command:

write memory

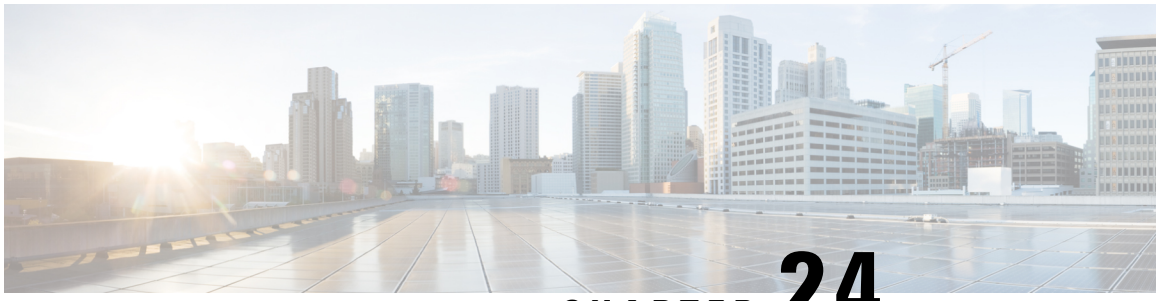
Step 3 See the CleanAir configuration for the 802.11a/n/ac or 802.11b/g/n network by entering this command:

show ap dot11 {**24ghz** | **5ghz**} **cleanair config**

Information similar to the following appears:

```
CleanAir Solution................................ : Enabled
Air Quality Settings:
Air Quality Reporting........................ : Enabled
Air Quality Reporting Period (min)........... : 15
Air Quality Alarms........................... : Disabled
Air Quality Alarm Threshold.................. : 10
Unclassified Interference.................... : Disabled
Unclassified Severity Threshold.............. : 35
Interference Device Settings:
Interference Device Reporting................ : Enabled
BLE Beacon.............................. : Enabled
Bluetooth Link........................... : Enabled
Microwave Oven........................... : Enabled
802.11 FH................................ : Enabled
Bluetooth Discovery...................... : Enabled
TDD Transmitter.......................... : Enabled
Jammer................................... : Enabled
Continuous Transmitter................... : Enabled
DECT-like Phone.......................... : Enabled
Video Camera............................. : Enabled
802.15.4................................. : Enabled
WiFi Inverted............................ : Enabled
WiFi Invalid Channel..................... : Enabled
SuperAG.................................. : Enabled
Canopy................................... : Enabled
Microsoft Device......................... : Enabled
WiMax Mobile............................. : Enabled
WiMax Fixed.............................. : Enabled
Interference Device Types Triggering Alarms:
BLE Beacon.............................. : Disabled
Bluetooth Link........................... : Disabled
Microwave Oven........................... : Disabled
802.11 FH................................ : Disabled
Bluetooth Discovery...................... : Disabled
TDD Transmitter.......................... : Disabled
Jammer................................... : Disabled
Continuous Transmitter................... : Disabled
DECT-like Phone.......................... : Disabled
Video Camera............................. : Disabled
```

```
802.15.4.............................. : Disabled
WiFi Inverted......................... : Enabled
WiFi Invalid Channel.................. : Enabled
SuperAG............................... : Disabled
Canopy................................ : Disabled
Microsoft Device...................... : Disabled
WiMax Mobile.......................... : Disabled
WiMax Fixed........................... : Disabled
Interference Device Alarms............ : Disabled
AdditionalClean Air Settings:
CleanAir Event-driven RRM State....... : Disabled
CleanAir Driven RRM Sensitivity....... : LOW
CleanAir Driven RRM Sensitivity Level..... : 35
CleanAir Event-driven RRM Rogue Option..... : Disabled
CleanAir Event-driven RRM Rogue Duty Cycle... : 80
CleanAir Persistent Devices state..... : Disabled
CleanAir Persistent Device Propagation..... : Disabled
```



CHAPTER 24

Coverage Hole Detection

• Coverage Hole Detection and Correction, on page 227

Coverage Hole Detection and Correction

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

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

Configuring Coverage Hole Detection (GUI)

Follow the procedure given below to configure client accounting.

Procedure

Step 1 Click **Configuration** > **Radio Configurations** > **RRM**.

On this page, you can configure Radio Resource Management parameters for 802.11a/n/ac (5 GHZ) and 802.11b/g/n (2.4 GHZ) radios, and flexible radio assignment parameters.

Step 2 Check the **Enable Coverage Hole Detection** check box.

Enables coverage hole detection.

Configuring Coverage Hole Detection (CLI)

Coverage Hole Detection (CHD) is based on upstream RSSI metrics observed by the AP.

Note To revert back radios from 5-GHz to 24-GHz for CHD, ensure that the 5-GHz radio is UP and Client Network Preference value is other than the default.

Follow the procedure given below to configure CHD:

Before you begin

Disable the 802.11 network before applying the configuration.

Procedure

	Command or Action	Purpose
Step 1	**ap dot11 {24ghz | 5ghz} rrm coverage** **Example:** `Device(config)# ap dot11 24ghz rrm coverage`	Configures the 802.11 coverage level for data packets. Use the **no** form of the command to disable CHD.

Step 2	**ap dot11 {24ghz | 5ghz} rrm coverage data** {**fail-percentage | packet-count | rssi-threshold**}
	Example:
	`Device(config)# ap dot11 24ghz rrm coverage`
	`data fail-percentage 60`
		Configures the 802.11 coverage level for data packets.
		• **fail-percentage**: Configures the 802.11 coverage failure-rate threshold for uplink data packets as a percentage that ranges from 1 to 100%.
		• **packet-count**: Configures the 802.11 coverage minimum failure count threshold for uplink data packets that ranges from 1 to 255.
		• **rssi-threshold**: Configures the 802.11 minimum receive coverage level for data packets that range from –90 to –60 dBm.

Step 3	**ap dot11 {24ghz | 5ghz} rrm coverage exception global** *exception level*
	Example:
	`Device(config)# ap dot11 24ghz rrm coverage`
	`exception global 50`
		Configures the 802.11 Cisco AP coverage exception level as a percentage that ranges from 0 to 100%.

	Command or Action	Purpose

Step 4	**ap dot11{24ghz | 5ghz}rrm coverage level global** *cli_min exception level*
	Example:
	`Device(config)# ap dot11 24ghz rrm coverage`
	`level global 10`
		Configures the 802.11 Cisco AP client minimum exception level that ranges from 1 to 75 clients.

Step 5	**ap dot11 {24ghz | 5ghz} rrm coverage voice** {**fail-percentage | packet-count | rssi-threshold**}
	Example:
	`Device(config)# ap dot11 24ghz rrm coverage`
	`voice packet-count 10`
		Configures the 802.11 coverage hole detection for voice packets.
		• **fail-percentage**: Configures the 802.11 coverage failure-rate threshold for uplink voice packets as a percentage that ranges from 1 to 100%.
		• **packet-count**: Configures the 802.11 coverage minimum failure count threshold for uplink voice packets that ranges from 1 to 255.
		• **rssi-threshold**: Configures the 802.11 minimum receive coverage level for voice packets that range from –90 to –60 dBm.

Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 7	**show ap dot11 {24ghz | 5ghz} coverage** **Example:** `Device# show ap dot11 5ghz coverage`	Displays the CHD details.

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.

Configuring CHD for RF Tag Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 On the **Coverage** tab, select the **Enable Coverage Hole Detection** check box.

Step 3 In the **Data Packet Count** field, enter the number of data packets.

Step 4 In the **Data Packet Percentage** field, enter the percentage of data packets.

Step 5 In the **Data RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 dBm to -90 dBm; the default value is –80 dBm.

Step 6 In the **Voice Packet Count** field, enter the number of voice data packets.

Step 7 In the **Voice Packet Percentage** field, enter the percentage of voice data packets.

Step 8 In the **Voice RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 dBm to -90 dBm; the default value is –80 dBm.

Step 9 In the **Minimum Failed Client per AP** field, enter the minimum number of clients on an AP with a signal-to-noise ratio (SNR) below the coverage threshold. Value ranges from 1 to 75 and the default value is 3.

Step 10 In the **Percent Coverage Exception Level per AP** field, enter the maximum desired percentage of clients on an access point's radio operating below the desired coverage threshold and click Apply. Value ranges from 0 to 100% and the default value is 25%.

Step 11 Click **Apply**.

Configuring CHD for RF Profile (CLI)

Follow the procedure given below to configure Coverage Hole Detection (CHD) for RF profile.

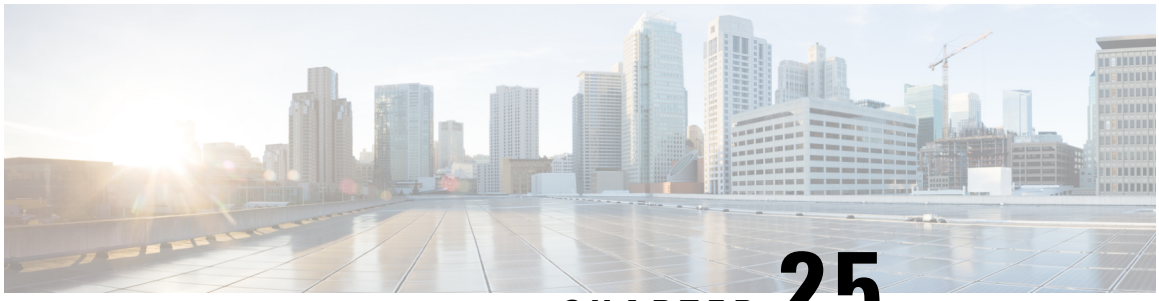
Before you begin

Ensure that the RF profile is already created.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** } **rf-profile** *rf-profile-tag* **Example:** `Device(config)# ap dot11 24ghz rf-profile alpha-rfprofile-24ghz`	Configures the 802.11 coverage hole detection for data packets.

	Command or Action	Purpose
Step 3	**coverage data rssi threshold** *threshold-value* **Example:** `Device(config-rf-profile)# coverage data rssi threshold -80`	Configures the minimum RSSI value for data packets received by the access point. Valid values range from -90 to -60 in dBm.
Step 4	**end** **Example:** `Device(config-rf-profile)# end`	Returns to privileged EXEC mode.
Step 5	**show ap dot11 24ghz rf-profile summary** **Example:** `Device# show ap dot11 24ghz rf-profile summary`	Displays summary of the available RF profiles.



CHAPTER 25

Optimized Roaming

- Optimized Roaming, on page 233
- Restrictions for Optimized Roaming, on page 233
- Configuring Optimized Roaming (GUI), on page 234
- Configuring Optimized Roaming (CLI), on page 234

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. 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) prealarm 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

- You cannot configure the optimized roaming interval until you disable the 802.11a/b network.

- 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.
- The Cisco Catalyst 9800 controller increments the 80211v smart roam failed counter while disconnecting the client due to optimized roaming.
- We recommend that you do not use the optimized roaming feature with RSSI low check.

Configuring Optimized Roaming (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Advanced**.

Step 2 On the **Advanced** page, click the relevant band's tab: either **5 GHz Band** or **2.4 GHz Band**.

Step 3 Check the **Optimized Roaming Mode** check box to enable the feature.

Step 4 Choose the required **Optimized Roaming Date Rate Threshold**. The threshold value options are different for 802.11a and 802.11b networks.

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.

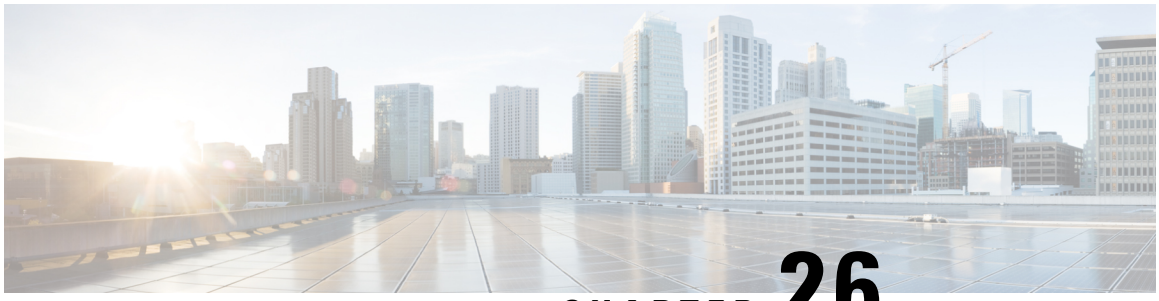
Step 5 Click **Apply** to save the configuration.

Configuring Optimized Roaming (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap dot11 5ghz rrm optimized-roam**	Configures 802.11a or 802.11b optimized roaming. By default, optimized roaming is disabled.
Step 2	**ap dot11 5ghz rrm optimized-roam reporting-interval** *interval-seconds*	Configures the client coverage reporting interval for 802.11a or 802.11b networks. The range is from 5 to 90 seconds. The default value is 90 seconds.

	Command or Action	Purpose
		Note You must disable the 802.11a network before you configure the optimized roaming reporting interval. The access point sends the client statistics to the controller based on the following conditions: • When the **reporting-interval** *interval-seconds* is set to 90 seconds by default. • When the **reporting-interval** *interval-seconds* is configured (for instance to 10 secs) only during optimized roaming failure due to the Coverage Hole Detection (CHD) RED ALARM.
Step 3	**ap dot11 5ghz rrm optimized-roam data-rate-threshold** *mbps*	Configure the threshold data rate for 802.11a networks. For 802.11a, the configurable data rates are 1, 2, 6, 9, 12, 18, 24, 36, 48, and 54. You can configure DISABLE to disable the data rate.
Step 4	**show wireless statistics ap dot11 5ghz optimized-roaming statistics**	Displays optimized roaming statistics for each band.



CHAPTER 26

Cisco Flexible Radio Assignment

- Information About Flexible Radio Assignment, on page 237
- Configuring an FRA Radio (CLI), on page 238
- Configuring an FRA Radio (GUI), on page 240

Information About Flexible Radio Assignment

Flexible Radio Assignment (FRA) takes advantage of the dual-band radios included in APs. The FRA is a new feature added to the RRM to analyze the Neighbor Discovery Protocol (NDP) measurements, which manages the hardware used to determine the role of the new flexible radio (2.4 GHz, 5 GHz, or monitor) in your network.

Traditional legacy dual–band APs always had 2 radio slots, (1 slot per band) and were organized by the band they were serving, that is slot 0= 802.11b,g,n and slot 1=802.11a,n,ac.

XOR Support in 2.4-GHz or 5-GHz Bands

The flexible radio (XOR) offers the ability to serve the 2.4-GHz or the 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 can 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 completely separate macro (wide-area cells) or two micro cells (small cells) for HDX or any combination.

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).

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 an AP propagated the change to the entire AP, that is both radio slot 0 and slot 1. The addition of the XOR radio in the slot 0 position provides the ability to operate a single radio interface in many of the previous modes, eliminating the need to place the whole AP into a mode. When this concept is applied to a single radio level, its is called *role*. Three such roles can be assigned now:

- Client Serving
- Either 2.4 GHz(1) or 5 GHz(2)
- Monitor-Monitor mode (3)

Note

- MODE: Assigned to a whole AP (slot 0 and slot 1)
- ROLE: Assigned to a single radio interface (slot 0)

Benefits of the FRA

- Solves the problem of 2.4–GHz over coverage.
- Creating two diverse 5–GHz cells doubles the airtime that is available.
- Permits one AP with one Ethernet drop to function like two 5–GHz APs.
- Introduces the concept of Macro/Micro cells for airtime efficiency.
- Allows more bandwidth to be applied to an area within a larger coverage cell.
- Can be used to address nonlinear traffic.
- Enhances the High-Density Experience (HDX) with one AP.
- XOR radio can be selected by the corresponding user in either band–servicing client mode or monitor mode.

Configuring an FRA Radio (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**[no] ap fra** **Example:** `Device(config)# [no] ap fra`	Enables or disables FRA on the AP.
Step 4	**ap fra interval** **Example:** `Device(config)# ap fra interval 3`	Configures the FRA interval in hours. The range is 1 to 24 hours. **Note** The FRA interval has to be more than the configured RRM interval.
Step 5	**ap fra sensitivity** {**high** | **medium** | **low**} **Example:** `Device(config)# ap fra sensitivity high`	Configures the FRA sensitivity. • **high**: Sets the FRA Coverage Overlap Sensitivity to **high**. • **medium**: Sets the FRA Coverage Overlap Sensitivity to **medium**. • **low**: Sets the FRA Coverage Overlap Sensitivity to **low**.
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 7	**ap fra revert** {**all** | **auto-only**}{**auto** | **static**} **Example:** `Device# ap fra revert all auto`	Rolls back the XOR Radio state. • **all**: Reverts all XOR Radios • **auto-only**: Revert only XOR radios currently in automatic band selection. • **auto**: Sets the XOR radios in automatic band selection. • **static**: Sets the XOR radio in static 2.4-GHz band.
Step 8	**show ap dot11** {**24ghz** | **5ghz**} **summary** **Example:** `Device# show ap dot11 5ghz summary`	Shows the configuration and statistics of 802.11 Cisco APs

Step 9	Device# **show ap fra**
	Example:
	`Device# show ap fra`
	`FRA State : Disabled`
	`FRA Sensitivity : medium (95%)`
		Shows the current FRA configuration.

	Command or Action	Purpose
	FRA Interval : 1 Hour(s) AP Name MAC Address Slot ID Current-Band COF % Suggested Mode --- AP00A6.CA36.295A 006b.f09c.8290 0 2.4GHz None 2.4GHz COF : Coverage Overlap Factor test_machine#	
Step 10	**show ap name** *ap-name* **config dot11 dual-band** **Example:** Device# **show ap name config dot11 dual-band**	Shows the current 802.11 dual-band parameters in a given AP.

Configuring an FRA Radio (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM** > **FRA**.

Step 2 In the **Flexible Radio Assignment** window, enable FRA status and determine the overlapping 2.4 GHz or 5 GHz coverage for each AP, choose **Enabled** in the **FRA Status** field. By default, the FRA status is disabled.

Step 3 Under the From the **FRA Interval** drop-down list, choose the FRA run interval. The interval values range from 1 hour to 24 hours. You can choose the FRA run interval value only after you enable the FRA status.

Step 4 From the **FRA Sensitivity** drop-down list, choose the percentage of Coverage Overlap Factor (COF) required to consider a radio as redundant. You can select the supported value only after you enable the FRA status.

The supported values are as follows:

- Low: 100 percent
- Medium (default): 95 percent
- High: 90 percent

The **Last Run** and **Last Run Time** fields will show the time FRA was run last and the time it was run.

Step 5 Check the **Client Aware** check box to take decisions on redundancy.

When enabled, the **Client Aware** feature monitors the dedicated 5-GHz radio and when the client load passes a pre-set threshold, automatically changes the Flexible Radio assignment from a monitor role into a 5-GHz role, effectively doubling the capacity of the cell on demand. Once the capacity crisis is over and Wi-Fi load returns to normal, the radios resume their previous roles.

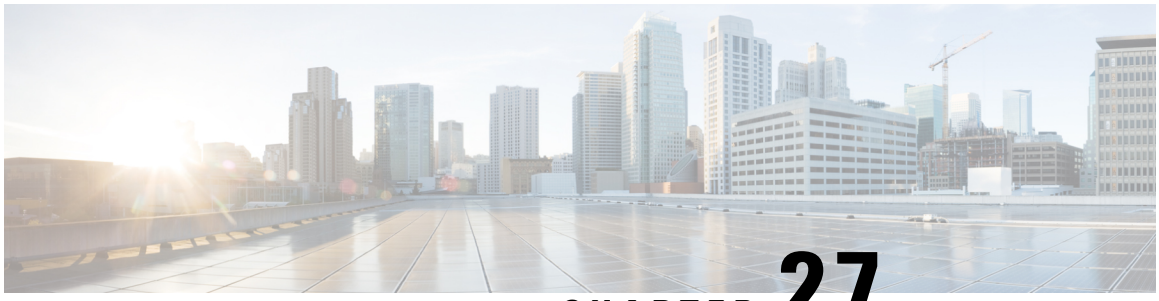
Step 6 In the **Client Select** field, enter a value for client selection. The valid values range between 0 and 100 percent. The default value is 50 percent.

This means that if the dedicated 5-GHz interface reaches 50% channel utilization, this will trigger the monitor role dual-band interface to transition to a 5-GHz client-serving role.

Step 7 In the **Client Reset** field, enter a reset value for the client. The valid values range between 0 and 100 percent. The default value is 5 percent.

Once the AP is operating as a dual 5-GHz AP, this setting indicates the reduction in the combined radios' overall channel utilization required to reset the dual-band radio to monitor role.

Step 8 Click **Apply** to save the configuration.



CHAPTER 27

XOR Radio Support

- Information About Dual-Band Radio Support , on page 243
- Configuring Default XOR Radio Support, on page 244
- Configuring XOR Radio Support for the Specified Slot Number (GUI), on page 246
- Configuring XOR Radio Support for the Specified Slot Number, on page 246

Information About Dual-Band Radio Support

The Dual-Band (XOR) radio in Cisco 2800, 3800, 4800, and the 9120 series AP models offer the ability to serve 2.4–GHz or 5–GHz bands or passively monitor both the bands on the same AP. These APs can be configured to serve clients in 2.4–GHz and 5–GHz bands, or serially scan both 2.4–GHz and 5–GHz bands on the flexible radio while the main 5–GHz radio serves clients.

Cisco APs models up and through the Cisco 9120 APs are designed to support dual 5–GHz band operations with the *i* model supporting a dedicated Macro/Micro architecture and the *e* and *p* models supporting Macro/Macro. The Cisco 9130AXI APs and the Cisco 9136 APs support dual 5-GHz operations as Micro/Messo cell.

When a radio moves between bands (from 2.4-GHz to 5-GHz and vice versa), clients need to be steered to get an optimal distribution across radios. When an AP has two radios in the 5–GHz band, client steering algorithms contained in the Flexible Radio Assignment (FRA) algorithm are used to steer a client between the same band co-resident radios.

The XOR radio support can be steered manually or automatically:

- Manual steering of a band on a radio—The band on the XOR radio can only be changed manually.
- Automatic client and band steering on the radios is managed by the FRA feature that monitors and changes the band configurations as per site requirements.

Note RF measurement will not run when a static channel is configured on slot 1. Due to this, the dual band radio slot 0 will move only with 5–GHz radio and not to the monitor mode.

When slot 1 radio is disabled, RF measurement will not run, and the dual band radio slot 0 will be only on 2.4–GHz radio.

Configuring Default XOR Radio Support

Before you begin

Note The default radio points to the XOR radio hosted on slot 0.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 dual-band antenna ext-ant-gain** *antenna_gain_value* **Example:** `Device# ap name ap-name dot11 dual-band antenna ext-ant-gain 2`	Configures the 802.11 dual-band antenna on a specific Cisco access point. *antenna_gain_value*: The valid range is from 0 to 40.
Step 3	**ap name** *ap-name* **[no] dot11 dual-band shutdown** **Example:** `Device# ap name ap-name dot11 dual-band shutdown`	Shuts down the default dual-band radio on a specific Cisco access point. Use the **no** form of the command to enable the radio.
Step 4	**ap name** *ap-name* **dot11 dual-band role manual client-serving** **Example:** `Device# ap name ap-name dot11 dual-band role manual client-serving`	Switchs to client–serving mode on the Cisco access point.
Step 5	**ap name** *ap-name* **dot11 dual-band band 24ghz** **Example:** `Device# ap name ap-name dot11 dual-band band 24ghz`	Switchs to 2.4-GHz radio band.
Step 6	**ap name** *ap-name* **dot11 dual-band txpower** {*transmit_power_level* | **auto**} **Example:**	Configures the transmit power for the radio on a specific Cisco access point.

	Command or Action	Purpose
	`Device# ap name ap-name dot11 dual-band txpower 2`	**Note** When an FRA-capable radio (slot 0 on 9120 AP[for instance]) is set to Auto, you cannot configure static channel and Txpower on this radio. If you want to configure static channel and Txpower on this radio, you will need to change the radio role to Manual Client-Serving mode.
Step 7	**ap name** *ap-name* **dot11 dual-band channel** *channel-number* **Example:** `Device# ap name ap-name dot11 dual-band channel 2`	Enters the channel for the dual band. *channel-number*—The valid range is from 1 to 173.
Step 8	**ap name** *ap-name* **dot11 dual-band channel auto** **Example:** `Device# ap name ap-name dot11 dual-band channel auto`	Enables the auto channel assignment for the dual-band.
Step 9	**ap name** *ap-name* **dot11 dual-band channel width**{**20 MHz** | **40 MHz** | **80 MHz** | **160 MHz**} **Example:** `Device# ap name ap-name dot11 dual-band channel width 20 MHz`	Chooses the channel width for the dual band.
Step 10	**ap name** *ap-name* **dot11 dual-band cleanair** **Example:** `Device# ap name ap-name dot11 dual-band cleanair`	Enables the Cisco CleanAir feature on the dual-band radio.

Step 11	**ap name** *ap-name* **dot11 dual-band cleanair band**{**24 GHz | 5 GMHz**}
	Example:
	`Device# ap name ap-name dot11 dual-band cleanair band 5 GHz`
	`Device# ap name ap-name [no] dot11 dual-band cleanair band 5 GHz`
		Selects a band for the Cisco CleanAir feature.
		Use the **no** form of this command to disable the Cisco CleanAir feature.

Step 12	**ap name** *ap-name* **dot11 dual-band dot11n antenna** {**A | B | C | D**} **Example:**	Configures the 802.11n dual-band parameters for a specific access point.

	Command or Action	Purpose
	`Device# ap name ap-name dot11 dual-band dot11n antenna A`	
Step 13	**show ap name** *ap-name* **auto-rf dot11 dual-band** **Example:** `Device# show ap name ap-name auto-rf dot11 dual-band`	Displays the auto-RF information for the Cisco access point.
Step 14	**show ap name** *ap-name* **wlan dot11 dual-band** **Example:** `Device# show ap name ap-name wlan dot11 dual-band`	Displays the list of BSSIDs for the Cisco access point.

Configuring XOR Radio Support for the Specified Slot Number (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Dual-Band Radios** section, select the AP for which you want to configure dual-band radios.

The AP name, MAC address, CleanAir capability and slot information for the AP are displayed. If the Hyperlocation method is HALO, the antenna PID and antenna design information are also displayed.

Step 3 Click **Configure**.

Step 4 In the **General** tab, set the **Admin Status** as required.

Step 5 Set the **CleanAir Admin Status** field to Enable or Disable.

Step 6 Click **Update & Apply to Device**.

Configuring XOR Radio Support for the Specified Slot Number

Procedure

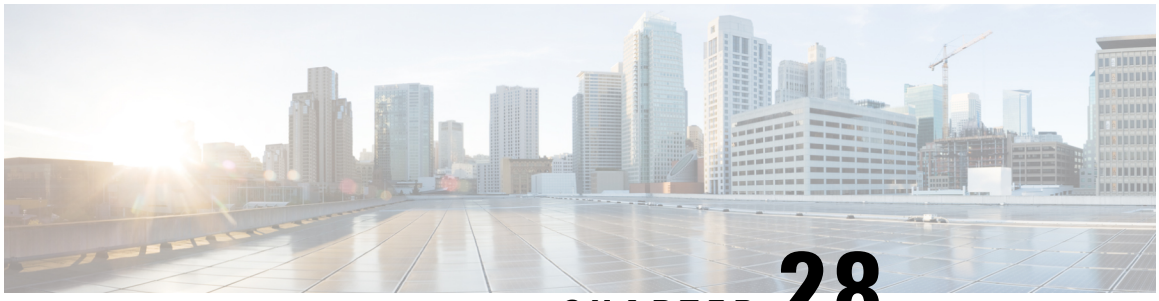
	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.

	Command or Action	Purpose
Step 2	**ap name** *ap-name* **dot11 dual-band slot 0 antenna ext-ant-gain** *external_antenna_gain_value* **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 antenna ext-ant-gain 2`	Configures dual-band antenna for the XOR radio hosted on slot 0 for a specific access point. *external_antenna_gain_value* - Is the external antenna gain value in multiples of .5 dBi unit. The valid range is from 0 to 40. **Note** • For APs supporting self-identifying antennas (SIA), the gain depends on the antenna, and not on the AP model. The gain is learned by the AP and there is no need for controller configuration. • For APs that do not support SIA, the APs send the antenna gain in the configuration payload, where the default antenna gain depends on the AP model.
Step 3	**ap name** *ap-name* **dot11 dual-band slot 0 band** {**24ghz** | **5ghz**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 band 24ghz`	Configures current band for the XOR radio hosted on slot 0 for a specific access point.
Step 4	**ap name** *ap-name* **dot11 dual-band slot 0 channel** {*channel_number* | **auto** | **width** [**160** | **20** | **40** | **80**]} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 channel 3`	Configures dual-band channel for the XOR radio hosted on slot 0 for a specific access point. *channel_number*- The valid range is from 1 to 165.
Step 5	**ap name** *ap-name* **dot11 dual-band slot 0 cleanair band** {**24Ghz** | **5Ghz**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 cleanair band 24Ghz`	Enables CleanAir features for dual-band radios hosted on slot 0 for a specific access point.
Step 6	**ap name** *ap-name* **dot11 dual-band slot 0 dot11n antenna** {**A** | **B** | **C** | **D**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 dot11n antenna A`	Configures 802.11n dual-band parameters hosted on slot 0 for a specific access point. Here, **A**- Enables antenna port A. **B**- Enables antenna port B.

	Command or Action	Purpose
		C- Enables antenna port C. **D**- Enables antenna port D.
Step 7	**ap name** *ap-name* **dot11 dual-band slot 0 role** {**auto** | **manual** [**client-serving** | **monitor**]} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 role auto`	Configures dual-band role for the XOR radio hosted on slot 0 for a specific access point. The following are the dual-band roles: • **auto**- Refers to the automatic radio role selection. • **manual**- Refers to the manual radio role selection.

Step 8	**ap name** *ap-name* **dot11 dual-band slot 0 shutdown**
	Example:
	`Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 shutdown`
	`Device# ap name AP-SIDD-A06 [no] dot11 dual-band slot 0 shutdown`
		Disables dual-band radio hosted on slot 0 for a specific access point.
		Use the **no** form of this command to enable the dual-band radio.

Step 9	**ap name** *ap-name* **dot11 dual-band slot 0 txpower** {*tx_power_level* | **auto**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 txpower 2`	Configures dual-band transmit power for XOR radio hosted on slot 0 for a specific access point. • *tx_power_level*- Is the transmit power level in dBm. The valid range is from 1 to 8. • **auto**- Enables auto-RF.



CHAPTER 28

Cisco Receiver Start of Packet

- Information About Receiver Start of Packet Detection Threshold, on page 249
- Restrictions for Rx SOP, on page 249
- Configuring Rx SOP (CLI), on page 250
- Customizing RF Profile (CLI), on page 250

Information About Receiver Start of Packet Detection Threshold

The Receiver Start of Packet (Rx SOP) Detection Threshold feature 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 in high-density deployments, such as stadiums and auditoriums where access points need to optimize the nearest and strongest clients.

Restrictions for Rx SOP

- Rx SOP configuration is not applicable to the third radio module pluggable on Cisco Aironet 3600 Series APs.
- Rx SOP configurations are supported only in Local, FlexConnect, Bridge, and Flex+Bridge modes.
- Rx SOP configurations are not supported in the FlexConnect+PPPoE, FlexConnect+PPPoE-wIPS, and FlexConnect+OEAP submodes.

The following table shows the permitted range for the Rx SOP threshold.

Table 7: Rx SOP Threshold

Radio Band	Threshold High	Threshold Medium	Threshold Low
2.4 GHz	-79 dBm	-82 dBm	-85 dBm
5 GHz	-76 dBm	-78 dBm	-80 dBm

Configuring Rx SOP (CLI)

Procedure

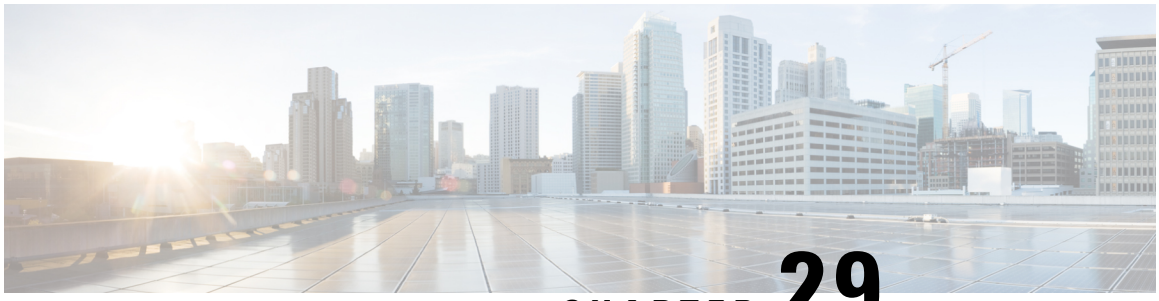
	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {24ghz | 5ghz} rx-sop threshold {auto | custom | high | low | medium}** **Example:** `Device(config)# ap dot11 5ghz rx-sop threshold high`	Configures the 802.11bg/802.11a radio Rx SOP threshold.
Step 3	end	Returns to privileged EXEC mode.
Step 4	**show ap dot11 {24ghz | 5ghz} high-density** **Example:** `Device# show ap dot11 5ghz high-density`	Displays the 802.11bg/802.11a high-density parameters.
Step 5	**show ap summary** **Example:** `Device# show ap summary`	Displays a summary of all the connected Cisco APs.

Customizing RF Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz | 5ghz** } **rf-profile** *profile-name* **Example:** `Device(config)# ap dot11 24ghz rf-profile AHS_2.4ghz`	Configures the 802.11a and 11b parameters.

	Command or Action	Purpose
Step 3	**high-density rx-sop threshold {auto | custom | high | low | medium}** **Example:** `Device(config-rf-profile)# high-density rx-sop threshold high`	Configures the 802.11bg, 802.11a high-density parameters.
Step 4	**show ap summary** **Example:** `Device# show ap summary`	Displays a summary of all the connected Cisco APs.
Step 5	end	Returns to privileged EXEC mode. **Note** • Irrespective of radio mode, the controller configures the radio with configured RX-SOP value. The AP determines whether to use the configured RX-SOP value. • For the XOR radio (Slot 0), when the AP is in monitor mode the RX-SOP value that gets pushed to AP depends on the band it was operating before moving to monitor mode (basically if radio operating band is 24g then RX-SOP params picked from 24GHz RF profile (or default rf-profile). If it was in 5g then RX-SOP params picked from 5GHz RF profile (or default rf-profile) configured for the AP).



CHAPTER 29

Client Limit

- Information About Client Limit, on page 253
- Configuring Client Limit Per WLAN (GUI), on page 253
- Configuring Client Limit Per WLAN (CLI), on page 253

Information About Client Limit

This feature enforces a limit on the number of clients that can to be associated with an AP. Further, you can configure the number of clients that can be associated with each AP radio.

Configuring Client Limit Per WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click a WLAN from the list of WLANs.

Step 3 Click the **Advanced** tab.

Step 4 Under the **Max Client Connections** settings, enter the client limit for **Per WLAN**, **Per AP Per WLAN**, and **Per AP Radio Per WLAN**.

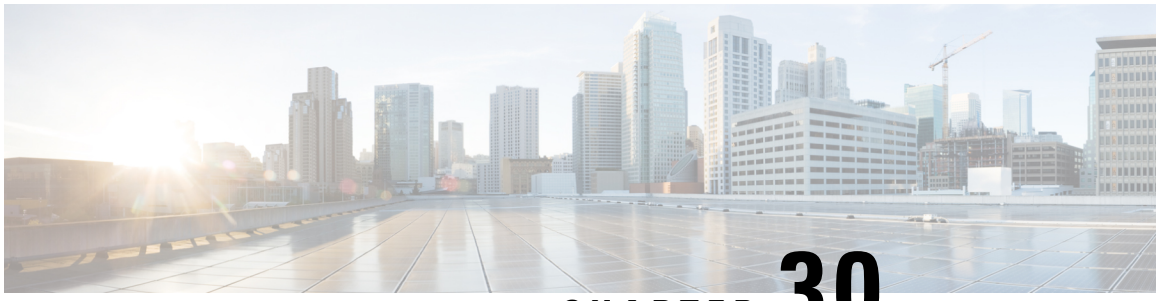
Step 5 Click **Update & Apply to Device**.

Configuring Client Limit Per WLAN (CLI)

Procedure

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

	Command or Action	Purpose
	`Device# enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wlan** *wlan-name* **Example:** `Device(config)# wlan ramban`	Specifies the WLAN name.
Step 4	**client association limit** *maximum-clients-per-WLAN* **Example:** `Device(config-wlan)# client association limit 110`	Configures the maximum number of clients that can be associated to the given WLAN.
Step 5	**client association limit ap** *max-clients-per-AP-per-WLAN* **Example:** `Device(config-wlan)# client association limit ap 120`	Configures the maximum number of clients that can be associated to an AP in the WLAN.
Step 6	**client association limit radio** *max-clients-per-AP-radio-per-WLAN* **Example:** `Device(config-wlan)# client association limit radio 100`	Configures the maximum number of clients that can be associated to an AP radio in the WLAN.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 8	**show wlan id** *wlan-id* **Example:** `Device#  show wlan id 2`	Displays the current configuration of the WLAN and the corresponding client association limits.



CHAPTER 30

IP Theft

- Introduction to IP Theft, on page 255
- Configuring IP Theft (GUI), on page 256
- Configuring IP Theft, on page 256
- Configuring the IP Theft Exclusion Timer, on page 256
- Adding Static Entries for Wired Hosts, on page 257
- Verifying IP Theft Configuration, on page 258

Introduction to IP Theft

The IP Theft feature prevents the usage of an IP address that is already assigned to another device. If the controller finds that two wireless clients are using the same IP address, it declares the client with lesser precedence binding as the IP thief and allows the other client to continue. If blocked list is enabled, the client is put on the exclusion list and thrown out.

The IP Theft feature is enabled by default on the controller. The preference level of the clients (new and existing clients in the database) are also used to report IP theft. The preference level is a learning type or source of learning, such as Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), data glean (looking at the IP data packet that shows what IP address the client is using), and so on. The wired clients always get a higher preference level. If a wireless client tries to steal the wired IP, that client is declared as a thief.

The order of preference for IPv4 clients are:

1. DHCPv4
2. ARP
3. Data packets

The order of preference for IPv6 clients are:

1. DHCPv6
2. NDP
3. Data packets

Note The static wired clients have a higher preference over DHCP.

Configuring IP Theft (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Wireless Protection Policies** > **Client Exclusion Policies**.

Step 2 Check the **IP Theft or IP Reuse** check box.

Step 3 Click **Apply**.

Configuring IP Theft

Follow the procedure given below to configure the IP Theft feature:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps client-exclusion ip-theft** **Example:** `Device(config)# wireless wps client-exclusion ip-theft`	Configures the client exclusion policy.

Configuring the IP Theft Exclusion Timer

Follow the procedure given below to configure the IP theft exclusion timer:

Procedure

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

	Command or Action	Purpose
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 3	**exclusionlist timeout** *time-in-seconds* **Example:** `Device(config-wireless-policy)# exclusionlist timeout 5`	Specifies the timeout, in seconds. The valid range is from 0-2147483647. Enter zero (0) for no timeout.

Adding Static Entries for Wired Hosts

Follow the procedure given below to create static wired bindings:

Note The statically configured wired bindings and locally configured SVI IP addresses have a higher precedence than DHCP.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	Use the first option to configure an IPv4 static entry or the second option to create an IPv6 static entry. • **device-tracking binding vlan** *vlan-id ipv4-address* **interface gigabitEthernet***ge-intf-num hardware-or-mac-address* • **device-tracking binding vlan** *vlan-id ipv6-address* **interface gigabitEthernet***ge-intf-num hardware-or-mac-address* **Example:** `Device(config)# device-tracking binding vlan 20 20.20.20.5 interface gigabitEthernet 1 0000.1111.2222` **Example:**	Configures IPv4 or IPv6 static entry.

	Command or Action	Purpose
	Device(config)# device-tracking binding vlan 20 2200:20:20::6 interface gigabitEthernet 1 0000.444.3333	

Verifying IP Theft Configuration

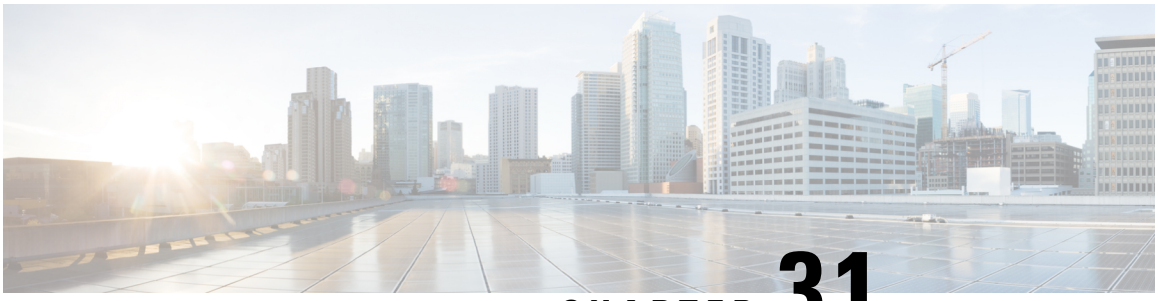
Use the following command to check if the IP Theft feature is enabled or not:

```
Device# show wireless wps summary

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
  Cids Shun failure                       : Enabled
  Misconfiguration failure                : Enabled
  Failed Qos Policy                       : Enabled
  Failed Epm                              : Enabled
```

Use the following commands to view additional details about the IP Theft feature:

```
Device# show wireless client summary

Number of Local Clients: 1

MAC Address    AP Name                WLAN State              Protocol Method     Role
-------------------------------------------------------------------------------------------
000b.bbb1.0001 SimAP-1                2    Run                11a      None       Local


Number of Excluded Clients: 1

MAC Address    AP Name                WLAN State              Protocol Method
-------------------------------------------------------------------------------------------
10da.4320.cce9 charlie2               2    Excluded           11ac     None


Device# show wireless device-tracking database ip

IP                              VLAN  STATE       DISCOVERY   MAC
  ------------------------------------------------------------------------
  20.20.20.2                     20    Reachable   Local       001e.14cc.cbff
  20.20.20.6                     20    Reachable   IPv4 DHCP   000b.bbb1.0001


Device# show wireless exclusionlist

Excluded Clients

MAC Address       Description          Exclusion Reason               Time Remaining
-------------------------------------------------------------------------------------------
10da.4320.cce9                         IP address theft                    59
```

```
Device# show wireless exclusionlist client mac 12da.4820.cce9 detail

Client State : Excluded
Client MAC Address : 12da.4820.cce9
Client IPv4 Address: 20.20.20.6
Client IPv6 Address: N/A
Client Username: N/A
Exclusion Reason : IP address theft
Authentication Method : None
Protocol: 802.11ac
AP MAC Address : 58ac.780e.08f0
AP Name: charlie2
AP slot : 1
Wireless LAN Id : 2
Wireless LAN Name: mhe-ewlc
VLAN Id : 20
```



CHAPTER 31

Unscheduled Automatic Power Save Delivery

- Information About Unscheduled Automatic Power Save Delivery, on page 261
- Viewing Unscheduled Automatic Power Save Delivery (CLI), on page 261

Information About Unscheduled Automatic Power Save Delivery

Unscheduled automatic power save delivery (U-APSD) is a QoS facility that is defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending the battery life, this feature reduces the latency of traffic flow that is delivered over the wireless media. Because U-APSD does not require the client to poll each individual packet that is 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.

Viewing Unscheduled Automatic Power Save Delivery (CLI)

Procedure

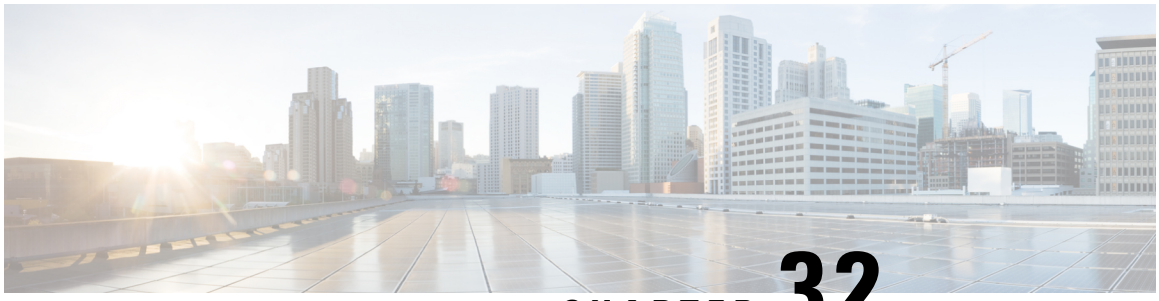
show wireless client mac-address *client_mac* **detail**

Example:

```
Device# show wireless client mac-address 2B:5B:B3:18:56:E9 detail
Output Policy State : Unknown
Output Policy Source : Unknown
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 15
  APSD ACs    : BK(T/D), BE, VI(T/D), VO(T/D)
Power Save : OFF
Current Rate :

--------------------------
BK : Background
BE : Best Effort
VI : Video
VO : Voice.

T: UAPSD Trigger Enabled
```

```
D: UAPSD Delivery Enabled
T/D : UAPSD Trigger and Delivery Enabled
```

Show detailed information of a client by MAC address.



CHAPTER 32

Enabling USB Port on Access Points

- USB Port as Power Source for Access Points, on page 263
- Configuring an AP Profile (CLI), on page 264
- Configuring USB Settings for an Access Point (CLI), on page 264
- Monitoring USB Configurations for Access Points (CLI), on page 265

USB Port as Power Source for Access Points

Some Cisco 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. Refer to the datasheet of your AP to check if the AP has a USB port that can act as a source of power.

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 an AP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters the AP profile configuration mode. **Note** When you delete a named profile, the APs associated with that profile will not revert to the default profile.
Step 3	**usb-enable** **Example:** `Device(config-ap-profile)# usb-enable`	Enables USB for each AP profile. **Note** By default, the USB for each AP profile is enabled. Use the **no usb-enable** command to disable USB for each AP profile.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring USB Settings for an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **usb-module** **Example:** `Device# ap name AP44d3.xy45.69a1 usb-module`	Enables the USB port on the AP. Use the **ap name** *ap-name* **no usb-module** command to disable the USB port on the AP.

	Command or Action	Purpose
Step 3	**ap name** *ap-name* **usb-module override** **Example:** `Device# ap name AP44d3.xy45.69a1 usb-module override`	Overrides USB status of the AP profile and considers the local AP configuration. Use the **ap name** *ap-name* **no usb-module override** command to override USB status of the AP and consider the AP profile configuration. **Note** You can configure the USB status for an AP only if you enable USB override for it.

Monitoring USB Configurations for Access Points (CLI)

- To view the inventory details of APs, use the following command:

  show ap name *ap-name* **inventory**

  The following is a sample output:

```
Device# show ap name AP500F.8059.1620  inventory
NAME: AP2800    , DESCR: Cisco Aironet 2800 Series (IEEE 802.11ac) Access Point
PID: AIR-AP2802I-D-K9  ,  VID: 01,  SN: XXX1111Y2ZZZZ2800
NAME: SanDisk    , DESCR: Cruzer Blade
PID: SanDisk  ,  SN: XXXX1110010, MaxPower: 224
```

- To view the summary of an AP module, use the following command:

  show ap module summary

  The following is a sample output:

```
Device# show ap module summary
AP Name               External Module       External Module PID   External Module
Description
-----------------------------------------------------------------------------------------------
AP500F.1111.2222      Enable                SanDisk               Cruzer Blade
```

- To view the USB configuration details for each AP, use the following command:

  show ap name *ap-name* **config general**

  The following is a sample output:

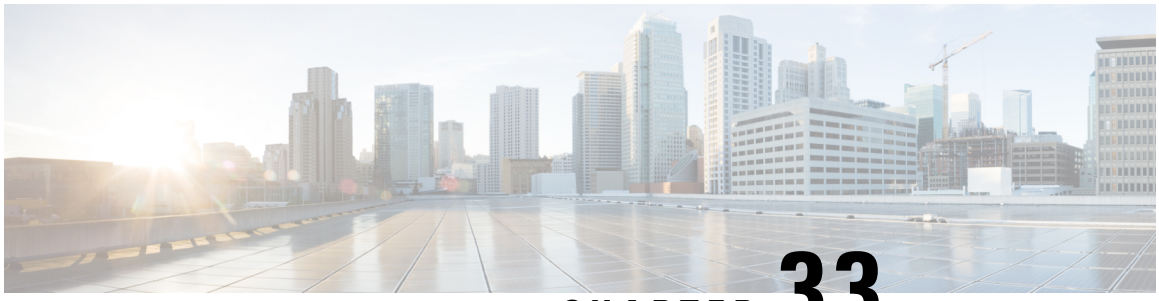
```
Device# show ap name AP500F.111.2222 config general

.
.
.
USB Module Type.................................. USB Module
USB Module Status................................ Disabled
USB Module Operational State..................... Enabled
USB Override ……..... Enabled
```

- To view status of the USB module, use the following command:

  show ap profile name *xyz* **detailed**

The following is a sample output:

```
Device# show ap profile name xyz detailed
USB Module                : ENABLED
```



CHAPTER 33

Dynamic Frequency Selection

- Information About Dynamic Frequency Selection, on page 267
- Configuring Dynamic Frequency Selection (GUI), on page 267
- Configuring Dynamic Frequency Selection, on page 267
- Verifying DFS, on page 268

Information About Dynamic Frequency Selection

Dynamic Frequency Selection (DFS) is the process of detecting radar signals and automatically setting the frequency on a DFS-enabled 5.0-GHz (802.11a/h) radio to avoid interference with the radar signals. Radios configured for use in a regulatory domain must not interfere with radar systems.

In normal DFS, when a radar signal is detected on any of the channels in the 40-MHz or 80-MHz bandwidth, the whole channel is blocked. With Flex DFS, if the radar signals are not detected on the secondary channel, the AP is moved to a secondary channel with a reduction in the bandwidth, usually, by half.

Configuring Dynamic Frequency Selection (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Choose a profile.

Step 3 In **General** tab, check the **Full sector DFS status** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Dynamic Frequency Selection

Follow the procedure given below to configure DFS:

Before you begin

- The corresponding AP must be on one of the DFS channels.
- Shut down the radio before applying the configuration changes.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**no ap dot11 5ghz dtpc** **Example:** `Device(config)# no ap dot11 5ghz dtpc`	Disables the 802.11a Dynamic Transmit Power Control (DTPC) setting.
Step 3	**ap dot11 5ghz channelswitch mode** *mode-num* **Example:** `Device(config)# ap dot11 5ghz channelswitch mode 1`	Configures the 802.11h channel switch mode.
Step 4	**ap dot11 5ghz power-constraint** *value* **Example:** `Device(config)# ap dot11 5ghz power-constraint 12`	Configures the 802.11h power-constraint value.
Step 5	**ap dot11 5ghz smart-dfs** **Example:** `Device(config)# ap dot11 5ghz smart-dfs`	Configures nonoccupancy time for the radar interference channel.

Verifying DFS

Use the following commands to verify the DFS configuration:

To display the 802.11h configuration, use the following command:

```
Device# show wireless dot11h
```

To display the auto-rF information for 802.11h configuration, use the following command:

```
Device# show ap auto-rf dot11 5ghz
```

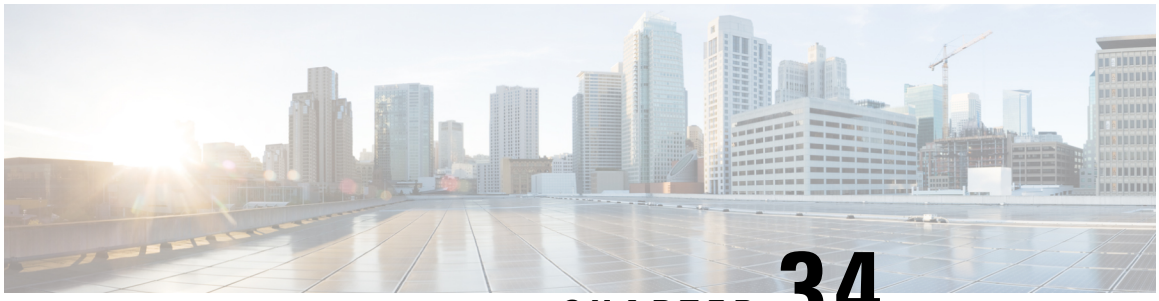
To display the auto-rF information for a Cisco AP, use the following command:

```
Device# show ap name ap1 auto-rf dot11 5gh
```

PART IV

Network Management

- AP Packet Capture, on page 271
- DHCP Option82, on page 275
- RADIUS Realm, on page 285
- Cisco StadiumVision, on page 291
- Persistent SSID Broadcast, on page 295
- Network Monitoring, on page 297
- Creating a Lobby Ambassador Account, on page 301
- Guest User Accounts, on page 305



CHAPTER 34

AP Packet Capture

- Introduction to AP Client Packet Capture, on page 271
- Enabling Packet Capture (GUI), on page 271
- Enabling Packet Capture (CLI), on page 272
- Create AP Packet Capture Profile and Map to an AP Join Profile (GUI), on page 272
- Create AP Packet Capture Profile and Map to an AP Join Profile, on page 272
- Start or Stop Packet Capture, on page 273

Introduction to AP Client Packet Capture

The AP Client Packet Capture feature allows the packets on an AP to be captured for wireless client troubleshooting. The packet capture operation is performed on the AP by the radio drivers on the current channel on which it is operational, based on the specified packet capture filter. All the packets that are captured for a specific client are uploaded to a file in the FTP server. This file can be opened in Wireshark for packet inspection.

Limitations for AP Client Packet Capture

- The packet capture task can be performed for only one client at a time per site.
- Packet capture can be started on a specific AP or a set of APs using static mode. It can be started or stopped for the same client on different APs, when the capture is in progress.

  When packet capture is started in auto mode, system automatically selects the set of nearby APs to start packet capture for a specific client. In this mode, you cannot start or stop packet capture on individual APs. Use the **stop all** command to stop the packet capture when it is started in auto-mode.
- After the SSO is complete, the packet capture action will not continue after a switchover.

Enabling Packet Capture (GUI)

Procedure

Step 1 Choose **Troubleshooting** > **AP Packet Capture**.

Step 2 On the **Troubleshooting** page, in the **Start Packet Capture** section, in the **Client MAC Address** field, enter the client's MAC address.

Step 3 From the **Capture Mode** options, choose **Auto**.

Step 4 Click **Start**.

Enabling Packet Capture (CLI)

Follow the procedure given below to enable packet capture:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap packet-capture start** *client-mac-address* **auto** **Example:** `Device# ap packet-capture start 0011.0011.0011 auto`	Enables packet capture for the specified client on a set of nearby access points.

Create AP Packet Capture Profile and Map to an AP Join Profile (GUI)

Procedure

Step 1 Click **Configuration** > **Tags & Profiles** > **AP Join Profile**.

Step 2 Click **Add** to create a new AP Join Profile and enter the requisite details.

Step 3 In the **Add AP Join Profile** area, click **AP** > **Packet Capture**.

Step 4 Click the **Plus** icon to create a new Packet Capture profile or select one from the drop-down menu.

Step 5 Click **Save**.

Create AP Packet Capture Profile and Map to an AP Join Profile

While packet capture profile configurations are used for an AP, the packet capture profile is mapped to an AP profile. The AP profile is in turn mapped to site tag.

While starting packet capture, APs use the packet capture profile configurations based on the site and AP join profile they belong to.

Follow the procedure given below to create an AP packet capture profile and map it to an AP join profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode..
Step 2	**wireless profile ap packet-capture** *packet-capture-profile-name* **Example:** `Device(config)# wireless profile ap packet-capture test1`	Configures an AP profile.
Step 3	**ap profile** *profile-name* **Example:** `Device(config)# ap profile default-ap-profile`	Configures an AP packet capture profile.
Step 4	**packet-capture** *profile-name* **Example:** `Device(config-ap-profile)# packet-capture capture-test`	Enables packet capture on the AP profile.
Step 5	**end** **Example:** `Device(config-ap-profile)# end`	Exits the AP profile configuration mode.
Step 6	**show wireless profile ap packet-capture detailed** *profile-name* **Example:** `Device# show wireless profile ap packet-capture detailed test1`	Displays detailed information of the selected AP packet capture profile.

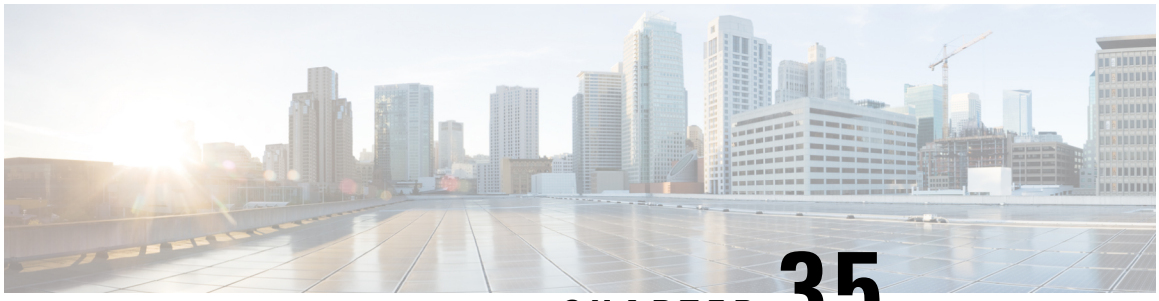
Start or Stop Packet Capture

Perform either of these tasks to start or stop a packet capture procedure.

Procedure

	Command or Action	Purpose
Step 1	**ap packet-capture start** *client-mac-address* {**auto** | **static** *ap-name* }	Enables packet capture for a client.

	Command or Action	Purpose
	Example: `Device# ap packet-capture start 0011.0011.0011 auto`	
Step 2	**ap packet-capture stop** *client-mac-address* {**all** | **static** *ap-name* } **Example:** `Device# ap packet-capture stop 0011.0011.0011 all`	Disables packet capture for a client.



CHAPTER 35

DHCP Option82

- Information About DHCP Option 82, on page 275
- Configuring DHCP Option 82 Global Interface, on page 276
- Configuring DHCP Option 82 Format, on page 278
- Configuring DHCP Option82 Through a VLAN Interface, on page 279

Information About DHCP Option 82

DHCP Option 82 is organized as a single DHCP option that contains information known by the relay agent. This feature provides additional security when DHCP is used to allocate network addresses, and enables the Cisco controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources.

The controller can be configured to add Option 82 information to DHCP requests from clients before forwarding the requests to a DHCP server. The DHCP server can then be configured to allocate IP addresses to the wireless client based on the information present in DHCP Option 82.

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the Options field of the DHCP message. The data items themselves are also called options. Option 82 contains information known by the relay agent.

The Relay Agent Information option is organized as a single DHCP option that contains one or more suboptions that convey information known by the relay agent. Option 82 was designed to allow a DHCP Relay Agent to insert circuit−specific information into a request that is being forwarded to a DHCP server. This option works by setting two suboptions:

- Circuit ID
- Remote ID

The Circuit ID suboption includes information that is specific to the circuit the request came in on. This suboption is an identifier that is specific to the relay agent. Thus, the circuit that is described will vary depending on the relay agent.

The Remote ID suboption includes information on the remote host–end of the circuit. This suboption usually contains information that identifies the relay agent. In a wireless network, this would likely be a unique identifier of the wireless access point.

You can configure the following DHCP Option 82 options in a controller :

- DHCP Enable

- DHCP Opt82 Enable
- DHCP Opt82 Ascii
- DHCP Opt82 RID
- DHCP Opt Format
- DHCP AP MAC
- DHCP SSID
- DHCP AP ETH MAC
- DHCP AP NAME
- DHCP Site Tag
- DHCP AP Location
- DHCP VLAN ID

Note The controller includes the SSID in ASCII and the VLAN-ID in hexadecimal format within the remote-ID sub-option of option 82 in the outgoing DHCP packets to the server for the following configurations:

```
ipv4 dhcp opt82 format ssid
ipv4 dhcp opt82 format vlan-id
```

However, if *ipv4 dhcp opt82 ascii* configuration is also present, the controller adds VLAN-ID and SSID in ASCII format.

For Cisco Catalyst 9800 Series Configuration Best Practices, see the following link: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/guide-c07-743627.html

Configuring DHCP Option 82 Global Interface

Configuring DHCP Option 82 Globally Through Server Override (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip dhcp-relay information option server-override** **Example:**	Inserts global server override and link selection suboptions.

	Command or Action	Purpose
	`Device(config)# ip dhcp-relay information option server-override`	

Configuring DHCP Option 82 Globally Through Different SVIs (GUI)

Procedure

Step 1 Choose **Configuration** > **VLAN**.

Step 2 Choose a VLAN from the drop-down list.

The **Edit SVI** window appears.

Step 3 Click the **Advanced** tab.

Step 4 Choose an option from the **IPv4 Inbound ACL** drop-down list.

Step 5 Choose an option from the **IPv4 Outbound ACL** drop-down list.

Step 6 Choose an option from the **IPv6 Inbound ACL** drop-down list.

Step 7 Choose an option from the **IPv6 Outbound ACL** drop-down list.

Step 8 Enter an IP address in the **IPv4 Helper Address** field.

Step 9 Set the status to **Enabled** if you want to enable the **Relay Information Option** setting.

Step 10 Enter the **Subscriber ID**.

Step 11 Set the status to **Enabled** if you want to enable the **Server ID Override** setting.

Step 12 Set the status to **Enabled** if you want to enable the **Option Insert** setting.

Step 13 Choose an option from the **Source-Interface Vlan** drop-down list.

Step 14 Click **Update & Apply to Device**.

Configuring DHCP Option 82 Globally Through Different SVIs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip dhcp-relay source-interface vlan** *vlan-id* **Example:** `Device(config)# ip dhcp-relay source-interface vlan 74`	Sets global source interface for relayed messages.

Configuring DHCP Option 82 Format

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-name* **Example:** `Device(config)# wireless profile policy pp3`	Enables configuration for the specified profile policy.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Shuts down the profile policy.
Step 4	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan 72`	Assigns the profile policy to a VLAN.
Step 5	**session-timeout** *value-btwn-20-86400* **Example:** `Device(config-wireless-policy)# session-timeout 300`	(Optional) Sets the session timeout value in seconds. The range is between 20-86400.
Step 6	**idle-timeout** *value-btwn-15-100000* **Example:** `Device(config-wireless-policy)# idle-timeout 15`	(Optional) Sets the idle timeout value in seconds. The range is between 15-100000.
Step 7	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Enables central switching.
Step 8	**ipv4 dhcp opt82** **Example:** `Device(config-wireless-policy)# ipv4 dhcp opt82`	Enables DHCP Option 82 for the wireless clients.
Step 9	**ipv4 dhcp opt82 ascii** **Example:**	(Optional) Enables ASCII on the DHCP Option 82 feature.

	Command or Action	Purpose
	`Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	
Step 10	**ipv4 dhcp opt82 rid** **Example:** `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	(Optional) Supports the addition of Cisco 2 byte Remote ID (RID) for the DHCP Option 82 feature.
Step 11	**ipv4 dhcp opt82 format** {**ap_ethmac**|**ap_location**|**apmac**|**apname**|**policy_tag**|**ssid**|**vlan_id**} **Example:** `Device(config-wireless-policy)# ipv4 dhcp opt82 format apmac`	Enables DHCP Option 82 on the corresponding AP. For information on the various options available with the command, see Cisco Catalyst 9800 Series Wireless Controller Command Reference.
Step 12	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the profile policy.

Configuring DHCP Option82 Through a VLAN Interface

Configuring DHCP Option 82 Through Option-Insert Command (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 72`	Configures a VLAN ID.
Step 3	**ip dhcp relay information option-insert** **Example:** `Device(config-if)# ip dhcp relay information option-insert`	Inserts relay information in BOOTREQUEST.
Step 4	**ip address** *ip-address* **Example:**	Configures the IP address for the interface.

	Command or Action	Purpose
	`Device(config-if)# ip address 9.3.72.38 255.255.255.0`	
Step 5	**ip helper-address** *ip-address* **Example:** `Device(config-if)# ip helper-address 9.3.72.1`	Configures the destination address for UDP broadcasts.
Step 6	**[no] mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables the MOP for an interface.
Step 7	**[no] mop sysid** **Example:** `Device(config-apgroup)# [no] mop sysid`	Disables the task of sending MOP periodic system ID messages.

Configuring DHCP Option 82 Through the server-ID-override Command (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip dhcp compatibility suboption server-override cisco** **Example:** `Device(config)# ip dhcp compatibility suboption server-override cisco`	Configures the server-id override suboption to an RFC or Cisco specific value.
Step 3	**ip dhcp compatibility suboption link-selection cisco** **Example:** `Device(config)# ip dhcp compatibility suboption link-selection cisco`	Configures the link-selection suboption to an RFC or Cisco specific value.
Step 4	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 72`	Configures a VLAN ID.
Step 5	**ip dhcp relay information option server-id-override** **Example:**	Inserts the server id override and link selection suboptions.

	Command or Action	Purpose
	`Device(config-if)# ip dhcp relay information option server-id-override`	
Step 6	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 9.3.72.38 255.255.255.0`	Configures the IP address for the interface.
Step 7	**ip helper-address** *ip-address* **Example:** `Device(config-if)# ip helper-address 9.3.72.1`	Configures the destination address for UDP broadcasts.
Step 8	**[no] mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables MOP for an interface.
Step 9	**[no] mop sysid** **Example:** `Device(config-if)# [no] mop sysid`	Disables the task of sending MOP periodic system ID messages.

Configuring DHCP Option 82 Through a Subscriber-ID (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 72`	Configures a VLAN ID.
Step 3	**ip dhcp relay information option subscriber-id** *subscriber-id* **Example:** `Device(config-if)# ip dhcp relay information option subscriber-id test10`	Inserts the subscriber identifier suboption.
Step 4	**ip address** *ip-address* **Example:**	Configures the IP address for the interface.

	Command or Action	Purpose
	`Device(config-if)# ip address 9.3.72.38 255.255.255.0`	
Step 5	**ip helper-address** *ip-address* **Example:** `Device(config-if)# ip helper-address 9.3.72.1`	Configures the destination address for UDP broadcasts.
Step 6	**[no] mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables MOP for an interface.
Step 7	**[no] mop sysid** **Example:** `Device(config-apgroup)# [no] mop sysid`	Disables the task of sending MOP periodic system ID messages.

Configuring DHCP Option 82 Through server-ID-override and subscriber-ID Commands (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 72`	Configures a VLAN ID.
Step 3	**ip dhcp relay information option server-id-override** **Example:** `Device(config-if)# ip dhcp relay information option server-id-override`	Inserts server ID override and link selection suboptions.
Step 4	**ip dhcp relay information option subscriber-id** *subscriber-id* **Example:** `Device(config-if)# ip dhcp relay information option subscriber-id test10`	Inserts the subscriber identifier suboption.

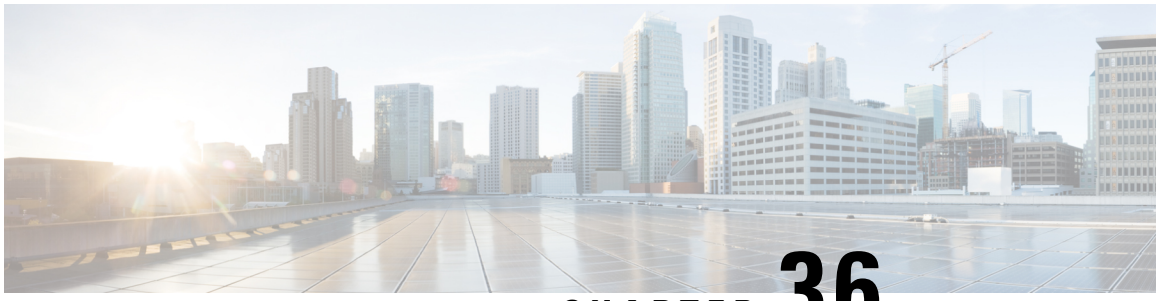
	Command or Action	Purpose
Step 5	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 9.3.72.38 255.255.255.0`	Configures the IP address for the interface.
Step 6	**ip helper-address** *ip-address* **Example:** `Device(config-if)# ip helper-address 9.3.72.1`	Configures the destination address for UDP broadcasts.
Step 7	**[no] mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables the MOP for an interface.
Step 8	**[no] mop sysid** **Example:** `Device(config-apgroup)# [no] mop sysid`	Disables the task of sending MOP periodic system ID messages.

Configuring DHCP Option 82 Through Different SVIs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 72`	Configures a VLAN ID.
Step 3	**ip dhcp relay source-interface vlan** *vlan-id* **Example:** `Device(config-if)# ip dhcp relay source-interface vlan 74`	Configures a source interface for relayed messages on a VLAN ID.
Step 4	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 9.3.72.38 255.255.255.0`	Configures the IP address for the interface.

	Command or Action	Purpose
Step 5	**ip helper-address** *ip-address* **Example:** `Device(config-if)# ip helper-address 9.3.72.1`	Configure the destination address for UDP broadcasts.
Step 6	**[no] mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables the MOP for an interface.
Step 7	**[no] mop sysid** **Example:** `Device(config-apgroup)# [no] mop sysid`	Disables the task of sending MOP periodic system ID messages.



CHAPTER 36

RADIUS Realm

- Information About RADIUS Realm, on page 285
- Enabling RADIUS Realm, on page 286
- Configuring Realm to Match the RADIUS Server for Authentication and Accounting, on page 286
- Configuring the AAA Policy for a WLAN, on page 287
- Verifying the RADIUS-Realm Configuration, on page 289

Information About RADIUS Realm

The RADIUS Realm feature is associated with the domain of the user. Using this feature, a client can choose the RADIUS server through which authentication and accounting is to be processed.

When mobile clients are associated with a WLAN, RADIUS realm is received as a part of Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA) identity response request in the authentication request packet. The Network Access Identifier (NAI) format (EAP-AKA) for WLAN can be specified as *username@domain.com*. The realm in the NAI format is represented after the @ symbol, which is specified as domain.com. If vendor-specific attributes are added as *test*, the NAI format is represented as test@domain.com.

The RADIUS Realm feature can be enabled and disabled on a WLAN. If Realm is enabled on a WLAN, the corresponding user should send the username in the NAI format. The controller sends the authentication request to the AAA server only when the realm, which is in the NAI format and is received from the client, is compiled as per the given standards. Apart from authentication, accounting requests are also required to be sent to the AAA server based on realm filtering.

Realm Support on a WLAN

Each WLAN is configured to support NAI realms. After 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. If the client does not send a username with the realm, the default RADIUS server that is configured on the WLAN is used for authentication. If the realm that is received from the client does not match the configured realms on the WLAN, the client is deauthenticated and dropped.

If the RADIUS Realm feature is not enabled on a WLAN, the username that is received as part of the EAP identity request is directly used as the username and the configured RADIUS server is used for authentication and accounting. By default, the RADIUS Realm feature is disabled on WLANs.

- **Realm Match for Authentication**: In dot1x with EAP methods (similar to EAP AKA), the username is received as part of an EAP identity response. A realm is derived from the username and are matched

with the realms that are already configured in the corresponding RADIUS authentication server. If there is a match, the authentication requests are forwarded to the RADIUS server. If there is a mismatch, the client is deauthenticated.

- **Realm Match for Accounting**: A client's username is received through an access-accept message. When accounting messages are triggered, the realm is derived from the corresponding client's username and compared with the accounting realms configured on the RADIUS accounting server. If there is a match, accounting requests are forwarded to the RADIUS server. If there is a mismatch, accounting requests are dropped.

Enabling RADIUS Realm

Follow the procedure given below to enable RADIUS realm:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless aaa policy** *aaa-policy* **Example:** `Device(config)# wireless aaa policy policy-1`	Creates a new AAA policy.
Step 3	**aaa-realm enable** **Example:** `Device(config-aaa-policy)# aaa-realm enable`	Enables AAA RADIUS realm selection. **Note** Use the **no aaa-realm enable** or the **default aaa-realm enable** command to disable the RADIUS realm.

Configuring Realm to Match the RADIUS Server for Authentication and Accounting

Follow the procedure given below to configure the realm to match the RADIUS server for authentication and accounting:

Procedure

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

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Creates a AAA authentication model.
Step 3	**aaa authorization network default group** *radius-server-group* **Example:** `Device(config)# aaa authorization network default group aaa_group_name`	Sets the authorization method.
Step 4	**aaa authentication dot1x** *realm* **group** *radius-server-group* **Example:** `Device(config)# aaa authentication dot1x cisco.com group cisco1`	Indicates that dot1x must use the realm group RADIUS server.
Step 5	**aaa authentication login** *realm* **group** *radius-server-group* **Example:** `Device(config)# aaa authentication login cisco.com group cisco1`	Defines the authentication method at login.
Step 6	**aaa accounting identity** *realm* **start-stop group** *radius-server-group* **Example:** `Device(config)# aaa accounting identity cisco.com start-stop group cisco1`	Enables accounting to send a start-record accounting notice when a client is authorized, and a stop-record at the end.

Configuring the AAA Policy for a WLAN

Follow the procedure given below to configure the AAA policy for a WLAN:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless aaa policy** *aaa-policy-name* **Example:** `Device(config)# wireless aaa policy aaa-policy-1`	Creates a new AAA policy for wireless.

	Command or Action	Purpose
Step 3	**aaa-realm enable** **Example:** `Device(config-aaa-policy)# aaa-realm enable`	Enables AAA RADIUS server selection by realm.
Step 4	**exit** **Example:** `Device(config-aaa-policy)# exit`	Returns to global configuration mode.
Step 5	**wireless profile policy** *wlan-policy-profile* **Example:** `Device(config)# wireless profile policy wlan-policy-a`	Configures a WLAN policy profile.
Step 6	**aaa-policy** *aaa-policy* **Example:** `Device(config-wireless-policy)# aaa-policy aaa-policy-1`	Maps the AAA policy.
Step 7	**accounting-list** *acct-config-realm* **Example:** `Device(config-wireless-policy)# accounting-list cisco.com`	Sets the accounting list.
Step 8	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.
Step 9	**wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# wlan wlan2 14 wlan-aaa`	Configures a WLAN.
Step 10	**security dot1x authentication-list** *auth-list-realm* **Example:** `Device(config-wlan)# security dot1x authentication-list cisco.com`	Enables the security authentication list for IEEE 802.1x.
Step 11	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.
Step 12	**wireless tag policy** *policy* **Example:** `Device(config)# wireless tag policy tag-policy-1`	Configures a policy tag.

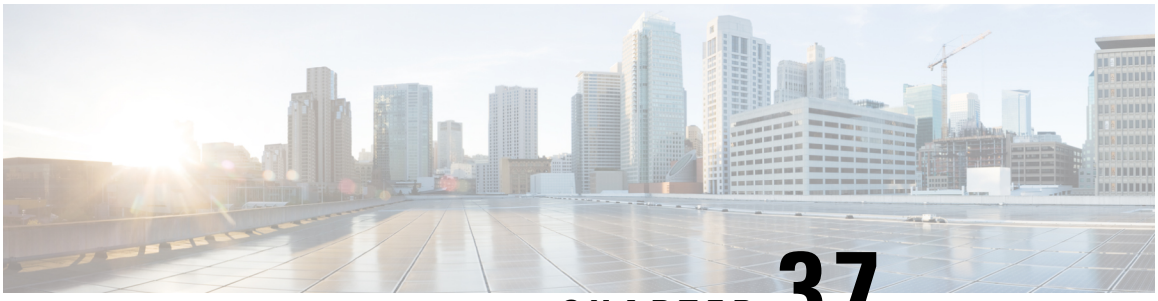
	Command or Action	Purpose
Step 13	**wlan** *wlan-name* **policy** *policy-profile* **Example:** `Device(config-policy-tag)# wlan Abc-wlan policy wlan-policy-a`	Maps a policy profile to the WLAN.
Step 14	**exit** **Example:** `Device(config-policy-tag)# exit`	Returns to global configuration mode.

Verifying the RADIUS-Realm Configuration

Use the following command to verify the RADIUS-realm configuration:

```
Device# show wireless client mac-address 14bd.61f3.6a24 detail


Client MAC Address : 14bd.61f3.6a24
Client IPv4 Address : 9.4.113.103
Client IPv6 Addresses : fe80::286e:9fe0:7fa6:8f4
Client Username : sacthoma@cisco.com
AP MAC Address : 4c77.6d79.5a00
AP Name: AP4c77.6d53.20ec
AP slot : 1
Client State : Associated
Policy Profile : name-policy-profile
Flex Profile : N/A
Wireless LAN Id : 3
Wireless LAN Name: ha_realm_WLAN_WPA2_AES_DOT1X
BSSID : 4c77.6d79.5a0f
Connected For : 26 seconds
Protocol : 802.11ac
Channel : 44
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Re-Authentication Timeout : 1800 sec (Remaining time: 1775 sec)
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Power Save : OFF
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 06/12/2018 19:52:35 IST
Policy Manager State: Run
```

```
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 25 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : PEAP
VLAN : 113
Multicast VLAN : 0
Access VLAN : 113
Anchor VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface        : capwap_9040000f
  IIF ID           : 0x9040000F
  Authorized       : TRUE
  Session timeout  : 1800
  Common Session ID: 097704090000000DF4607B3B
  Acct Session ID  : 0x00000fa2
  Aaa Server Details
  Server IP        : 9.4.23.50
  Auth Method Status List
       Method : Dot1x
              SM State         : AUTHENTICATED
              SM Bend State    : IDLE
  Local Policies:
       Service Template : wlan_svc_name-policy-profile_local (priority 254)
              Absolute-Timer   : 1800
              VLAN             : 113
  Server Policies:
  Resultant Policies:
              VLAN             : 113
              Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Central
FlexConnect Dhcp Status : Central
FlexConnect Authentication : Central
FlexConnect Central Association : No
.
.
.
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
```



CHAPTER 37

Cisco StadiumVision

- Cisco StadiumVision Overview, on page 291
- Configure Parameters for Cisco StadiumVision (GUI), on page 292
- Configure Parameters for Cisco StadiumVision (CLI), on page 292
- Verify StadiumVision Configurations, on page 293

Cisco StadiumVision Overview

Cisco StadiumVision solution is a proven, end-to-end, high-definition IPTV solution that provides advanced digital content management and delivery that can transform the look and feel of venues. It is built on top of the Cisco Connected Stadium solution and centrally-managed through the StadiumVision Director. Cisco StadiumVision solution enables the integration and automated delivery of customised and dynamic content from multiple sources to different areas of the stadium in high definition quality.

This technology allows you to replay certain exciting and critical moments of a game on Wi-Fi capable devices.

To enable Cisco StadiumVision solution on the controller , you need to configure these parameters:

1. On Wireless Controller :
    - Multicast Data Rate
    - RX Sensitivity SOP
    - Multicast Buffer
2. CAPWAP
3. AP Radio Driver and Firmware:
    - Multicast Data Rate
    - RX Sensitivity SOP
    - Multicast Buffer

Configure Parameters for Cisco StadiumVision (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Advanced**.

Step 2 Click the **High Density** tab.

Step 3 In the **Multicast Data Rate** section, set the data rate for 5 GHz radio or 2.4 GHz radio using the drop-down lists.

Step 4 Click **Apply** .

Configure Parameters for Cisco StadiumVision (CLI)

Note Multicast buffer and data rate configurations are supported for all AP models.

Procedure

	Command or Action	Purpose
Step 1	**wlan** *wlan-name wlan-id* **Example:** `Device(config)# wlan wlan1 10`	Configures a WLAN.
Step 2	**multicast buffer** *multicast-buffer-number* **Example:** `Device(config-wlan)# multicast buffer 45`	Configures enhanced multicast buffer size between 30 (default) and 60 on a WLAN. **Note** You can enable only two out of the possible 512 WLANs configured on Controller embedded wireless controller for enhanced multicast buffers.
Step 3	**ap dot11 [5ghz| 24ghz] multicast data-rate** *rate* **Example:** `Device(config)# ap dot11 [5ghz| 24ghz] rx-sop threshold custom -70`	Configures the radio receive sensitivity SOP threshold between -60 to -85 dB, which can also be configured as predefined auto, low, high, medium values specific to 5ghz or 24ghz bands. By default, the configuration is disabled and it's value is set to *auto*. If the RxSOP value of *auto* (0) is pushed, then the AP considers the value burnt-in during manufacturing.

Verify StadiumVision Configurations

- **show ap rf-profile name** *rf-name* **detail**
- **show ap dot11 5ghz** *high-density*

Rx SOP

```
Device#show ap rf-profile name Typical_Client_Density_rf_5gh detail | i SOP
Rx SOP Threshold                 : auto
```

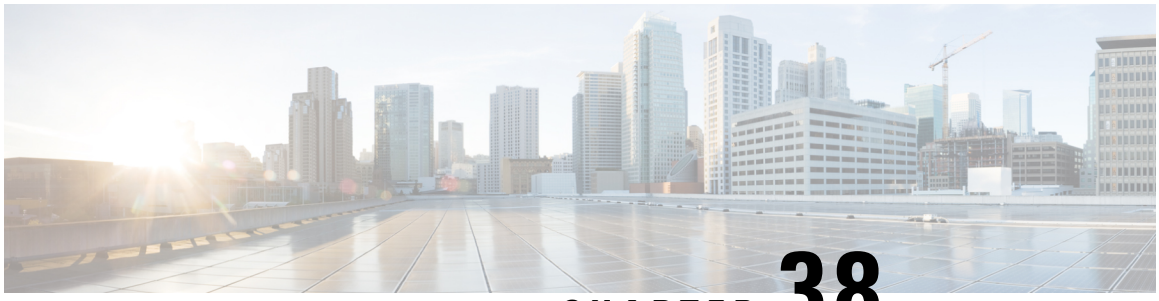
Multicast Buffer

```
Device#show wlan id 1 | sec Buffer
Multicast Buffer                              : Enabled
Multicast Buffer Size                         : 45

Device#

Device#sh wlan name vwlc-OpenAuth | inc Buffer
Multicast Buffer                              : Enabled
Multicast Buffer Size                         : 45
Device#
```

Multicast Data Rate

```
Device#sh ap dot11 24ghz high-density
AP Name                          Mac Address            Slot         Rxsop
Threshold Type Value (dbm)       Multicast Data Rate(Mbps)
-------------------------------------------------------------------------------------
-------------------------------------------------
test-1800-AP                      aaaa.bbbb.cccc            0         auto
        0                         54
AP4001.7AB2.BEB6                  aaab.bbbb.cccc            2         auto
        0                         54
AP70DF.2FA2.72EE                  aaac.bbbb.cccc            0         auto
        0                         0

Device#show ap dot11 5ghz high-density
AP Name                          Mac Address            Slot         Rxsop
Threshold Type Value (dbm)       Multicast Data Rate(Mbps)
-------------------------------------------------------------------------------------
-------------------------------------------------
Saji-1800-AP                      aaab.bbbb.cccc            1         auto
        0                         12
Saji-2802I-AP                     aaab.bbbb.cccc            0         custom
         -82                       12
Saji-2802I-AP                     aaac.bbbb.cccc            1         custom
         -82                       12
AP4001.7AB2.BEB6                  aaad.bbbb.cccc            0         custom
         -82                       12
AP4001.7AB2.BEB6                  aaae.bbbb.cccc            1         custom
         -82                       0
AP500F.8086.8B56                  aaaf.bbbb.cccc            0         custom
         -82                       12
AP500F.8086.8B56                  aaag.bbb.cccc            1         custom
```

```
         -82                          12
AP70DF.2FA2.72EE                  aaah.bbbb.cccc            1         auto
        0                         0

Device#
Device(config)#ap dot11 5ghz rf-profile test_5ghz_rf
Device(config-rf-profile)#high-density multicast data-rate RATE_18M


Device#  show ap rf-profile name test_5ghz_rf detail | inc Multicast
Multicast Data Rate               : 18 Mbps
Device#
```



CHAPTER 38

Persistent SSID Broadcast

- Persistent SSID Broadcast, on page 295
- Configuring Persistent SSID Broadcast, on page 295
- Verifying Persistent SSID Broadcast, on page 296

Persistent SSID Broadcast

Access Points within a mesh network work as Root Access Points (RAP) or Mesh Access Points (MAP). RAPs have wired connection to the controller and MAPs have wireless connection to the controller . This feature is applicable only to the Cisco Aironet 1542 Access Points in the Flex+Bridge mode.

This feature is about the Root Access Points (RAPs) and Mesh Access Points (MAPs) broadcasting the SSID even when the WAN connectivity is down. This is required in order to isolate the responsibility; whether the fault is with backhaul or with the access wireless network, since there can be different operators owning each part of the network.

RAPs and MAPs broadcast SSID while in standalone mode, as long as the default gateway is reachable.

Also refer Mesh Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers.

Configuring Persistent SSID Broadcast

Procedure

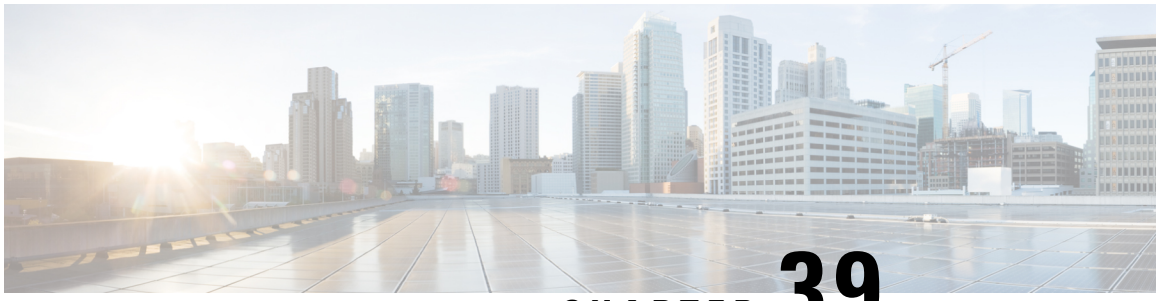
	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures the AP profile.

	Command or Action	Purpose
Step 3	**[no]ssid broadcast persistent** **Example:** `Device(config-ap-profile)# [no] ssid broadcast persistent`	The **ssid broadcast** command configures the SSID broadcast mode. The **persistent** keyword enables a persistent SSID broadcast, where the associated APs will re-join. Use the **[no]** form of the command to disable the feature. **Note** Enabling or disabling this feature causes the AP to re-join.

Verifying Persistent SSID Broadcast

To view the configuration of all Cisco APs, use the following **show** command:

```
Device#show ap config general
Cisco AP Name   : AP4C77.6DF2.D598
================================================
Office Extend Mode                              : Disabled
Persistent SSID Broadcast                       : Enabled
Remote AP Debug                                 : Disabled
```



CHAPTER 39

Network Monitoring

- Network Monitoring , on page 297
- Status Information Received Synchronously - Configuration Examples, on page 297
- Alarm and Event Information Received Asynchronously - Configuration Examples, on page 299

Network Monitoring

The mechanism that is used to transfer data to the third-party system is NETCONF/YANG. YANG can be used with the Network Configuration Protocol (NETCONF) to provide the desired solution of automated and programmable network operations.

You can contact the API or Developer Support for NETCONF/YANG features using the following link:

https://developer.cisco.com/site/support/#

The two types of information provided are:

- Status information received synchronously - NETCONF is the management interface used for status information, which allows to publish the operational state of the device, including the controller .
- Alarm and event information sent asynchronously - NETCONF/YANG push is the solution used for alarm and event information, which provides the mechanism to send NETCONF notifications subscribed for.

Status Information Received Synchronously - Configuration Examples

NETCONF/YANG interface is used to accomplish customer requests.

The prerequisite configuration for Status Information and Alarm and Event Information is to enable NETCONF server on the controller by using the following command:

netconf-yang

The above command not only enables notifications, but also allows for configuration and operation access (OAM) via Netconf/Yang. For more information on Netconf/Yang, see the *NETCONF Protocol* chapter of the Programmability Configuration Guide at: https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/products-installation-and-configuration-guides-list.html

In the Status Information Received Synchronously type, the following information is exported though NETCONF:

- Name of the village
- APs in each village
- Status of each AP
- Number of clients currently connected and logged on in each village and each AP

All the data for the items listed above is already available as the controller operational data exported through NETCONF. The examples below explain where the data items listed are available.

The following command is used in the controller :

```
wireless tag site village_name_1
```

The site tags can be retrieved by NETCONF using the **get-config** operation.

Example output for **Name of the Village**:

```
<site-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-site-cfg">
[...]
<site-tag-configs>
  <site-tag-config>
    <site-tag-name>village_name_1</site-tag-name>
    <description>custom user site tag for a village</description>
  </site-tag-config>
[...]
</site-tag-configs>
```

The controller 's operational data contains all the connected (joined) APs and lists their site tags. The example output displays the detailed information about the APs and the site tags. The following example displays the relevant fields and the corresponding controller show commands:

Example output of **Access Point per Village**:

```
<data>
    <access-point-oper-data
xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-access-point-oper">
    [...]
      <radio-oper-data>
        <wtp-mac>00:1b:0c:00:02:00</wtp-mac>   #show ap dot11 {24ghz|5ghz} summary "MAC
Address"
        <radio-slot-id>0</radio-slot-id>       #show ap dot11 {24ghz|5ghz} summary "Slot"
        <ap-mac>00:1b:0c:00:02:00</ap-mac>
        <slot-id>0</slot-id>
        <radio-type>1</radio-type>             # 1 - 2.4GHz, 2 - 5GHz
        <admin-state>enabled</admin-state>     #show ap dot11 {24ghz|5ghz} summary "Admin
State"
        <oper-state>radio-up</oper-state>      #show ap dot11 {24ghz|5ghz} summary "Oper
State"
    [...]
[...]
      <capwap-data>
        <wtp-mac>00:1b:0c:00:02:00</wtp-mac>               #show ap summary  "Radio MAC"
        <ap-operation-state>registered</ap-operation-state> #show ap summary  "State"
        <ip-addr>10.102.140.10</ip-addr>                   #show ap summary  "IP Address"
        [...]
        <admin-state>1</admin-state>              #show ap status   "Status", 1 - Enabled,
 2 - Disabled
        <location>default-location </location>    #show ap summary  "Location"
        <country-code>CH </country-code>
```

```
       <name>AP_A-1</name>                          #show ap summary  "AP Name"
 [...]
       <tag-info>
         [...]
         <site-tag>
          <site-tag-name>village_name_1</site-tag-name> #show ap name AP_A-1 config general
 "Site Tag Name"
           [...]
         </site-tag>
[...]
```

The operational data of the controller contains all the connected wireless clients information, which includes detailed client device information, such as the MAC address, IP address, State and the AP name.

Example output of the **Number of clients currently online and logged in each village and each AP**:

```
<data>
    <client-oper-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-client-oper">
      <common-oper-data>
        <client-mac>00:00:1a:04:00:02</client-mac>     #show wireless client summary  "MAC
 Address"
        <ap-name>AP_A-1</ap-name>                      #show wireless client summary  "AP
Name"
        [...]
       <co-state>client-status-run</co-state>        #show wireless client summary  "State"
```

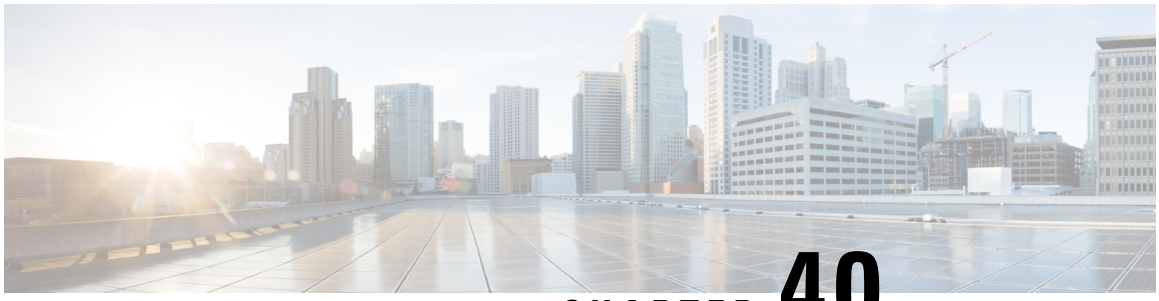
Alarm and Event Information Received Asynchronously - Configuration Examples

The push functionality for the alarm and event information is fulfilled with on-change notifications through NETCONF dynamic subscriptions, with XML encoding.

Example output of **AP Up/Down Events - Subscription**

```
Request:

<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="urn:uuid:b0c581c9-ff5a-4352-9e64-7f2ce1ec603a"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <establish-subscription xmlns="urn:ietf:params:xml:ns:yang:ietf-event-notifications"
   xmlns:yp="urn:ietf:params:xml:ns:yang:ietf-yang-push">
  <stream>yp:yang-push</stream>
  <yp:xpath-filter>/access-point-oper-data/capwap-data/ap-operation-state</yp:xpath-filter>

  <yp:dampening-period>0</yp:dampening-period>
 </establish-subscription>
</rpc>

Reply:

<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="urn:uuid:673b42b2-e988-4e20-a6c3-0679c08e6114"><subscription-result
xmlns='urn:ietf:params:xml:ns:yang:ietf-event-notifications'
xmlns:notif-bis="urn:ietf:params:xml:ns:yang:ietf-event-notifications">notif-bis:ok</subscription-result>
<subscription-id
```

```
xmlns='urn:ietf:params:xml:ns:yang:ietf-event-notifications'>2147483652</subscription-id>
</rpc-reply>
-->>
(Default Callback)
Event time      : 2018-03-09 15:08:21.880000+00:00
Subscription Id : 2147483651
Type            : 2
Data            :
<datastore-changes-xml xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-push">
  <yang-patch xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-patch">
    <patch-id>null</patch-id>
    <edit>
      <edit-id>edit1</edit-id>
      <operation>merge</operation>
      <target>/access-point-oper-data/capwap-data</target>
      <value>
       <capwap-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-access-point-oper">

          <ap-operation-state>registered</ap-operation-state>
          <wtp-mac>00ab11006600</wtp-mac>
        </capwap-data>
      </value>
    </edit>
  </yang-patch>
</datastore-changes-xml>
<<--
```



CHAPTER 40

Creating a Lobby Ambassador Account

- Information About Lobby Ambassador Account, on page 301
- Creating a Lobby Ambassador User Account (GUI), on page 301
- Creating a Lobby Ambassador Account (CLI), on page 303

Information About Lobby Ambassador Account

A global administrator can create a lobby ambassador (lobby admin) user for creating guest users.

While creating a guest user, a lobby ambassador can create and delete a guest user, besides setting the following parameters for a guest user:

- Password
- Lifetime of the guest user
- Guest role profiles (Quality-of-Service profiles that should be applied on a guest using the AAA attribute list.

You must ensure that the RADIUS server must be configured with Cisco-AV-pair privilege level with a value greater than zero.

Note You can create a lobby admin from a RADIUS or TACACS server, instead of creating one locally.

Only the admin can create WLAN and web authentication policies. The admin can also create an AAA attribute list, which the lobby admin can use to map to the corresponding guest user.

After an upgrade to Cisco Catalyst 9800 Controller Software release 17.2.x , you must clear the browser cache data to view the lobby admin GUI correctly.

Creating a Lobby Ambassador User Account (GUI)

You can configure administrator or lobby ambassador usernames and passwords to prevent unauthorized users from reconfiguring the controller and viewing configuration information.

Creating a User Account

Procedure

Step 1 From the home page, choose **Administration** > **User Administration**.

Step 2 Click **Add**.

Step 3 In the **User Name** field, enter a user name for the new account.

Step 4 From the **Policy** drop-down list, choose the policy that you want to associate with the user.

Step 5 From the **Privilege** drop-down list, choose the privilege level that you want to associate with the user by clicking the user privilege icon. The following are the options:

- **Go to Basic Mode**
- **Go to Advanced Mode**

Go to Basic Mode: This privilege level defines the commands that users can enter using the CLI after they have logged into the device. Privilege 1 allows access in user EXEC mode and privilege 15 allows access in Privileged EXEC mode.

Go to Advanced Mode:

Admin: Users with Privilege 15 can execute all the **show**, **config**, and **exec** commands on the device. These users will have access to all the sections of the GUI.

Read Only: Users with Privileges 1 to 14 are considered read-only users. The default privilege is 1 if a user is created using the GUI. These users will have access only to the Dashboard and the Monitoring sections.

No Access: Users with Privilege 0 can log in to the device through Telnet or SSH and access the CLI. However, they cannot access the GUI.

Lobby Admin: Users who can create only guest user accounts. While creating a guest user, a lobby ambassador can create and delete a guest user, besides setting the following parameters for a guest user:

- Password
- Lifetime of the guest user
- Guest role profiles (auality-of-service) profiles that should be applied on a guest using the AAA attribute list.

Step 6 In the **Password** field, enter a password for the new account.

Step 7 In the **Confirm Password** field, enter the same password again to reconfirm.

Step 8 Click **Apply to Device**.

Logging In Using the Lobby Account

Note Execute the following commands before logging in using the lobby credentials:

aaa new-model

aaa authorization exec default local

ip http authentication aaa

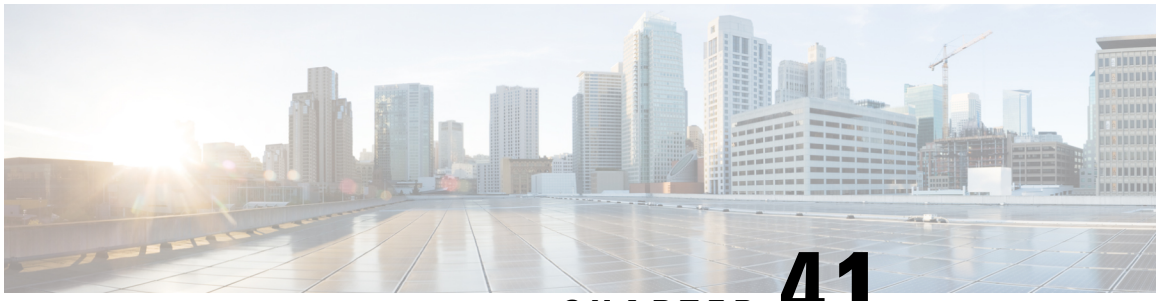
Logout from the Administrator account and login using the lobby credentials.

You get to view the **Guest User** page.

Creating a Lobby Ambassador Account (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**user-name** *user-name* **Example:** `Device(config)# user-name example-user`	Creates a user account.
Step 3	**type lobby-admin** **Example:** `Device(config-user-name)# type lobby-admin`	Specifies the account type as lobby admin.
Step 4	**password 0** *password* **Example:** `Device(config-user-name)# password 0 example-password`	Creates a password for the lobby administrator account.
Step 5	**exit** **Example:** `Device(config-user-name)# exit`	Returns to global configuration mode.



CHAPTER 41

Guest User Accounts

- Information About Creating Guest User Accounts, on page 305
- Creating a Guest User Account (GUI), on page 305
- Creating a Guest User Account (CLI), on page 306
- Verifying Guest User Account, on page 307
- Assigning Username to Guest Users in a WLAN (CLI), on page 308

Information About Creating Guest User 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 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.

You can associate user name with WLAN profile name to restrict guest users in a specific WLAN.

Prerequisites for Guest Users

- Guest users are created by administrator or lobby ambassador.
- Guest user should not have device access either through telnet/ssh or WebUI.
- Guest user should be role-based.
- Guest user should be able to connect to the network and access internet.

Creating a Guest User Account (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Guest User**.

Step 2 On the **Guest User** page, click **Add**.

Step 3 Enter a user name, password, and description for the new account. Check the **Generate password** check box to automatically generate a password.

Step 4 Enter the number of simultaneous user logins. Valid values range between 0 to 64.

Enter 0 for unlimited users.

Step 5 In the **Lifetime** section, choose the number of years, months, days, hours, and minutes.

Step 6 Click **Save & Apply to Device**.

Creating a Guest User Account (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**user-name** *guest-user-name* **Example:** `Device(config)# user-name guest`	Creates a guest user account.
Step 3	**type network-user description** *description* **guest-user max-login-limit** *number of simultaneous logins* **lifetime year** *yy* **month** *mm* **day** *day* **hour** *hour* **minute** *minute* **second** *second* **Example:** `Device(config-user-name)# type network-user description sample-description guest-user max-login-limit 3 lifetime 1 years 0 months 0 days 0 hours 0 mins 0 secs`	Specifies the account type as guest user account.
Step 4	**password 0** *password* **Example:** `Device(config-user-name)# password 0 guest`	Creates a password for the guest user account.
Step 5	**aaa attribute list** *aaa-attribute-list-name* **Example:** `Device(config-user-name)# aaa attribute list aaa-attribute-list-name`	Creates a AAA attribute list to apply QoS profiles on the guest user account.

	Command or Action	Purpose

Step 6	**exit**
	Example:
	`Device(config-user-name)# exit`
		Returns to global configuration mode.
		Note If the lobby admin is local, enter the following command:
		`aaa authentication login default local`
		If the lobby admin is a remote user, enter the following commands:
		`aaa authentication login default group radius/tacacs`
		`aaa remote username <remote-lobby-admin-name>`
		In case of local or remote lobby, enter the following command to map the authorization policies:
		`aaa authorization exec default local`

Verifying Guest User Account

To verify all the guest user accounts, use the following command:

```
Device# show aaa local guest_user all
User-Name           : new4
     Type                :  GUEST USER
     Password            : *
     Is_passwd_encrypted : No
     Attribute-List      : Not-Configured
     Viewname            : Not-Configured
     Lobby Admin Name    : NEW_LOBBY_ADMIN
     Max Login Limit     : 0
     Description         : guest
     Start-Time          : 07:56:39 IST Jan 25 2019
     Lifetime            : 1 years 0 months 0 days 0 hours 0 mins 0 secs
     Expiry-Time         : 07:56:39 IST Jan 20 2020 Remaining Lifetime  : 0 years 11 months
 29 days 22 hours 52 mins 49 secs
```

To verify a specific guest user account, use the following command:

```
Device# show aaa local guest_user new_guest3
User-Name           : new_guest3
 Type                :  GUEST USER
 Password            : *
 Is_passwd_encrypted : No
 Attribute-List      : Not-Configured
 Viewname            : Not-Configured
 Lobby Admin Name    : INVALID_ADMIN
 Max Login Limit     : 9
 Description         : new
 Start-Time          : 04:39:01 IST Feb 4 2019
 Lifetime            : 1 years 0 months 0 days 0 hours 0 mins 0 secs
```

```
Expiry-Time         : 04:39:01 IST Jan 30 2020
Remaining Lifetime  : 0 years 11 months 11 days 21 hours 16 mins 34 secs
```

Assigning Username to Guest Users in a WLAN (CLI)

Before you begin

- If wlan-profile-name is configured for a user, guest user authentication is allowed only from that WLAN.
- If wlan-profile-name is not configured for a user, guest user authentication is allowed on any WLAN.
- To work in a connected mode, you need to configure AAA policy override under both SSID policies before assigning a username to a guest user on a WLAN.

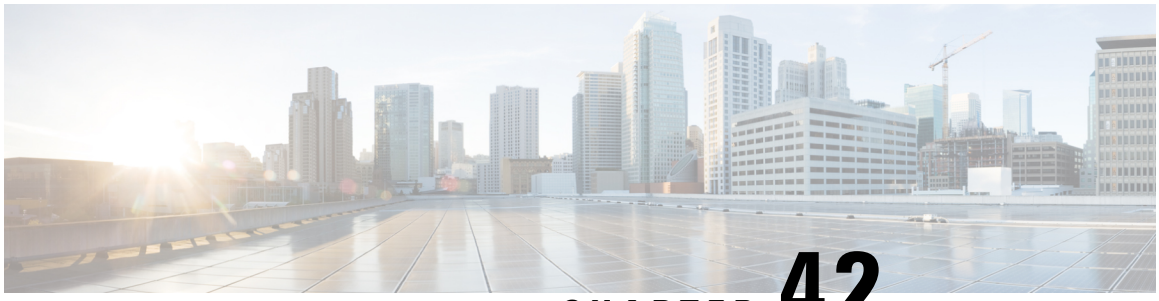
Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters configuration mode.
Step 2	**username user_name mac wlan-profile-name profile_name** **Example:** `Device(config)# username user_name mac wlan-profile-name profile_name`	Assigns a username to the WLAN profile. **Note** The wlan-profile-name per user is applicable for MAC type users.
Step 3	**show aaa local guest_user new_guest3** **Example:** `Device# show aaa local guest_user new_guest3`	(Optional) Displays the values of the WLAN profile.
Step 4	**end** **Example:** `Device# end`	Returns to privileged EXEC mode.

PART V

System Management

- Network Mobility Services Protocol, on page 311
- Application Visibility and Control, on page 325
- Cisco Hyperlocation, on page 347
- BLE Beacons in CiscoWave 2 Access Points, on page 359
- Cisco Connected Mobile Experiences Cloud, on page 363
- EDCA Parameters, on page 367
- 802.11 parameters and Band Selection, on page 371
- Predownloading an Image to an Access Point, on page 391
- Efficient Image Upgrade, on page 395
- N+1 Hitless Rolling AP Upgrade, on page 401
- Wireless Sub-Package for Switch, on page 405
- NBAR Protocol Discovery, on page 411
- NBAR Dynamic Protocol Pack Upgrade, on page 413
- Conditional Debug, Radioactive Tracing, and Packet Tracing, on page 415
- Aggressive Client Load Balancing, on page 427
- Accounting Identity List, on page 431
- Wireless Multicast, on page 435
- Map-Server Per-Site Support, on page 455
- Volume Metering, on page 463
- Enabling Syslog Messages in Access Points and Controller for Syslog Server, on page 465
- Software Maintenance Upgrade, on page 475



CHAPTER 42

Network Mobility Services Protocol

- Information About Network Mobility Services Protocol, on page 311
- Radioactive Tracing for NMSP, on page 312
- Enabling NMSP on Premises Services, on page 312
- Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues , on page 313
- Modifying the NMSP Notification Threshold for Clients, RFID Tags, and Rogues, on page 313
- Configuring NMSP Strong Cipher, on page 314
- Verifying NMSP Settings, on page 314
- Examples: NMSP Settings Configuration, on page 317
- NMSP by AP Groups with Subscription List from CMX, on page 317
- Verifying NMSP by AP Groups with Subscription List from CMX, on page 317
- Probe RSSI Location, on page 319
- Configuring Probe RSSI , on page 319
- RFID Tag Support, on page 321
- Configuring RFID Tag Support, on page 321
- Verifying RFID Tag Support, on page 322

Information About Network Mobility Services Protocol

Cisco Network Mobility Services Protocol (NMSP) is a secure two-way protocol that can be run over a connection-oriented (TLS) or HTTPS transport. The wireless infrastructure runs the NMSP server and Cisco Connected Mobile Experiences (Cisco CMX) acts as an NMSP client. The controller supports multiple services and multiple Cisco CMXs can connect to the NMSP server to get the data for the services (location of wireless devices, probe RSSI, hyperlocation, wIPS, and so on.) over the NMSP or HTTPS session.

NMSP defines the intercommunication between Cisco CMX and the controller. Cisco CMX communicates to the controller over a routed IP network. Both publish-subscribe and request-reply communication models are supported. Typically, Cisco CMX establishes a subscription to receive services data from the controller in the form of periodic updates. The controller acts as a data publisher, broadcasting services data to multiple CMXs. Besides subscription, Cisco CMX can also send requests to the controller, causing the controller to send a response back.

The following is a list of the Network Mobility Services Protocol features:

- NMSP is disabled by default.
- NMSP communicates with Cisco CMX using TCP, and uses TLS for encryption.

- Wireless intrusion prevention system (wIPS) is supported only over TCP and TLS.
- Bidirectional communication is supported and Cisco CMX can send a message asynchronously over the established channel.

Note HTTPS is not supported for data transport between controller and Cisco CMX.

Radioactive Tracing for NMSP

This feature collects and provides all CMX-related events.

When a controller is added to CMX with an existing logging or serviceability tools, the following occurs:

- CMX reaches out to the controller through SNMP and CLI.
- Configures the CMX hash key on the controller.
- CMX requests the controller to open an NMSP connection.

RA tracing simplifies troubleshooting by allowing:

- RA trace the CMX IP on the controller.
- Collect all logs about it.

Enabling NMSP on Premises Services

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**nmsp enable** **Example:** `Device(config)# nmsp enable`	Enables NMSP on premises services. **Note** By default, the NMSP is enabled on the controller.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues

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.

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

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**nmsp notification interval** {**rssi** {**clients** | **rfid** | **rogues** {**ap** | **client** } | **spectrum interferers** } *interval*} **Example:** `Device(config)# nmsp notification interval rssi rfid 50`	Sets the NMSP notification interval value for clients, RFID tags, rogue clients, and access points. *interval*-NMSP notification interval value, in seconds for RSSI measurement. Valid range is from 1 to 180.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Modifying the NMSP Notification Threshold for Clients, RFID Tags, and Rogues

Procedure

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

	Command or Action	Purpose
Step 2	**location notify-threshold** {**clients** | **rogues ap** | **tags** } *threshold* **Example:** `Device(config)# location notify-threshold clients 5`	Configures the NMSP notification threshold for clients, RFID tags, rogue clients, and access points. *threshold*- RSSI threshold value in db. Valid range is from 0 to 10, with a default value of 0..
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring NMSP Strong Cipher

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**nmsp strong-cipher** **Example:** `Device(config)# nmsp strong-cipher`	Enable strong ciphers for NMSP server, which contains "ECDHE-RSA-AES128-GCM-SHA256:, ECDHE-ECDSA-AES128-GCM-SHA256:, AES256-SHA256:AES256-SHA:, and AES128-SHA256:AES128-SHA". Normal cipher suite contains, "ECDHE-RSA-AES128-GCM-SHA256:, ECDHE-ECDSA-AES128-GCM-SHA256:, and AES128-SHA".
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying NMSP Settings

To view the NMSP capabilities of the controller , use the following command:

```
Device# show nmsp capability
Service            Subservice
-----------------------------
RSSI               Rogue, Tags, Mobile Station,
```

```
Spectrum           Aggregate Interferer, Air Quality, Interferer,
Info               Rogue, Mobile Station,
Statistics         Rogue, Tags, Mobile Station,
AP Monitor         Subscription
On Demand Services Device Info
AP Info            Subscription
```

To view the NMSP notification intervals, use the following command:

```
Device# show nmsp notification interval
NMSP Notification Intervals
---------------------------

RSSI Interval:
  Client              : 2 sec
  RFID                : 50 sec
  Rogue AP            : 2 sec
  Rogue Client        : 2 sec
  Spectrum            : 2 sec
```

To view the connection-specific statistics counters for all CMX connections, use the following command:

```
Device# show nmsp statistics connection
NMSP Connection Counters
------------------------
 CMX IP Address: 10.22.244.31, Status: Active
 State:
      Connections : 1
      Disconnections : 0
      Rx Data Frames : 13
      Tx Data Frames : 99244
      Unsupported messages : 0
  Rx Message Counters:
     ID  Name                                  Count
    ---------------------------------------------
      1  Echo Request                          6076
      7  Capability Notification                  2
     13  Measurement Request                      5
     16  Information Request                      3
     20  Statistics Request                       2
     30  Service Subscribe Request                1

  Tx Message Counters:
     ID  Name                                  Count
    ---------------------------------------------
      2  Echo Response                         6076
      7  Capability Notification                  1
     14  Measurement Response                    13
     15  Measurement Notification             91120
     17  Information Response                     6
     18  Information Notification              7492
     21  Statistics Response                      2
     22  Statistics Notification                305
     31  Service Subscribe Response               1
     67  AP Info Notification                   304
```

To view the common statistic counter of the controller 's NMSP service, use the following command:

```
Device# show nmsp statistics summary
NMSP Global Counters
--------------------
Number of restarts                :

SSL Statistics
--------------------
Total amount of verifications      : 6
```

```
Verification failures              : 6
Verification success               : 0
Amount of connections created      : 8
Amount of connections closed       : 7
Total amount of accept attempts    : 8
Failures in accept                 : 0
Amount of successful accepts       : 8
Amount of failed registrations     : 0

AAA Statistics
--------------------
Total amount of AAA requests       : 7
Failed to send requests            : 0
Requests sent to AAA               : 7
Responses from AAA                 : 7
Responses from AAA to validate     : 7
Responses validate error           : 6
Responses validate success         : 1
```

To view the overall NMSP connections, use the following command:

```
Device# show nmsp status
NMSP Status
-----------

CMX IP Address   Active    Tx Echo Resp  Rx Echo Req   Tx Data     Rx Data     Transport
------------------------------------------------------------------------------------------
127.0.0.1        Active    6             6             1           2           TLS
```

To view all mobility services subscribed by all CMXs, use the following command:

```
Device# show nmsp subscription detail
CMX IP address 127.0.0.1:
Service            Subservice
-----------------------------
RSSI               Rogue, Tags, Mobile Station,
Spectrum
Info               Rogue, Mobile Station,
Statistics         Tags, Mobile Station,
AP Info            Subscription
```

To view all mobility services subscribed by a specific CMX, use the following command:

```
Device# show nmsp subscription detail <ip_addr>
CMX IP address 127.0.0.1:
Service            Subservice
-----------------------------
RSSI               Rogue, Tags, Mobile Station,
Spectrum
Info               Rogue, Mobile Station,
Statistics         Tags, Mobile Station,
AP Info            Subscription
```

To view the overall mobility services subscribed by all CMXs, use the following command:

```
Device# show nmsp subscription summary
Service            Subservice
-----------------------------
RSSI               Rogue, Tags, Mobile Station,
Spectrum
Info               Rogue, Mobile Station,
Statistics         Tags, Mobile Station,
AP Info            Subscription
```

Examples: NMSP Settings Configuration

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

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

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

```
Device# configure terminal
Device(config)# nmsp notification interval rssi clients 180
Device(config)# end
Device# show nmsp notification interval
```

NMSP by AP Groups with Subscription List from CMX

The Cisco CMX group support allows you to send only the required Network Mobility Services Protocol (NMSP) data to Cisco CMX (applicable to both on-premises and cloud-based CMX). The Cisco CMX can subscribe to NMSP data of specific APs or AP groups based on the active services in the wireless controller.

This feature helps in load balancing and optimizing the data flow load, when the APs are distributed across different CMX servers. The Cisco CMX server creates a CMX AP group giving it a unique name and groups the APs under it.

Note The Cisco CMX AP Group is the list of Cisco APs managed by the Cisco CMX for location services. This AP group is not the same as the wireless controller AP group.

This feature supports the following services:

- Client
- Probe client filtering
- Hyperlocation
- BLE Services

Note NMSP subscription is available only for those services that are in enabled state in the wireless controller.

Verifying NMSP by AP Groups with Subscription List from CMX

To verify mobility services group subscription summary of all CMX connections, use the following command:

```
Device# show nmsp subscription group summary

CMX IP address: 127.0.0.1
  Groups subscribed by this CMX server:
  Group name: Group1
```

To view the services that are subscribed for an AP group by a CMX connection, use the following command:

```
Device# show nmsp subscription group details services group-name cmx-IP-addrress

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group filtered services:
Service            Subservice
-----------------------------
RSSI               Mobile Station,
Spectrum
Info
Statistics
```

To view the AP MAC list that is subscribed for an AP group by a CMX connection, use the following command:

```
Device show nmsp subscription group detail ap-list group-name  cmx-IP-addrress

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group AP MACs:
: 00:00:00:00:70:02  00:00:00:00:66:02  00:99:00:00:00:02  00:00:00:bb:00:02
  00:00:00:00:55:02  00:00:00:00:50:02  00:33:00:00:00:02  00:d0:00:00:00:02
  00:10:00:10:00:02  00:00:00:06:00:02  00:00:00:02:00:02  00:00:00:00:40:02
  00:00:00:99:00:02  00:00:00:00:a0:02  00:00:77:00:00:02  00:22:00:00:00:02
  00:00:00:00:00:92  00:00:00:00:00:82  00:00:00:00:03:02  aa:00:00:00:00:02
  00:00:00:50:00:42  00:00:0d:00:00:02  00:00:00:00:00:32  00:00:00:cc:00:02
  00:00:00:88:00:02  20:00:00:00:00:02  10:00:00:00:00:02  01:00:00:00:00:02
  00:00:00:00:00:02  00:00:00:00:00:01  00:00:00:00:00:00
```

To view CMX-AP grouping details for all CMXs, use the following command:

```
Device# show nmsp subscription group detail all
CMX IP address: 127.0.0.1
  Groups subscribed by this CMX server:
  Group name: Group1
    CMX Group filtered services:
    Service            Subservice
    -----------------------------
    RSSI               Mobile Station,
    Spectrum
    Info
    Statistics

    CMX Group AP MACs:
    : 00:00:00:00:00:03  00:00:00:00:00:02  00:00:00:00:00:01

  Group name: Group2
    CMX Group filtered services:
    Service            Subservice
    -----------------------------
    RSSI               Tags,
    Spectrum
    Info
    Statistics
```

```
    CMX Group AP MACs:
    : 00:00:00:00:03:00  00:00:00:00:02:00  00:00:00:00:01:00

  Group name: Group3
    CMX Group filtered services:
    Service            Subservice
    ----------------------------
    RSSI               Rogue,
    Spectrum
    Info
    Statistics

    CMX Group AP MACs:
    : 00:00:00:03:00:00  00:00:00:02:00:00  00:00:00:01:00:00
```

To view all the AP lists subscribed by all CMXs, use the following command:

```
Device# show nmsp subscription group detail ap-list <group> <cmx-ip>
```

To view all the services subscribed by all CMXs, use the following command:

```
Device# show nmsp subscription group detail services <group> <cmx-ip>
```

Probe RSSI Location

The Probe RSSI Location feature allows the wireless controller and Cisco CMX to support the following:

- Load balancing
- Coverage Hole detection
- Location updates to CMX

When a wireless client is enabled, it sends probe requests to identify the wireless networks in the vicinity and also to find the received signal strength indication (RSSI) associated with the identified Service Set Identifiers (SSIDs).

The wireless client periodically performs active scanning in background even after being connected to an access point. This helps them to have an updated list of access points with best signal strength to connect. When the wireless client can no longer connect to an access point, it uses the access point list stored to connect to another access point that gives it the best signal strength. The access points in the WLAN gather these probe requests, RSSI and MAC address of the wireless clients and forwards them to the wireless controller s. The Cisco CMX gathers this data from the wireless controller and uses it to compute the updated location of the wireless client when it roams across the network.

Configuring Probe RSSI

Procedure

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

	Command or Action	Purpose
Step 2	**wireless probe filter** **Example:** `Device(config)# wireless probe filter`	Enables filtering of unacknowledged probe requests from AP to improve the location accuracy. Filtering is enabled by default. Use the **no** form of the command to disable the feature. This will forward both acknowledged and unacknowledged probe requests to the controller.
Step 3	**wireless probe limit** *limit-value interval* **Example:** `Device(config)# wireless probe limit 10 100`	Configures the number of probe request reported to the wireless controller from the AP for the same client on a given interval. Use the **no** form of the command to revert to the default limit, which is 2 probes at an interval of 500 ms.
Step 4	**wireless probe locally-administered-mac** **Example:** `Device(config)# wireless probe locally-administered-mac`	Enables the reporting of probes from clients having locally administered MAC address.
Step 5	**location algorithm rssi-average** **Example:** `Device(config)# location algorithm rssi-average`	Sets the probe RSSI measurement updates to a more accurate algorithm but with more CPU overhead.
Step 6	**location algorithm simple** **Example:** `Device(config)# location algorithm simple`	(Optional) Sets the probe RSSI measurement updates to a faster algorithm with smaller CPU overhead, but less accuracy. Use the **no** form of the command to revert the algorithm type to the default one, which is *rssi-average*.
Step 7	**location expiry client** *interval* **Example:** `Device(config)# location expiry client 300`	Configures the timeout for RSSI values. The **no** form of the command sets it to a default value of 15.
Step 8	**location notify-threshold client** *threshold-db* **Example:** `Device(config)# location notify-threshold client 5`	Configures the notification threshold for clients. The **no** form of the command sets it to a default value of 0.
Step 9	**location rssi-half-life client** *time-in-seconds* **Example:** `Device(config)# location rssi-half-life client 20`	Configures half life when averaging two RSSI readings. To disable this option, set the value to 0.

What to do next

Use the **show wireless client probing** command to view each probing client (associated and probing only) by batch of 10 MAC addresses.

RFID Tag Support

The controller enables you to configure radio frequency identification (RFID) tag tracking. RFID tags are small wireless battery-powered tags that continuously broadcast their own signal and are affixed to assets for real-time location tracking. They operate by advertising their location using special 802.11 packets, which are processed by access points, the controller , and the Cisco CMX. Only active RFIDs are supported. A combination of active RFID tags and wireless controller allows you to track the current location of equipment. *Active* tags are typically used in real-time tracking of high-value assets in *closed-loop* systems (that is,) systems in which the tags are not intended to physically leave the control premises of the tag owner or originator.

For more information on RFID tags, see the Active RFID Tags section of the *Wi-Fi Location-Based Services 4.1 Design Guide*.

General Guidelines

- Only Cisco-compliant active RFID tags are supported.
- You can verify the RFID tags on the controller .
- High Availability for RFID tags are supported.

Configuring RFID Tag Support

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless rfid** **Example:** `Device(config)# wireless rfid`	Enables RFID tag tracking. The default value is enabled. Use the **no** form of this command to disable RFID tag tracking.
Step 3	**wireless rfid timeout** *timeout-value* **Example:** `Device(config)# wireless rfid timeout 90`	Configures the RFID tag data timeout value to cleanup the table. The timeout value is the amount of time that the controller maintains tags before expiring them. For example, if a tag is configured to beacon every 30 seconds, we recommend that you set the timeout value to 90 seconds

	Command or Action	Purpose
		(approximately three times the beacon value). The default value is 1200 seconds.

Verifying RFID Tag Support

To view the summary of RFID tags that are clients, use the following command:

```
Device# show wireless rfid client
```

To view the detailed information for an RFID tag, use the following command:

```
Device# show wireless rfid detail <rfid-mac-address>

RFID address  000c.cc96.0001
Vendor Cisco
Last Heard 6 seconds  ago
Packets Received 187
Bytes Received 226

Content Header
==============
  CCX Tag Version 0
  Tx power: 12
  Channel: 11
  Reg Class: 4
CCX Payload
==============
  Last Sequence Control 2735
  Payload length 221
  Payload Data Hex Dump:
  00000000  00 02 00 00 01 09 00 00  00 00 0c b8 ff ff ff 02  |................|
  00000010  07 42 03 20 00 00 0b b8  03 4b 00 00 00 00 00 00  |.B. .....K......|
  00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
  00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
  00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

To view the summary information for all known RFID tags, use the following command:

```
Device# show wireless rfid summary

Total RFID entries: : 16
Total Unique RFID entries : 16
RFID ID VENDOR Closet AP RSSI Time Since Last Heard
0012.b80a.c791 Cisco 7069.5a63.0520 -31 3 minutes 30 seconds ago
0012.b80a.c953 Cisco 7069.5a63.0460 -33 4 minutes 5 seconds ago
0012.b80b.806c Cisco 7069.5a63.0520 -46 15 seconds ago
0012.b80d.e9f9 Cisco 7069.5a63.0460 -38 4 minutes 28 seconds ago
0012.b80d.ea03 Cisco 7069.5a63.0520 -43 4 minutes 29 seconds ago
0012.b80d.ea6b Cisco 7069.5a63.0460 -39 4 minutes 26 seconds ago
0012.b80d.ebe8 Cisco 7069.5a63.0520 -43 3 minutes 21 seconds ago
0012.b80d.ebeb Cisco 7069.5a63.0520 -43 4 minutes 28 seconds ago
0012.b80d.ec48 Cisco 7069.5a63.0460 -42 4 minutes 7 seconds ago
0012.b80d.ec55 Cisco 7069.5a63.0520 -41 1 minute 52 seconds ago
```

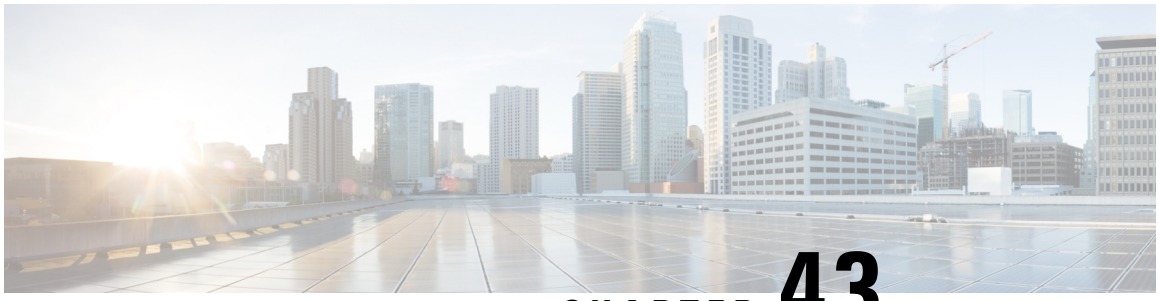
To view the location-based system RFID statistics, use the following command:

```
Device# show wireless rfid stats
```

```
RFID stats :
==============
RFID error db full : 0
RFID error invalid paylod : 0
RFID error invalid tag : 0
RFID error dot11 hdr : 0
RFID error pkt len : 0
RFID error state drop : 0
RFID total pkt received : 369
RFID populated error value : 0
RFID error insert records : 0
RFID error update records : 0
RFID total insert record : 16
RFID ccx payload error : 0
RFID total delete record : 0
RFID error exceeded ap count : 0
RFID error record remove : 0
RFID old rssi expired count: 0
RFId smallest rssi expireed count : 0
RFID total query insert : 0
RFID error invalid rssi count : 0
```

To view the NMSP notification interval, use the following command:

```
Device# show nmsp notification interval

NMSP Notification Intervals
---------------------------

RSSI Interval:
  Client              : 2 sec
  RFID                : 50 sec
  Rogue AP            : 2 sec
  Rogue Client        : 2 sec
  Spectrum            : 2 sec
```



CHAPTER 43

Application Visibility and Control

- Information About Application Visibility and Control, on page 325
- Create a Flow Monitor, on page 328
- Configuring a Flow Monitor (GUI), on page 330
- Create a Flow Record, on page 330
- Create a Flow Exporter , on page 332
- Configuring a Policy Tag, on page 333
- Attaching a Policy Profile to a WLAN Interface (GUI), on page 334
- Attaching a Policy Profile to a WLAN Interface (CLI), on page 334
- Attaching a Policy Profile to an AP, on page 335
- Verify the AVC Configuration, on page 336
- Default DSCP on AVC, on page 337
- AVC-Based Selective Reanchoring, on page 339
- Restrictions for AVC-Based Selective Reanchoring, on page 340
- Configuring the Flow Exporter, on page 340
- Configuring the Flow Monitor, on page 340
- Configuring the AVC Reanchoring Profile, on page 341
- Configuring the Wireless WLAN Profile Policy , on page 342
- Verifying AVC Reanchoring, on page 343

Information About Application Visibility and Control

Application Visibility and Control (AVC) is a subset of the entire Flexible NetFlow (FNF) package that can provide traffic information. The AVC feature employs a distributed approach that benefits from NBAR running on the access point (AP) or controller whose goal is to run deep packet inspection (DPI) and reports the results using FNF messages.

AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades. Traffic flows are analyzed and recognized using the NBAR2 engine. The specific flow is marked with the recognized protocol or application. This per-flow information can be used for application visibility using FNF. After the application visibility is established, a user can define control rules with policing mechanisms for a client.

Using AVC rules, 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 that takes precedence over the per-application rate limits.

FNF feature is supported in wireless, and relies on the NetFlow enablement on the controller for all modes: flex, local and Fabric.

In local mode, the NBAR runs on the controller hardware and the process client traffic flows through the data plane of the controller using the AP CAPWAP tunnels.

In FlexConnect or Fabric mode, NBAR runs on the AP, and only statistics are sent to the controller . When operating in these two modes, APs regularly send FNFv9 reports back to the controller . The controller's FNF feature consumes those FNFv9 reports to provide the application statistics shown by AVC.

The Fabric mode of operation does not populate the FNF cache. It relays the FNFv9 reports at the time they arrive. As a result, some configuration of flow monitors, for example, cache timeout, is not taken into account.

The behavior of the AVC solution changes based on the wireless deployments. The following sections describe the commonalities and differences in all scenarios:

Local Mode

- NBAR is enabled on the controller .
- AVC does not push the FNF configuration to the APs.
- Roaming events are ignored.

  However, AVC supports L3 roams in local mode as traffic flows through the anchor controller (where NBAR was initially processing the roaming client's traffic when the client joined).
- IOSd needs to trigger NBAR attach.
- Supports flow monitor cache.
- Supports NetFlow exporter.

Flex Mode

- NBAR is enabled on an AP
- AVC pushes the FNF configuration to the APs.
- Supports context transfer for roaming in AVC-FNF.
- Supports flow monitor cache.
- Supports NetFlow exporter.

Fabric Mode

- NBAR is enabled on an AP.
- AVC pushes the FNF configuration to the APs.
- Supports context transfer for roaming in AVC-FNF.
- Flow monitor cache is not supported.
- Supports NetFlow exporter (for the C9800 embedded on Catalyst switches for SDA, there is no FNF cache on the box).

Prerequisites for Application Visibility and Control

- The access points should be AVC capable.

  However, this requirement is not applicable in Local mode.

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

Restrictions for Application Visibility and Control

- IPv6 (including ICMPv6 traffic) packet classification is not supported in FlexConnect mode and Fabric mode. However, it is supported in Local mode.
- Layer 2 roaming is not supported across controller controllers.
- Multicast traffic is not supported.
- AVC is supported only on the following access points:
  - Cisco Catalyst 9100 Series Access Points
  - Cisco Aironet 1800 Series Access Points
  - Cisco Aironet 2700 Series Access Point
  - Cisco Aironet 2800 Series Access Point
  - Cisco Aironet 3700 Series Access Points
  - Cisco Aironet 3800 Series Access Points
  - Cisco Aironet 4800 Series Access Points
- AVC is not supported on Cisco Aironet 702W, 702I (128 M memory), and 1530 Series access points.
- Only the applications that are recognized with App visibility can be used for applying QoS control.
- Data link is not supported for NetFlow fields in AVC.
- You cannot map the same WLAN profile to both the AVC-not-enabled policy profile and the AVC-enabled policy profile.
- AVC is not supported on the management port (Gig 0/0).
- NBAR-based QoS policy configuration is allowed only on wired physical ports. Policy configuration is not supported on virtual interfaces, for example, VLAN, port channel and other logical interfaces.

When AVC is enabled, the AVC profile supports only up to 23 rules, which includes the default DSCP rule. The AVC policy will not be pushed down to the AP, if rules are more than 23.

AVC Configuration Overview

To configure AVC, follow these steps:

1. Create a flow monitor using the **record wireless avc basic** command.
2. Create a wireless policy profile.

3. Apply the flow monitor to the wireless policy profile.
4. Create a wireless policy tag.
5. Map the WLAN to the policy profile
6. Attach the policy tag to the APs.

Create a Flow Monitor

The NetFlow configuration requires a flow record, a flow monitor, and a flow exporter. This configuration should be the first step in the overall AVC configuration.

Note In Flex mode and Local mode, the default values for **cache timeout active** and **cache timeout inactive** commands are not optimal for AVC. We recommend that you set both the values to 60 in the flow monitor.

For Fabric mode, the cache timeout configuration does not apply.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**flow monitor** *monitor-name* **Example:** `Device(config)# flow monitor fm_avc`	Creates a flow monitor.

Step 3	**record wireless avc basic**
	Example:
	`Device(config-flow-monitor)# record wireless`
	`avc basic`
		Specifies the basic wireless AVC flow template.
		Note The **record wireless avc basic** command is same as **record wireless avc ipv4 basic** command. However, **record wireless avc ipv4 basic** command is not supported in Flex or Fabric modes. In such scenarios, use the **record wireless avc basic** command.

Step 4	**record wireless avc** {**ipv4** | **ipv6**} **basic** **Example:**	Specifies the basic IPv4 or IPv6 wireless AVC flow template.

	Command or Action	Purpose
	`Device(config-flow-monitor)# record wireless avc ipv6 basic`	**Note** If you want to have both Application Performance Monitoring (APM) and AVC-FNF in the device simultaneously, use the **record wireless avc {ipv4 | ipv6} assurance** command, which is a superset of the fields contained in **record wireless avc {ipv4 | ipv6} basic** command. If the containing flow monitor is configured with the local exporter using **destination wlc local** command, AVC-FNF will populate the statistics exactly as that of the **record wireless avc {ipv4 | ipv6} basic** configuration. As a result, both APM and AVC-FNF can be configured simultaneously with two flow monitors per direction, per IP version, in local (central switching) mode. **Note** The **record wireless avc basic** command is same as **record wireless avc ipv4 basic** command. However, **record wireless avc ipv4 basic** command is not supported in Flex or Fabric modes. In such scenarios, use the **record wireless avc basic** command.
Step 5	**cache timeout active** *value* **Example:** `Device(config-flow-monitor)# cache timeout active 60`	Sets the active flow timeout in seconds.
Step 6	**cache timeout inactive** *value* **Example:** `Device(config-flow-monitor)# cache timeout inactive 60`	Sets the inactive flow timeout in seconds.

Configuring a Flow Monitor (GUI)

Before you begin

You must have created a flow exporter to export data from the flow monitor.

Procedure

Step 1 Choose **Configuration** > **Services** > **Application Visibility** and go to the **Flow Monitor** tab .

Step 2 In the **Monitor** area, click **Add** to add a flow monitor.

Step 3 In the **Flow Monitor** window, add a flow monitor and a description.

Step 4 Select the Flow exporter from the drop-down list to export the data from the flow monitor to a collector.

Note To export wireless netflow data, use the templates below:

- ETA (Encrypted Traffic Analysis)
- wireless avc basic
- wireless avc basic IPv6

Step 5 Click **Apply to Device** to save the configuration.

Create a Flow Record

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

Procedure

	Command or Action	Purpose
Step 1	**flow record** *flow_record_name* **Example:** `Device(config)# flow record record1`	Creates a flow record. **Note** When a custom flow record is configured in Flex and Fabric modes, the optional fields (fields that are not present in record wireless avc basic) are ignored.
Step 2	**description** *string* **Example:** `Device(config-flow-record)# description IPv4flow`	(Optional) Describes the flow record as a maximum 63-character string.

	Command or Action	Purpose
Step 3	**match ipv4 protocol** **Example:** `Device(config-flow-record)# match ipv4 protocol`	Specifies a match to the IPv4 protocol.
Step 4	**match ipv4 source address** **Example:** `Device(config-flow-record)# match ipv4 source address`	Specifies a match to the IPv4 source address-based field.
Step 5	**match ipv4 destination address** **Example:** `Device(config-flow-record)# match ipv4 destination address`	Specifies a match to the IPv4 destination address-based field.
Step 6	**match transport source-port** **Example:** `Device(config-flow-record)# match transport source-port`	Specifies a match to the transport layer's source port field.
Step 7	**match transport destination-port** **Example:** `Device(config-flow-record)# match transport destination-port`	Specifies a match to the transport layer's destination port field.
Step 8	**match flow direction** **Example:** `Device(config-flow-record)# match flow direction`	Specifies a match to the direction the flow was monitored in.
Step 9	**match application name** **Example:** `Device(config-flow-record)# match application name`	Specifies a match to the application name. **Note** This action is mandatory for AVC support because this allows the flow to be matched against the application.
Step 10	**match wireless ssid** **Example:** `Device(config-flow-record)# match wireless ssid`	Specifies a match to the SSID name identifying the wireless network.
Step 11	**collect counter bytes long** **Example:** `Device(config-flow-record)# collect counter bytes long`	Collects the counter field's total bytes.

	Command or Action	Purpose
Step 12	**collect counter packets long** **Example:** `Device(config-flow-record)# collect counter bytes long`	Collects the counter field's total packets.
Step 13	**collect wireless ap mac address** **Example:** `Device(config-flow-record)# collect wireless ap mac address`	Collects the BSSID with the MAC addresses of the access points that the wireless client is associated with.
Step 14	**collect wireless client mac address** **Example:** `Device(config-flow-record)# collect wireless client mac address`	Collects the MAC address of the client on the wireless network.

Create a Flow Exporter

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

Note For the AVC statistics to be visible at the controller , you should configure a local flow exporter using the following commands:

- **flow exporter** *my_local*
- **destination local wlc**

Also, your flow monitor must use this local exporter for the statistics to be visible at the controller .

Procedure

	Command or Action	Purpose
Step 1	**flow exporter** *flow-export-name* **Example:** `Device(config)# flow exporter export-test`	Creates a flow monitor.
Step 2	**description** *string* **Example:** `Device(config-flow-exporter)# description IPv4flow`	Describes the flow record as a maximum 63-character string.

	Command or Action	Purpose
Step 3	**destination** {*hostname/ipv4address* | *hostname/ipv6address* |*local {wlc}*} **Example:** `Device(config-flow-exporter)# destination local wlc`	Specifies the hostname or IP address of the system or the local WLC to which the exporter sends data.
Step 4	**transport udp** *port-value* **Example:** `Device(config-flow-exporter)# transport udp 1024`	(Optional) Configures the destination UDP port to reach the external collector. The default value is 9995. **Note** This step is required only for external collectors; not required for local wlc collector.
Step 5	**option application-table timeout** *seconds* **Example:** `Device(config-flow-exporter)# option application-table timeout 500`	(Optional) Specifies the application table timeout option, in seconds. The valid range is from 1 to 86400.
Step 6	**end** **Example:** `Device(config-flow-exporter)# end`	Returns to privileged EXEC mode.
Step 7	**show flow exporter** **Example:** `Device# show flow exporter`	(Optional) Verifies your configuration.

Configuring a Policy Tag

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config-policy-tag)# wireless tag policy rr-xyz-policy-tag`	Configures policy tag and enters policy tag configuration mode.
Step 3	**end** **Example:**	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-policy-tag)# end`	

Attaching a Policy Profile to a WLAN Interface (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 On the**Manage Tags** page, click **Policy** tab.

Step 3 Click **Add** to view the **Add Policy Tag** window.

Step 4 Enter a name and description for the policy tag.

Step 5 Click **Add** to map WLAN and policy.

Step 6 Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.

Step 7 Click **Save & Apply to Device**.

Attaching a Policy Profile to a WLAN Interface (CLI)

Before you begin

- Do not attach different AVC policy profiles on the same WLAN across different policy tags.

  The following is an example of incorrect configuration:

```
wireless profile policy avc_pol1
   ipv4 flow monitor fm-avc1 input
   ipv4 flow monitor fm-avc1 output
   no shutdown
  wireless profile policy avc_pol2
   ipv4 flow monitor fm-avc2 input
   ipv4 flow monitor fm-avc2 output
   no shutdown
  wireless tag policy avc-tag1
   wlan wlan1 policy avc_pol1
  wireless tag policy avc-tag2
   wlan wlan1 policy avc_pol2
```

  This example violates the restriction stated earlier, that is, the WLAN *wlan1* is mapped to 2 policy profiles, *avc_pol1* and *avc_pol2*. This configuration is, therefore, incorrect because the WLAN *wlan1* should be mapped to either *avc_pol1* or *avc_pol2* everywhere.

- Conflicting policy profiles on the same WLAN are not supported. For example, policy profile (with and without AVC) applied to the same WLAN in different policy tags.

  The following is an example of an incorrect configuration:

```
wireless profile policy avc_pol1
   no shutdown
```

```
wireless profile policy avc_pol2
 ipv4 flow monitor fm-avc2 input
 ipv4 flow monitor fm-avc2 output
 no shutdown
wireless tag policy avc-tag1
 wlan wlan1 policy avc_pol1
wireless tag policy avc-tag2
 wlan wlan1 policy avc_pol2
```

In this example, a policy profile with and without AVC is applied to the same WLAN in different tags.

Procedure

	Command or Action	Purpose
Step 1	**wireless tag policy** *avc-tag* **Example:** `Device(config)# wireless tag policy avc-tag`	Creates a policy tag.
Step 2	**wlan** *wlan-avc* **policy** *avc-policy* **Example:** `Device(config-policy-tag)# wlan wlan_avc policy avc_pol`	Attaches a policy profile to a WLAN profile.

What to do next

- Run the **no shutdown** command on the WLAN after completing the configuration.
- If the WLAN is already in **no shutdown** mode, run the **shutdown** command, followed by **no shutdown** command.

Attaching a Policy Profile to an AP

Procedure

	Command or Action	Purpose
Step 1	**ap** *ap-ether-mac* **Example:** `Device(config)# ap 34a8.2ec7.4cf0`	Enters AP configuration mode.
Step 2	**policy-tag** *policy-tag* **Example:** `Device(config)# policy-tag avc-tag`	Specifies the policy tag that is to be attached to the access point.

Verify the AVC Configuration

Procedure

	Command or Action	Purpose
Step 1	**show avc wlan** *wlan-name* **top** *num-of-applications* **applications {aggregate | downstream | upstream}** **Example:** `Device# show avc wlan wlan_avc top 2 applications aggregate`	Displays information about top applications and users using these applications. **Note** Ensure that wireless clients are associated to the WLAN and generating traffic, and then wait for 90 seconds (to ensure the availability of statistics) before running the command.
Step 2	**show avc client** *mac* **top** *num-of-applications* **applications {aggregate | downstream | upstream}** **Example:** `Device# show avc client 9.3.4 top 3 applications aggregate`	Displays information about the top number of applications. **Note** Ensure that wireless clients are associated to the WLAN and generating traffic, and then wait for 90 seconds (to ensure the availability of statistics) before running the command.
Step 3	**show avc wlan** *wlan-name* **application** *app-name* **top** *num-of-clients* **aggregate** **Example:** `Device# show avc wlan wlan_avc application app top 4 aggregate`	Displays information about top applications and users using these applications.
Step 4	**show ap summary** **Example:** `Device# show ap summary`	Displays a summary of all the access points attached to the controller .
Step 5	**show ap tag summary** **Example:** `Device# show ap tag summary`	Displays a summary of all the access points with policy tags.

Default DSCP on AVC

Configuring Default DSCP for AVC Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **QoS**.

Step 2 Click **Add**.

Step 3 Enter the **Policy Name**.

Step 4 Click **Add Class-Maps**.

Step 5 Choose **AVC** in the **AVC/User Defined** drop-down list.

Step 6 Click either **Any** or **All** match type radio button.

Step 7 Choose **DSCP** in the **Mark Type** drop-down list.

Step 8
a) Check the **Drop** check box to drop traffic from specific sources.
b) If you do not want to drop the traffic, enter the **Police(kbps)** and choose the match type from the **Match Type** drop-down list. Choose the items from the available list and click move them to the selected list.

Step 9 Click **Save**.

Step 10 Click **Apply to Device**.

Configuring Default DSCP for AVC Profile

In Cisco Catalyst 9800 Series Wireless Controller, only up to 32 filters can be specified in the policy. As there was no way of classifying the packets that are not specified in the filters, now, you can mark down these packets in the policy.

The marking action can be applied to the traffic when creating a class map and creating a policy map.

Creating Class Map

Procedure

	Command or Action	Purpose
Step 1	**Configure Terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**class** *class-map-name*] **Example:** `Device(config-pmap)# class-map avc-class`	Creates a class map.

	Command or Action	Purpose

Step 3	**match protocol** { *application-name* | **attribute category** *category-name* | **attribute sub-category** *sub-category-name* | **attribute application-group** *application group-name*
	Example:
	`Device(config)# class-map avc-class`
	`Device(config-cmap)# match protocol avc-media`
	`Device(config)# class-map class-avc-category`
	`Device(config-cmap)# match protocol attribute category avc-media`
	`Device# class-map class-avc-sub-category`
	`Device(config-cmap)# match protocol attribute sub-category avc-media`
	`Device# class-map avcS-webex-application-group`
	`Device(config-cmap)# match protocol attribute application-group webex-media`
		Specifies match to the application name, category name, subcategory name, or application group.

Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Creating Policy Map

Procedure

	Command or Action	Purpose
Step 1	**Configure Terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map** *policy-map-name* **Example:** `Device(config)#policy-map avc-policy`	Creates a policy map by entering the policy map name, and enters policy-map configuration mode. By default, no policy maps are defined. The default behaviour of a policy map is to set the DSCP to 0 if the packet is an IP packet and to set the CoS to 0 if the packet is tagged. No policing is performed. **Note** To delete an existing policy map, use the no policy-map policy-map-name global configuration command.

	Command or Action	Purpose
Step 3	**class** [*class-map-name* | **class-default**] **Example:** `Device(config-pmap)# class-map avc-class`	Defines a traffic classification, and enters policy-map class configuration mode. By default, no policy map and class maps are defined. If a traffic class has already been defined by using the class-map global configuration command, specify its name for class-map-name in this command. A class-default traffic class is predefined and can be added to any policy. It is always placed at the end of a policy map. With an implied match any is included in the class-default class, all packets that have not already matched the other traffic classes will match class-default . **Note** To delete an existing class map, use the no class class-map-name policy-map configuration command.
Step 4	**set dscp** *new-dscp* **Example:** `Device(config-pmap-c)# set dscp 45`	Classifies IP traffic by setting a new value in the packet. For **dscp new-dscp** , enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63.
Step 5	**class** *class-default*	Specifies the default class so that you can configure or modify its policy.
Step 6	**set dscp default**	Configures the default DSCP.
Step 7	**end**	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

AVC-Based Selective Reanchoring

The AVC-Based Selective Reanchoring feature is designed to reanchor clients when they roam from one controller to another. Reanchoring of clients prevents the depletion of IP addresses available for new clients in Cisco WLC. The AVC profile-based statistics are used to decide whether a client must be reanchored or deferred. This is useful when a client is actively running a voice or video application defined in the AVC rules.

The reanchoring process also involves deauthentication of anchored clients. The clients get deauthenticated when they do not transmit traffic for the applications listed in the AVC rules while roaming between WLCs.

Restrictions for AVC-Based Selective Reanchoring

- This feature is supported only in local mode. FlexConnect and fabric modes are not supported.
- This feature is not supported in guest tunneling and export anchor scenarios.
- The old IP address is not released after reanchoring, until IP address' lease period ends.

Configuring the Flow Exporter

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**flow exporter** *name* **Example:** `Device(config)# flow exporter avc-reanchor`	Creates a flow exporter and enters flow exporter configuration mode. **Note** You can use this command to modify an existing flow exporter too.
Step 3	**destination local wlc** **Example:** `Device(config-flow-exporter)# destination local wlc`	Sets the exporter as local.

Configuring the Flow Monitor

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**flow monitor** *monitor-name* **Example:** `Device(config)# flow monitor fm_avc`	Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. **Note** You can use this command to modify an existing flow monitor too.

	Command or Action	Purpose
Step 3	**exporter** *exporter-name* **Example:** `Device(config-flow-monitor)# exporter avc-reanchor`	Specifies the name of an exporter.
Step 4	**record wireless avc basic** **Example:** `Device(config-flow-monitor)# record wireless avc basic`	Specifies the flow record to use to define the cache.
Step 5	**cache timeout active** *value* **Example:** `Device(config-flow-monitor)# cache timeout active 60`	Sets the active flow timeout, in seconds.
Step 6	**cache timeout inactive** *value* **Example:** `Device(config-flow-monitor)# cache timeout inactive 60`	Sets the inactive flow timeout, in seconds.

Configuring the AVC Reanchoring Profile

Before you begin

- Ensure that you use the AVC-Reanchor-Class class map. All other class-map names are ignored by Selective Reanchoring.
- During boot up, the system checks for the existence of the AVC-Reanchor-Class class map. If it is not found, default protocols, for example, jabber-video, wifi-calling, and so on, are created. If AVC-Reanchor-Class class map is found, configuration changes are not made and updates to the protocols that are saved to the startup configuration persist across reboots.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**class-map** *cmap-name* **Example:** `Device(config)# class-map AVC-Reanchor-Class`	Configures the class map.

	Command or Action	Purpose
Step 3	**match any** **Example:** `Device(config-cmap)# match any`	Instructs the device to match with any of the protocols that pass through it.
Step 4	**match protocol jabber-audio** **Example:** `Device(config-cmap)# match protocol jabber-audio`	Specifies a match to the application name. You can edit the class-map configuration later, in order to add or remove protocols, for example, jabber-video, wifi-calling, and so on, if required.

Configuring the Wireless WLAN Profile Policy

Follow the procedure given below to configure the WLAN profile policy:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures the WLAN policy profile and enters wireless policy configuration mode.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables the policy profile.
Step 4	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Enables central switching.
Step 5	**ipv4 flow monitor** *monitor-name* **input** **Example:** `Device(config-wireless-policy)# ipv4 flow monitor fm_avc input`	Specifies the name of the IPv4 ingress flow monitor.
Step 6	**ipv4 flow monitor** *monitor-name* **output** **Example:** `Device(config-wireless-policy)# ipv4 flow monitor fm_avc output`	Specifies the name of the IPv4 egress flow monitor.

	Command or Action	Purpose
Step 7	**reanchor class** *class-name* **Example:** `Device(config-wireless-policy)# reanchor class AVC-Reanchor-Class`	Configure a class map with protocols for the Selective Reanchoring feature.
Step 8	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the policy profile.

Verifying AVC Reanchoring

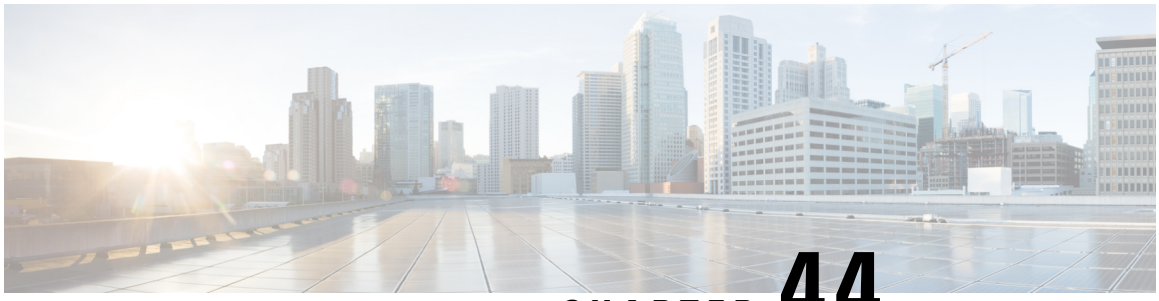
Use the following commands to verify the AVC reanchoring configuration:

```
Device# show wireless profile policy detailed avc_reanchor_policy

Policy Profile Name           : avc_reanchor_policy
Description                   :
Status                        : ENABLED
VLAN                          : 1
Wireless management interface VLAN        : 34
!
.
.
.
AVC VISIBILITY                : Enabled
Flow Monitor IPv4
  Flow Monitor Ingress Name   : fm_avc
  Flow Monitor Egress Name    : fm_avc
Flow Monitor IPv6
  Flow Monitor Ingress Name   : Not Configured
  Flow Monitor Egress Name    : Not Configured
NBAR Protocol Discovery       : Disabled
Reanchoring                   : Enabled
Classmap name for Reanchoring
  Reanchoring Classmap Name   : AVC-Reanchor-Class
!
.
.
.
  ------------------------------------------------------


Device# show platform software trace counter tag wstatsd chassis active R0 avc-stats debug

Counter Name Thread ID Counter Value
-----------------------------------------------------------------------------
Reanch_deassociated_clients 28340 1
Reanch_tracked_clients 28340 4
Reanch_deleted_clients 28340 3

Device# show platform software trace counter tag wncd chassis active R0 avc-afc debug

Counter Name Thread ID Counter Value
-----------------------------------------------------------------------------
Reanch_co_ignored_clients 30063 1
```

```
Reanch_co_anchored_clients 30063 5
Reanch_co_deauthed_clients 30063 4


Device# show platform software wlavc status wncd

Event history of WNCD DB:

AVC key: [1,wlan_avc,N/A,Reanc,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Reanchoring
Flow-mon-name : N/A
Policy-tag : default-policy-tag
Switching Mode : CENTRAL

Timestamp FSM State Event RC Ctx
------------------------- ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.630342 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822780 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822672 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.172073 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738367 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.738261 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.162689 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757643 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757542 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.468749 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.18857 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.18717 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164304 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163877 2 :READY 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:18.593257 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:18.593152 1 :INIT 24:CREATE_FSM 0 0

AVC key: [1,wlan_avc,fm_avc,v4-In,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Ingress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL

Timestamp FSM State Event RC Ctx
------------------------- ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.664772 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822499 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822222 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.207605 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738105 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.737997 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.164225 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757266 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757181 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.472778 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.15413 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.15263 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164254 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163209 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:20.163189 1 :INIT 24:CREATE_FSM 0 0

AVC key: [1,wlan_avc,fm_avc,v4-Ou,default-policy-tag]
Current state : READY
```

```
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Egress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL

Timestamp FSM State Event RC Ctx
------------------------- ------------------ ------------------------- ---- ----
06/12/2018 16:45:30.630764 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822621 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822574 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.172357 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738212 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.738167 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.164048 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757403 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757361 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.472561 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.18660 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.18588 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164293 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163799 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:20.163773 1 :INIT 24:CREATE_FSM 0 0


Device# show platform software wlavc status wncmgrd

Event history of WNCMgr DB:

AVC key: [1,wlan_avc,N/A,Reanc,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Reanchoring
Flow-mon-name : N/A
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

Timestamp FSM State Event RC Ctx
------------------------- ------------------ ------------------------- ---- ----
06/12/2018 16:45:30.629278 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.629223 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.629179 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.510867 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510411 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510371 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.886377 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
!

AVC key: [1,wlan_avc,fm_avc,v4-In,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Ingress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

Timestamp FSM State Event RC Ctx
------------------------- ------------------ ------------------------- ---- ----
06/12/2018 16:45:30.664032 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.663958 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
```

```
06/12/2018 16:45:30.663921 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.511151 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510624 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510608 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.810867 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
06/12/2018 16:45:28.807239 4 :READY 25:UNBIND_WNCD 0 0
06/12/2018 16:45:28.807205 4 :READY 23:UNBIND_IOSD 0 0
06/12/2018 16:45:28.806734 4 :READY 3 :FSM_WLAN_DOWN 0 0
!

AVC key: [1,wlan_avc,fm_avc,v4-Ou,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Egress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

Timestamp FSM State Event RC Ctx
------------------------- ------------------ ------------------------- ---- ----
06/12/2018 16:45:30.629414 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.629392 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.629380 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.510954 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510572 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510532 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.886293 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
06/12/2018 16:45:28.807844 4 :READY 25:UNBIND_WNCD 0 0
06/12/2018 16:45:28.807795 4 :READY 23:UNBIND_IOSD 0 0
06/12/2018 16:45:28.806990 4 :READY 3 :FSM_WLAN_DOWN 0 0
!
```



CHAPTER 44

Cisco Hyperlocation

- Information About Cisco Hyperlocation, on page 347
- Restrictions on Cisco Hyperlocation, on page 349
- Configuring Cisco Hyperlocation (GUI), on page 350
- Configuring Cisco Hyperlocation (CLI), on page 350
- Configuring Hyperlocation BLE Beacon Parameters for AP (GUI), on page 351
- Configuring Hyperlocation BLE Beacon Parameters for AP (CLI), on page 352
- Configuring Hyperlocation BLE Beacon Parameters (CLI), on page 352
- Verifying Cisco Hyperlocation, on page 353
- Verifying Hyperlocation BLE Beacon Configuration, on page 356
- Verifying Hyperlocation BLE Beacon Configuration for AP, on page 356

Information About Cisco Hyperlocation

Cisco Hyperlocation is an ultraprecise location solution that allows you to track the location of wireless clients. This is possible with the Cisco Hyperlocation radio module in the Cisco Aironet 3600, 3700, and 4800 Series Access Points. The Cisco Hyperlocation module combines Wi-Fi and Bluetooth Low Energy (BLE) technologies to allow beacons, inventory, and personal mobile devices to be pinpointed.

Hyperlocation is also supported in Fabric mode. In particular, when the wireless controller is running on the switch, the controller takes the necessary steps to provision the APs, so that they can generate Hyperlocation VxLAN packets that can traverse the fabric network taking advantage of the fabric infrastructure and be correctly delivered to the destination CMX.

The Hyperlocation VxLAN packets are special packets marked with SGT 0 and using the L3VNID of the APs. For more information, refer to the SDA documentation.

The Cisco Hyperlocation radio module provides the following:

- WSM or WSM2 radio module functions that are extended to:
  - 802.11ac
  - Wi-Fi Transmit
  - 20-MHz, 40-MHz, and 80-MHz channel bandwidth.
- Expanded location functionality:
  - Low-latency location optimized channel scanning

- 32-antenna angle of arrival (AoA); available only with the WSM2 module.

Note When using the WSM2 module (includes the WSM module and the antenna add-on), the accuracy of tracking the location of wireless clients can be as close as one meter.

Cisco Hyperlocation works in conjunction with Cisco Connected Mobile Experiences (CMX). Combining the Cisco Hyperlocation feature on Cisco Catalyst 9800 Series Wireless Controller with a CMX device allows you to achieve better location accuracy, which can result in delivering more targeted content to users. When you use CMX with Cisco CleanAir frequency scanning, it is simple to locate failed, lost, and even rogue beacons.

The Cisco Hyperlocation radio module with an integrated BLE radio allows transmission of Bluetooth Low Energy (BLE) broadcast messages by using up to 5 BLE transmitters. Cisco Catalyst 9800 Series Wireless Controller is used to configure transmission parameters such as interval for the beacons, universally unique identifier (UUID), and transmission power, per beacon globally for all the access points. Also, the controller can configure major, minor, and transmission power value of each AP to provide more beacon granularity.

Note The Cisco Hyperlocation feature must be enabled on the controller and CMX and CMX must be connected for BLE to work.

In the absence of a Cisco Hyperlocation radio module, Hyperlocation will still work in a modality named *Hyperlocation Local Mode*, which guarantees a slightly lower location accuracy in the range between five meters and seven meters. This is accomplished through CPU cycle stealing.

Using the controller, you can configure Cisco Hyperlocation for APs based on their profile.

Network Time Protocol Server

Cisco Hyperlocation requires the AP to be synchronized with regard to time. To achieve this, the controller sends network time protocol (NTP) information to the AP. The AP then uses the NTP server to synchronize its clock. Therefore, the AP needs connectivity to the NTP server.

APs can be geographically dispersed. Therefore, it is necessary to provide different NTP servers to different APs. This is achieved by allowing the configuration of NTP server information on a per AP profile basis. If NTP information is not configured on the AP profile, the controller uses one of the global NTP peers defined on its configuration or the management IP address is sent as the NTP server to be used if the controller is acting as an NTP server. If the NTP server is not available, Cisco Hyperlocation will be disabled.

Note In scale setup, the NTP server should be configured on the respective AP profiles, so that the APs and CA servers used for LSC provisioning are time synchronized. If the NTP server is not configured, a few APs would fail in LSC provisioning.

Bluetooth Low Energy Configuration

The BLE configuration is split into two parts: per-AP profile and per AP. The BLE feature can be configured partially from the AP profile (by default, the AP profile BLE configuration is applied) and partially per-AP (some or all the attributes are applied).

Table 8: BLE Configuration Details

Attribute	BLE Configuration Per AP Profile	BLE Configuration Per AP
Attributes with per-AP granularity (global for all the beacons)	• Interval • Advertised transmission power	• Interval • Advertised transmission power
Attributes with per-AP per0-beacon granularity	• Transmission power • UUID • Status	• Transmission power • UUID • Status • Major • Minor

Note The *default-ap-profile* BLE configuration can be considered the default BLE configuration because all the APs will join the *default-ap-profile* AP profile in case the other profiles are removed.

For more information about Cisco Hyperlocation, see the following documents:

- Cisco Hyperlocation Solution
- Cisco CMX Configuration Guide to enable Cisco Hyperlocation
- Cisco CMX Release Notes

Restrictions on Cisco Hyperlocation

- Currently, as Cisco Hyperlocation is an IPv4 solution, the Wireless Management, CMX, and the NTP server addresses must be in IPv4 format only.
- It is not possible to modify detection, trigger, and reset thresholds while Hyperlocation is in enabled state.
- Changes to the reset threshold are allowed for values in the range of zero to one less than the current threshold value. For example, if the current threshold reset value is 10, changes to the reset threshold are allowed for values in the range of 0 to 9.
- When Cisco Hyperlocation is in use on the Cisco Catalyst 9800 Series Wireless Controller in a non-Fabric deployment, CMX must be reachable through an SVI interface (VLAN). Deployments where CMX is reachable through an L3 port results in an error.

- In Fabric deployments, the wireless management interface (typically loopback interface) must not be in Fabric.
- It is not possible to set the wireless management interface to a loopback interface in non-Fabric deployments.

Configuring Cisco Hyperlocation (GUI)

Cisco Hyperlocation is a location solution that allows to track the location of wireless clients with the accuracy of one meter. Selecting this option disables all other fields in the screen, except NTP Server.

Procedure

Step 1 In the **Configuration > Tags & Profiles > AP Join** page, click **Add**.

The **Add AP Join Profile** dialog box appears.

Step 2 Under the **AP** > **Hyperlocation** tab, select the **Enable Hyperlocation** check box.

Step 3 In the **Detection Threshold (dBm)** field, enter a value to filter out packets with low RSSI. You must enter a value between –100 dBm and –50 dBm.

Step 4 In the **Trigger Threshold (cycles)** field, enter a value to set the number of scan cycles before sending a BAR to clients. You must enter a value between 0 and 99.

Step 5 In the **Reset Threshold is required** field, enter a value to reset value in scan cycles after trigger. You must enter a value between 0 and 99.

Step 6 Click **Save & Apply to Device**.

Configuring Cisco Hyperlocation (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile profile-name`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**[no] hyperlocation** **Example:** `Device(config-ap-profile)# [no] hyperlocation`	Enables Cisco Hyperlocation feature on all the supported APs that are associated with this AP profile.

	Command or Action	Purpose
		Use the **no** form of the command to disable the Cisco Hyperlocation feature.
Step 4	**[no] hyperlocation threshold detection** *value-in-dBm* **Example:** `Device(config-ap-profile)# [no] hyperlocation threshold detection -100`	Sets threshold to filter out packets with low RSSI. The **no** form of this command resets the threshold to its default value. Valid range is between –100 and –50.
Step 5	**[no] hyperlocation threshold reset** *value-btwn-0-99* **Example:** `Device(config-ap-profile)# [no] hyperlocation threshold reset 8`	Resets the value of scan cycles after a trigger. The **no** form of this command resets the threshold to its default value.
Step 6	**[no] hyperlocation threshold trigger** *value-btwn-1-100* **Example:** `Device(config-ap-profile)# [no] hyperlocation threshold trigger 10`	Sets the number of scan cycles before sending a block acknowledgment request (BAR) to clients. The **no** form of this command resets the threshold to its default value.
Step 7	**[no] ntp ip** *ip-address* **Example:** `Device(config-ap-profile)# [no] ntp ip 9.0.0.4`	Sets the IP address of the NTP server. The **no** form of this command removes the NTP server.

Configuring Hyperlocation BLE Beacon Parameters for AP (GUI)

Procedure

Step 1 In the **Configuration > Tags & Profiles > AP Join** page, click **Add**.

The **Add AP Join Profile** dialog box appears.

Step 2 Under the **AP** tab, click **BLE**.

Step 3 In the **Beacon Interval (Hz)** field, enter a value.

Step 4 In the **Advertised Attenuation Level (dBm)** field, enter a value.

Step 5 Select the check box against each ID and click **Reset**, if required.

Step 6 Optional, click an ID to edit the values of the following fields, and click **Save**.

- **Status**
- **Tx Power (dBm)**
- **UUID**

Step 7 Click **Save & Apply to Device**.

Configuring Hyperlocation BLE Beacon Parameters for AP (CLI)

Follow the procedure given below to configure hyperlocation BLE beacon parameters for an AP:

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **hyperlocation ble-beacon** *beacon-id* {**enable** | **major** *major-value* | **minor** *minor-value* | **txpwr** *value-in-dBm* | **uuid** *uuid-value* } **Example:** `Device# ap name test-ap hyperlocation ble-beacon 3 major 65535`	Configures Hyperlocation and related parameters for an AP, and the specified beacon ID: • **enable**—Enables BLE beacon on the AP. • **major** *major-value*—Configures BLE beacon's major parameter. Valid value is between 0 and 65535; the default value is 0. • **minor** *minor-value*—Configures BLE beacon's minor parameter. Valid value is between 0 and 65535; the default value is 0. • **txpwr** *value-in-dBm*—Configures BLE beacon attenuation level. Valid value is between –52 dBm and 0 dBm. • **uuid** *uuid-value*—Configures a UUID.
Step 2	**ap name** *ap-name* **hyperlocation ble-beacon advpwr** *value-in-dBm* **Example:** `Device# ap name test-ap hyperlocation ble-beacon advpwr 90`	Configures BLE beacon's advertised attenuation level for an AP. The valid range for *value-in-dBm* is between –40 dBm and –100 dBm; the default value is –59 dBm (all values must be entered as positive integers).

Configuring Hyperlocation BLE Beacon Parameters (CLI)

Before you begin

For Hyperlocation BLE to be enabled, CMX must be fully joined and enabled for Hyperlocation.

Procedure

	Command or Action	Purpose
Step 1	**ap profile** *profile-name* **Example:** `Device(config)# ap profile profile-name`	Enables configuration for all the APs that are associated with the specified AP profile name.
Step 2	**hyperlocation ble-beacon** *beacon-id* **Example:** `Device(config-ap-profile)# hyperlocation ble-beacon 3`	Specifies the BLE beacon parameters and enters BLE configuration mode.
Step 3	**enabled** **Example:** `Device(config-halo-ble)# enabled`	Enables BLE for the beacon ID specified.
Step 4	**exit** **Example:** `Device(config-halo-ble)# exit`	Returns to AP profile configuration mode.
Step 5	**hyperlocation ble-beacon interval** *value-in-hertz* **Example:** `Device(config-ap-profile)# hyperlocation ble-beacon interval 1`	Configures the BLE beacon interval as 1 Hz for the selected profile.
Step 6	**hyperlocation ble-beacon advpwr** *value-in-dBm* **Example:** `Device(config-ap-profile)# hyperlocation ble-beacon advpwr 40`	Configures the BLE beacon-advertised attenuation level. Valid range is between –40 dBm and –100 dBm. The default value is –59 dBm.

Verifying Cisco Hyperlocation

To display the hyperlocation status values and parameters for all the AP profiles, use the following command:

```
Device# show ap hyperlocation summary

Profile Name: custom-profile

Hyperlocation operational status: Down
Reason: Hyperlocation is administratively disabled
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Disabled
Hyperlocation detection threshold (dBm): -100
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8


Profile Name: default-ap-profile
```

```
Hyperlocation operational status: Up
Reason: N/A
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -90
Hyperlocation trigger threshold: 22
Hyperlocation reset threshold: 8
```

To display both the overall and and the per-AP configuration values and operational status, use the following command:

```
Device# show ap hyperlocation detail

Profile Name: house24

Hyperlocation operational status: Up
 Reason: NTP server is not properly configured
Hyperlocation NTP server: 198.51.100.1
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -90
Hyperlocation trigger threshold: 8
Hyperlocation reset threshold: 7

AP Name                 Radio MAC         Method      CMX IP            AP Profile
-------------------------------------------------------------------------------------------
APe865.49d9.bfe0        e865.49ea.a4b0    WSM2+Ant    198.51.100.2        house24

APa89d.21b9.69d0        a89d.21b9.69d0    Local       198.51.100.3        house24

APe4aa.5d3f.d750        e4aa.5d5f.3630    WSM         198.51.100.4        house24
```

To display the overall (profile specific) configuration values and operational status for a given profile, use the following command:

```
Device# show ap profile profile-name hyperlocation summary

Profile Name: profile-name
Hyperlocation operational status: Up
   Reason: N/A
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -100
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8
```

To display both the overall (profile specific) and per-AP configuration values and operational status for a given profile, use the following command. The APs listed are only those APs that belong to the specified join profile.

```
Device# show ap profile profile-name hyperlocation detail

Profile Name: profile-name
Hyperlocation operational status: Up
 Reason: N/A
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -90
Hyperlocation trigger threshold: 8
Hyperlocation reset threshold: 7
```

```
AP Name                 Radio MAC         Method      CMX IP
-----------------------------------------------------------------
APf07f.0635.2d40        f07f.0635.2d40    WSM2+Ant    198.51.100.2
APf07f.0635.2d41        f07f.0635.2d41    Local       198.51.100.3
APf07f.0635.2d42        f07f.0635.2d42    WSM         198.51.100.4
```

To display configuration values for an AP profile, use the following command:

```
Device# show ap profile profile-name detailed

Hyperlocation :
  Admin State             : ENABLED
  PAK RSSI Threshold Detection: -100
  PAK RSSI Threshold Trigger  : 10
  PAK RSSI Threshold Reset    : 8
.
.
.
```

To display the Cisco CMXs that are correctly joined and used by hyperlocation, use the following command:

```
Device# show ap hyperlocation cmx summary

Hyperlocation-enabled CMXs

IP            Port Dest MAC        Egress src MAC Egress VLAN Ingress src MAC Join time

-------------------------------------------------------------------------------------------------
198.51.100.4  2003 aaaa.bbbb.cccc  aabb.ccdd.eeff 2           0000.0001.0001  12/14/18
09:27:14
```

To display the hyperlocation client statistics, use the following command:

```
Device# show platform hardware chassis active qfp
feature wireless wlclient cpp-client summary

Client Type Abbreviations:
  RG - REGULAR BL - BLE
  HL - HALO    LI - LWFL INT
Auth State Abbreviations:
  UK - UNKNOWN IP - LEARN IP IV - INVALID
  L3 - L3 AUTH RN - RUN
Mobility State Abbreviations:
  UK - UNKNOWN IN - INIT
  LC - LOCAL   AN - ANCHOR
  FR - FOREIGN MT - MTE
  IV - INVALID
EoGRE Abbreviations:
  N - NON EOGRE Y - EOGRE
 CPP IF_H     DPIDX      MAC Address    VLAN  CT  MCVL  AS  MS  E  WLAN POA
------------------------------------------------------------------------------
   0X32     0XF0000001  0000.0001.0001   9    HL   0    RN  LC  N       NULL
```

To display the interface handle value statistics, use the following command:

```
Device# show platform hardware chassis active
qfp feature wireless wlclient datapath cpp-if-handle 0x32 statistics start
```

To display the recorded flow, use the following command:

```
Device# show platform hardware chassis active
qfp feature wireless wlclient datapath cpp-if-handle 0X32 statistics

                   Pkts                Bytes
Rx                  26                 3628
```

To stop statistics capture, use the following command:

```
Device# show platform hardware chassis active
qfp feature wireless wlclient datapath cpp-if-handle 0x32 statistics stop
```

To view the APs requested by Cisco CMX with AP groups' support, use the following commands:

```
Device# show nmsp subscription group summary

CMX IP address: 198.51.100.4
  Groups subscribed by this CMX server:
  Group name: CMX_1198.51.100.4

Device# show nmsp subscription group detail ap-list CMX_198.51.100.1 198.51.100.1

CMX IP address: 198.51.100.1
CMX Group name: CMX_198.51.100.1
CMX Group AP MACs:
: aa:bb:cc:dd:ee:01 aa:bb:cc:dd:ee:02 aa:bb:cc:dd:ee:03 aa:bb:cc:dd:ee:03
```

Verifying Hyperlocation BLE Beacon Configuration

To verify the list of configured BLE beacons, use the following command:

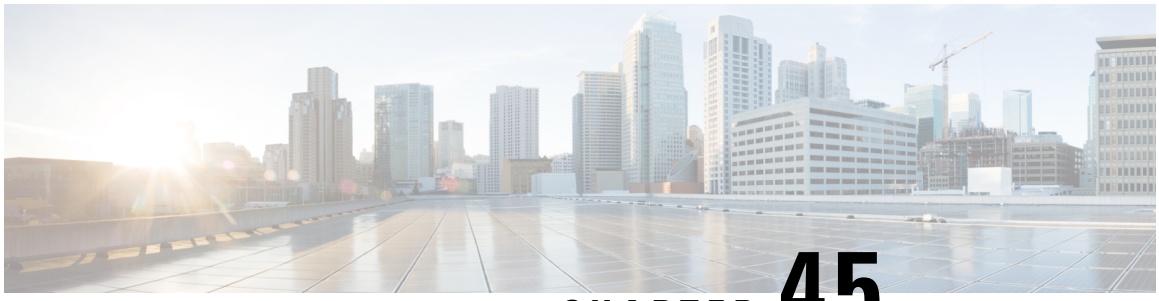
```
Device# show ap profile ap-profile-name hyperlocation ble-beacon
BLE Beacon interval (Hz): 1
BLE Beacon advertised attenuation value (dBm): -59

ID              UUID                 TX Power(dBm) Status
------------------------------------------------------------------------
0 ffffffff-aaaa-aaaa-aaaa-aaaaaaaaaaaa 0 Enabled
1 ffffffff-bbbb-bbbb-bbbb-bbbbbbbbbbbb 0 Enabled
2 ffffffff-gggg-gggg-gggg-gggggggggggg 0 Enabled
3 ffffffff-dddd-dddd-dddd-dddddddddddd 0 Enabled
4 ffffffff-eeee-eeee-eeee-eeeeeeeeeeee 0 Enabled
```

Verifying Hyperlocation BLE Beacon Configuration for AP

To verify the Hyperlocation BLE Beacon configuration for an AP, use the following command:

```
Device# show ap name test-ap hyperlocation ble-beacon
BLE Beacon interval (Hz): 1
BLE Beacon advertised attenuation value (dBm): -60

ID Status UUID Major Minor TXPower(dBm)
```

```
------------------------------------------------------------------------------
0 Enabled 99999999-9999-9999-9999-999999999999 8 0 -0
1 Enabled bbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbbb 8 1 -0
2 Enabled 88888888-8888-8888-8888-888888888888 8 2 -0
3 Enabled dddddddd-dddd-dddd-dddd-dddddddddddd 8 3 -0
4 Enabled eeeeeeee-eeee-eeee-eeee-eeeeeeeeeeee 8 4 -0
```



CHAPTER 45

BLE Beacons in CiscoWave 2 Access Points

- Managing BLE Beacons in Cisco Wave 2 and 802.11ax Access Points, on page 359
- Monitoring BLE Management, on page 361

Managing BLE Beacons in Cisco Wave 2 and 802.11ax Access Points

The BLE Management feature supports both sending of beacons and listening to beacons from small battery-powered devices.

BLE beacons support the following profiles:

- iBeacon profile
- Eddystone-URL profile
- Eddystone-UID profile
- viBeacon (contains up to 5 iBeacons internally)

Bluetooth-enabled smartphones that are nearby can pick up the transmission from beacons and communicate with the back-end server to push advertisements or other information. The transmission power range is from –21 dBm to +5 dBm in increments of 3 dB. You can also configure the broadcast frequency in the range of 100 milliseconds to 10000 milliseconds.

The end-to-end solution comprises the following components:

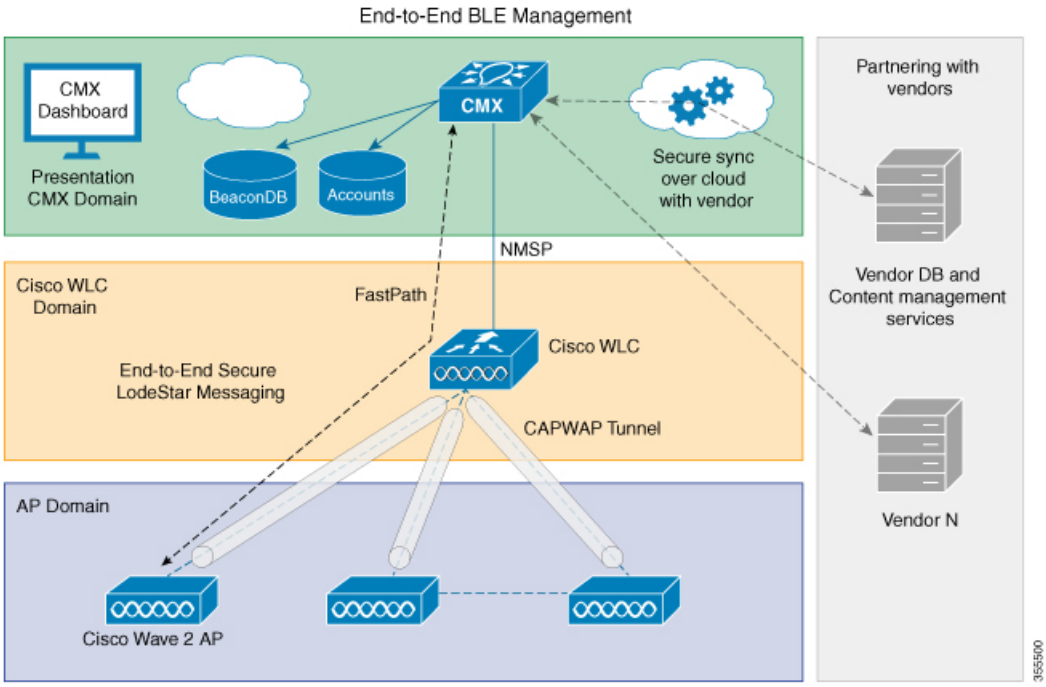
- Cisco Wave 2 or Catalyst 9100 series AP with BLE chip
- Cisco Catalyst 9800 Series Wireless Controller
- On-premise Cisco Connected Mobile Experiences (CMX)
- Cisco Digital Network Architecture (DNA) Spaces

Table 9: Feature Support in AP Models

AP Platform	SKU
Cisco Aironet 1542 Access Point	I

AP Platform	SKU
Cisco Aironet 1810 Access Point	W, T
Cisco Aironet 1815 Access Point	W, T
Cisco Aironet 1800 Access Point	I
Cisco Aironet 4800 Access Point	-

Figure 5: End-to-End BLE Management



Functional Role

An AP's BLE firmware that is running on an integrated radio can be configured to function as a nonconnectable broadcaster. The beacons are picked up by any other application running on a smartphone, or another Cisco AP, for internal processing. This broadcasting function is mutually exclusive, and no scan operations or other BLE management functions are in operation during this period.

In the Broadcaster role, the AP's BLE beacon supports different profiles. Profiles are different beaconing formats that have been approved by the Bluetooth Special Interest Group. Each profile has its own meaning and these profiles are mutually exclusive, that is, the firmware can only send one format at a time and not a mixed one.

The AP's BLE firmware supports the following beaconing profiles:

- iBeacon: This is Apple's iBeacon broadcast format. In this profile, you can configure the following broadcast data:
  - UUID (16 bytes value, which can uniquely identify an organization)
  - Major number (2 bytes value, which can identify a unique store of the organization)

- Minor number (2 bytes value, which can identify a particular product or section)

Typical use cases are iOS or Android apps that use Major, Minor, or UUID to show local store data to smartphone user, when they walk close to a Cisco Wave 2 or Catalyst AP.

- Eddystone UID: This is one of Google's BLE broadcasting formats, where Namespace and InstanceID are broadcast in the BLE beacon. In this profile, you can configure the following parameters:
  - Eddystone Namespace (10 bytes)
  - Eddystone InstanceID (6 bytes)
- Eddystone URL: This is another BLE broadcasting format used by Google, in which an AP broadcasts the configured URL for a broadcast data. Any smartphone app such as Android's physical web or the latest Google Chrome plugin can pick up the beacon and render the URL into a web page without the need for users to install any apps. Note that the physical web is yet to be standardized as a plugin to all the smartphone Chrome or web browsers. In this profile, you can configure URL strings, which must start with one of the following prefixes:
  - http://www.
  - https://www.
  - http://
  - https://
- viBeacon—Up to five AP beacons can be configured. These beacons are compatible only with Cisco Aironet 3700 Series AP.

  All of these profiles can be configured to transmit at a particular Transmit (Tx) power –21 dBm to +5 dBm and advertising interval (100 ms to 10000 ms). This Tx power is common to the iBeacon, Eddystone UID, and Eddystone URL profiles.

Note All of these profiles can be configured on Cisco DNA Spaces.

Monitoring BLE Management

To view the list of joined APs that support the BLE Management feature along with the BLE details for each AP, use the following command:

```
Device# show ap ble summary
AP Name                          Interface             Status      CMX IP
-------------------------------------------------------------------------------
AP4001.7AB2.C39A                 Integrated            Open        10.1.2.3
AP4001.7AB2.C39B                 Integrated            Closed      10.1.2.4
```

Note The BLE Management feature is enabled and APs are displayed only when CMX is registered with the controller, and BLE is enabled on CMX.

To view the list of all the CMXs registered for the BLE Management feature and their global values for BLE, use the following command:

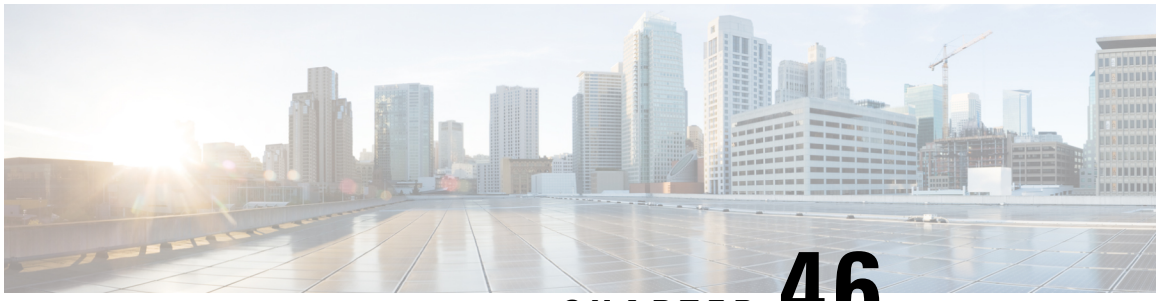
```
Device# show ap ble cmx summary
CMX IP: 10.1.2.3
-----------------------
  BLE administrative status: Up
  BLE operational status: Up
  Scanning interval: 12

CMX IP: 10.1.2.4
-----------------------
  BLE administrative status: Down
  BLE operational status: Down
   Reason: BLE is administratively down
  Scanning interval: 0

CMX IP: 10.1.2.5
------------------
BLE administrative status: Up
BLE operational status: Down
 Reason: CMX is not subscribed to AP Monitor and RSSI services, or NMSP connection is down
Scanning interval: 10
```

To view the BLE management feature-related global values for a specific CMX along with all the APs associated to that CMX, use the following command:

```
Device# show ap ble cmx detail ip 10.1.2.3
BLE administrative status: Up
BLE operational status: Up
Scanning interval: 10

  AP Name                          Interface             Status
  ------------------------------------------------------------------
  AP4001.7AB2.C39A                 Integrated             Open
```

To view the global values for BLE and BLE details for a specific AP, use the following command:

```
Device# show ap name AP4001.7AB2.C39A ble detail

CMX IP: 10.1.2.4
-----------------------
  BLE administrative status: Up
  BLE operational status: Up
  Scanning interval: 10

  AP Name                          Interface             Status
  ------------------------------------------------------------------
  AP4001.7AB2.C39B                 Integrated             Open
```



CHAPTER 46

Cisco Connected Mobile Experiences Cloud

Cisco Connected Mobile Experiences (CMX) communicates with the Cisco wireless controller using the Network Mobility Services Protocol (NMSP), which runs over a connection-oriented (TLS) transport. This transport provides a secure 2-way connectivity and is convenient when both the controller and CMX are on-premise and there is direct IP connectivity between them.

Cisco CMX Cloud is a cloud-delivered version of the on-premise CMX. To access Cisco CMX Cloud services, HTTPS is used as a transport protocol.

- Configuring Cisco CMX Cloud , on page 363
- Verifying Cisco CMX Cloud Configuration, on page 364

Configuring Cisco CMX Cloud

Follow the procedure given below to configure CMX Cloud:

Before you begin

- **Configure DNS**—To resolve fully qualified domain names used by NMSP cloud-services, configure a **DNS** using the **ip name-server** *server_address* configuration command as shown in Step 2.
- **Import 3rd party root CAs**—The controller verifies the peer and the host based on the certificate that is sent by the CMX when a connection is established. However, root CAs are not preinstalled on the controller. You have to import a set of root CAs trusted by Cisco to the trustpool of the crypto PKI by using the **crypto pki trustpool import url <url>** configuration command as shown in Step 3.
- A successful registration to Cisco Spaces is required to enable **server url** and **server token** parameters configuration which is needed to complete this setup.

Procedure

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

	Command or Action	Purpose
Step 2	**ip name-server** *namesvr-ip-addr* **Example:** `Device(config)#ip name-server 10.10.10.205`	Configures the DNS on the controller to resolve the FQDN names used by the NMSP cloud-services.
Step 3	**crypto pki trustpool import url** *url* **Example:** `Device(config)#crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b`	Imports the 3rd party root CA. The controller verifies the peer using the imported certificate.
Step 4	**[no] nmsp cloud-services server url** *url* **Example:** `Device(config)# nmsp cloud-services server url https://cisco.com`	Configures the URL used for cloud services. Use the **no** form of the command to delete the server url from the configuration.
Step 5	**[no] nmsp cloud-services server token** *token* **Example:** `Device(config)# nmsp cloud-services server token test`	Configures the authentication token for the NMSP cloud service. Use the **no** form of the command to delete the server token from the configuration.
Step 6	**[no] nmsp cloud-services http-proxy** *proxy-server port* **Example:** `Device(config)# nmsp cloud-services http-proxy 10.0.0.1 10`	(Optional) Configures HTTP proxy details for the NMSP cloud service. Use the **no** form of the command to disable the use of a HTTP proxy.
Step 7	**[no] nmsp cloud-services enable** **Example:** `Device(config)# nmsp cloud-services enable`	Enables NMSP cloud services. Use the **no** form of the command to disable the feature.

Verifying Cisco CMX Cloud Configuration

Use the following commands to verify the CMX Cloud configuration.

To view the status of active NMSP connections, use the following command:

```
Device# show nmsp status

MSE IP Address   Tx Echo Resp  Rx Echo Req   Tx Data     Rx Data   Transport
------------------------------------------------------------------------------
9.9.71.78        0             0             1           1         TLS
64.103.36.133    0             0             1230        2391      HTTPs
```

To view the NMSP cloud service status, use the following command:

```
Device# show nmsp cloud-services summary

CMX Cloud-Services Status
```

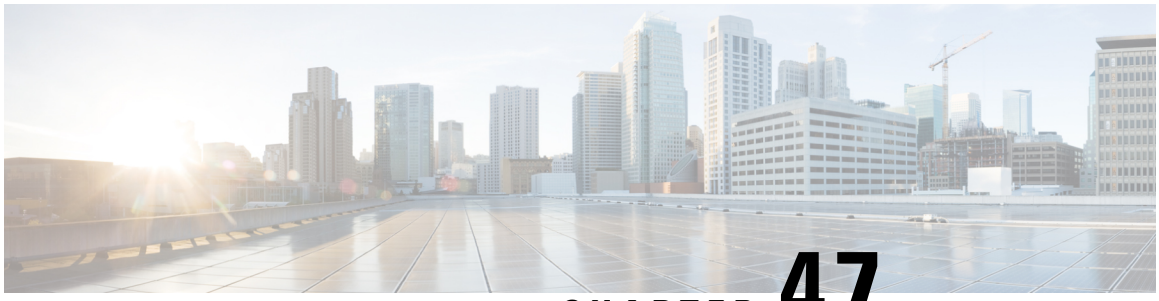
```
-------------------------

   Server:                                 https://yenth8.cmxcisco.com
   IP Address:                             64.103.36.133
   Cmx Service:                            Enabled
   Connectivity:                           https: UP
   Service Status:                         Active
   Last Request Status:                    HTTP/1.1 200 OK
   Heartbeat Status:                       OK
```

To view the NMSP cloud service statistics, use the following command:

```
Device# show nmsp cloud-services statistics

CMX Cloud-Services Statistics
-----------------------------

   Tx DataFrames:                           3213
   Rx DataFrames:                           1606
   Tx HeartBeat Req:                       31785
   Heartbeat Timeout:                          0
   Rx Subscr Req:                           2868
   Tx DataBytes:                           10069
   Rx DataBytes:                           37752
   Tx HeartBeat Fail:                          2
   Tx Data Fail:                               0
   Tx Conn Fail:                               0
```

To view the mobility services summary, use the following command:

```
Device# show nmsp subscription summary

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
```



CHAPTER 47

EDCA Parameters

- Enhanced Distributed Channel Access Parameters, on page 367
- Configuring EDCA Parameters (GUI), on page 367
- Configuring EDCA Parameters (CLI), on page 368

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 **Configuration > Radio Configurations > Parameters**. Using this page, you can configure global parameters for 802.11a/n/ac (5 GHz) and 802.11b/g/n (2.4 GHz) radios.

Note You cannot configure or modify parameters, if the radio network is enabled. Disable the network status on the Configuration > Radio Configurations > Network page before you proceed.

Step 2 In the **EDCA Parameters** section, choose an EDCA profile from the **EDCA Profile** drop-down list. Enhanced Distributed Channel Access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic.

Step 3 For 802.11a/n/ac (5 GHZ) radios, in the (DFS 802.11h) section, enter the local power constraint. You cannot configure power constraint if the DTPC Support check box on the **Configure > Radio Configurations > Network** page is checked. The valid range is between 0 dBm and 30 dBm.

Step 4 Check the **Channel Switch Announcement Mode** check box, if you want the AP to announce when it is switching to a new channel and the new channel number. The default value is disabled.

Step 5 Check the **Smart DFS** check box to enable Dynamic Frequency Selection (DFS) and avoid interference with the radar signals.

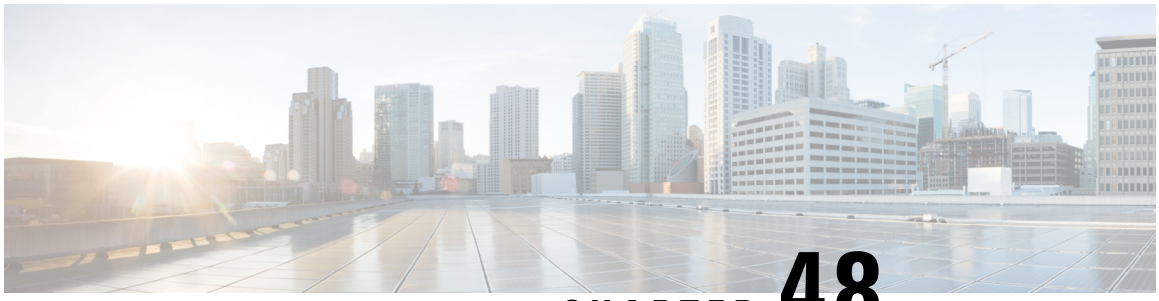
Step 6 Click **Apply**.

Configuring EDCA Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {5ghz | 24ghz } shutdown** **Example:** `Device(config)# ap dot11 5ghz shutdown`	Disables the radio network.
Step 3	**ap dot11 {5ghz | 24ghz} edca-parameters {custom-voice | fastlane | optimized-video-voice | optimized-voice | svp-voice | wmm-default}** **Example:** `Device(config)# ap dot11 5ghz edca-parameters optimized-voice`	Enables specific EDCA parameters for the 802.11a or 802.11b/g network. **Note** The **custom-voice** option is not supported for Cisco Catalyst 9800 Series Wireless Controller. • **custom-voice**: Enables custom voice parameters for the 802.11a or 802.11b/g network. • **fastlane**: Enables the fastlane parameters for the 802.11a or 802.11b/g network. • **optimized-video-voice**: Enables EDCA voice-optimized and video-optimized parameters for the 802.11a or 802.11b/g network. Choose this option when both voice and video services are deployed on your network. • **optimized-voice**: Enables non-SpectraLink voice-optimized profile parameters for the 802.11a or 802.11b/g network. Choose this option when voice services other than SpectraLink are deployed on your network. • **svp-voice**: Enables SpectraLink voice-priority parameters for the 802.11a or 802.11b/g network. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.

	Command or Action	Purpose
		• **wmm-default**: Enables the Wi-Fi Multimedia (WMM) default parameters for the 802.11a or 802.11b/g network. This is the default option. Choose this option when voice or video services are not deployed on your network.
Step 4	**no ap dot11 {5ghz | 24ghz} shutdown** **Example:** `Device(config)# no ap dot11 5ghz shutdown`	Re-enables the radio network.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 6	**show ap dot11 {5ghz | 24ghz} network** **Example:** `Device# show ap dot11 5ghz network`	Displays the current status of MAC optimization for voice.



CHAPTER 48

802.11 parameters and Band Selection

- Information About Configuring Band Selection, 802.11 Bands, and Parameters, on page 371
- Restrictions for Band Selection, 802.11 Bands, and Parameters, on page 373
- How to Configure 802.11 Bands and Parameters, on page 373
- Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters, on page 383
- Configuration Examples for Band Selection, 802.11 Bands, and Parameters, on page 388

Information About Configuring Band Selection, 802.11 Bands, and Parameters

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 device.

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.

Note You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.

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.

802.11 Bands

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

This section contains the following subsections:

802.11n Parameters

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

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

Note 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.

802.11h Parameters

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

Restrictions for Band Selection, 802.11 Bands, and Parameters

- Band selection-enabled WLANs do not support time-sensitive applications such as voice and video because of roaming delays.
- Band selection is supported only on Cisco Wave 2 and 802.11ax APs.

  For more information about support on specific APs, see https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html.
- Band selection operates only on APs that are connected to a controller. A FlexConnect AP 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 AP, and it only runs on an AP when both the 2.4-GHz and 5-GHz radios are up and running.
- It is not possible to enable or disable band selection and client load balancing globally through the controller GUI or CLI. You can, however, enable or disable band selection and client load balancing for a particular WLAN. Band selection and client load balancing are enabled globally by default.

How to Configure 802.11 Bands and Parameters

Configuring Band Selection (GUI)

Before you begin

Ensure that you have configured an AP Join Profile prior to configuring the primary and backup controllers.

Procedure

Step 1 Choose **Configuration** > **Wireless Advanced** > **Band Select**.

Step 2 In the **Cycle Count** field, enter a value between 1 and 10. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

Step 3 In the **Cycle Threshold (milliseconds)** field, 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. The default cycle threshold is 200 milliseconds.

Step 4 In the **Age Out Suppression (seconds)** field, 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)** field, 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 50 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 6 In the Client RSSI (dbm) field, enter a value between -90 to -20. This is the average of the client packets received.

Step 7 In the Client Mid RSSI (dbm) field, enter a value between -90 to -20. This the instantaneous RSSI value of the probe packets.

Step 8 On the **AP Join Profile** page, click the AP Join Profile name.

Step 9 Click **Apply**.

Configuring Band Selection (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless client band-select cycle-count** *cycle_count* **Example:** `Device(config)# wireless client band-select cycle-count 3`	Sets the probe cycle count for band select. Valid range is between 1 and 10.
Step 3	**wireless client band-select cycle-threshold** *milliseconds* **Example:** `Device(config)# wireless client band-select cycle-threshold 5000`	Sets the time threshold for a new scanning cycle period. Valid range is between 1 and 1000.
Step 4	**wireless client band-select expire suppression** *seconds* **Example:** `Device(config)# wireless client band-select expire suppression 100`	Sets the suppression expire to the band select. Valid range is between 10 and 200.
Step 5	**wireless client band-select expire dual-band** *seconds* **Example:** `Device(config)# wireless client band-select expire dual-band 100`	Sets the dual band expire. Valid range is between 10 and 300.
Step 6	**wireless client band-select client-rssi** *client_rssi* **Example:** `Device(config)# wireless client band-select client-rssi 40`	Sets the client RSSI threshold. Valid range is between 20 and 90.
Step 7	**wlan** *wlan_profile_name wlan_ID SSID_network_name* **band-select** **Example:**	Configures band selection on specific WLANs. Valid range is between 1 and 512. You can enter up to 32 alphanumeric characters for *SSID_network_name* parameter.

	Command or Action	Purpose
	`Device(config)# wlan wlan1 25 ssid12` `Device(config-wlan)# band-select`	

Configuring the 802.11 Bands (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **Network**.

Step 2 Click either **5 GHz Band** or **2.4 GHz Band**.

Step 3 Uncheck the **Network Status** check box to disable the network in order to be able to configure the network parameters.

Step 4 In the **Beacon Interval** field, enter the rate at which the SSID is broadcast by the APs, from 100 to 600 milliseconds. The default is 100 milliseconds.

Step 5 For 802.11b/g/n (2.4-GHz) radios, to enable short preamble on the radio, check the **Short Preamble** check box. A short preamble improves throughput performance.

Step 6 In the **Fragmentation Threshold (in bytes)** field, enter a value between 256 to 2346 bytes. Packets larger than the size you specify here will be fragmented.

Step 7 Check the **DTPC Support** check box to advertise the transmit power level of the radio in the beacons and the probe responses. 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. You cannot configure a power constraint value on your 802.11a/n/ac (5-GHz) radio network if the **DTPC Support** check box is checked.

Step 8 Click **Apply**.

Step 9 In the **CCX Location Measurement** section, check the **Mode** check box to globally enable CCX radio management for the network. This parameter causes the APs connected to this device to issue broadcast radio measurement requests to clients running CCX v2 or later releases.

Step 10 In the **Interval** field, enter a value to specify how often the APs must issue broadcast radio measurement requests.

Step 11 Click **Apply**.

Step 12 In the **Data Rates** section, choose a value to specify the rates at which data can be transmitted between the access point and the client:

- Mandatory: Clients must support this data rate in order to associate to an access point on the controller embedded wireless controller.
- Supported: Any associated clients that support this data rate may communicate with the access point using that rate.
- Disabled: The clients specify the data rates used for communication.

Step 13 Click **Apply**.

Step 14 Save the configuration.

Configuring the 802.11 Bands (CLI)

Follow the procedure given below to configure 802.11 bands and parameters:

Procedure

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

Step 6	**[no] ap dot11** {**5ghz** | **24ghz** } **dtpc**
	Example:
	`Device(config)# ap dot11 5ghz dtpc`
	`Device(config)# no ap dot11 24ghz dtpc`
		Enables access points to advertise their channels and transmit the power levels in beacons and probe responses.
		The default value is enabled. Client devices using dynamic transmit power control (DTPC) receive the channel-level and power-level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan can rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.

	Command or Action	Purpose
		The **no** form of the command disables the DTPC setting.
Step 7	**wireless client association limit** *number* **interval** *milliseconds* **Example:** `Device(config)# wireless client association limit 50 interval 1000`	Specifies the maximum allowed clients that can be configured. You can configure the maximum number of association requests on a single access point slot at a given interval. The range of association limit that you can configure is from 1 to 100. The association request limit interval is measured between 100 to 10000 milliseconds.
Step 8	**ap dot11 {5ghz | 24ghz} rate** *rate* {**disable** | **mandatory** | **supported**} **Example:** `Device(config)# ap dot11 5ghz rate 36 mandatory`	Specifies the rate at which data can be transmitted between the controller embedded wireless controller and the client. • **disable**: Defines that the clients specify the data rates used for communication. • **mandatory**: Defines that the clients support this data rate in order to associate to an access point on the controller embedded wireless controller. • **supported**: Any associated clients that support this data rate can communicate with the access point using that rate. However, the clients are not required to use this rate in order to associate. • *rate*: Specifies the rate at which data is transmitted. For the 802.11a and 802.11b bands, the data is transmitted at the rate of 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps.
Step 9	**no ap dot11 5ghz shutdown** **Example:** `Device(config)# no ap dot11 5ghz shutdown`	Enables the 802.11a band. **Note** The default value is enabled.
Step 10	**no ap dot11 24ghz shutdown** **Example:** `Device(config)# no ap dot11 24ghz shutdown`	Enables the 802.11b band. **Note** The default value is enabled.
Step 11	**ap dot11 24ghz dot11g** **Example:**	Enables or disables 802.11g network support.

	Command or Action	Purpose
	`Device(config)# ap dot11 24ghz dot11g`	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 12	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring a Band-Select RF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Advanced**.

Step 2 In the **Band Select** tab, enter a value between 1 and 10 in the **Cycle Count** field. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

Step 3 In the **Cycle Threshold** field, 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. The default cycle threshold is 200 milliseconds.

Step 4 In the **Age Out Suppression** field, 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** field, 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 50 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 6 In the **Client RSSI** field, enter a value between -90 dBm and -20 dBm. This is the minimum RSSI for a client to respond to a probe.

Step 7 In the **Client Mid RSSI** field, enter a value between –20 dBm 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.

Step 8 Click **Apply**.

Configuring a Band-Select RF Profile (CLI)

Procedure

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

	Command or Action	Purpose
Step 2	**ap dot11 24ghz rf-profile** *rf-profile* **Example:** `Device(config)# ap dot11 24ghz rf-profile test1`	Configures the RF profile name and enters RF profile configuration mode.
Step 3	**band-select client** {**mid-rssi** | **rssi** }*dbm* **Example:** `Device(config-rf-profile)# band-select client rssi -90`	Sets the band-select client threshold.
Step 4	**band-select cycle** {**count** | **threshold**}*count* **Example:** `Device(config-rf-profile)# band-select cycle count 10`	Sets the band-select cycle parameters.
Step 5	**band-select expire** {**dual-band** | **suppression** }*time* **Example:** `Device(config-rf-profile)# band-select expire dual-band 100`	Configures the RF profile's band-select expiry time.
Step 6	**band-select probe-response** **Example:** `Device(config-rf-profile)# band-select probe-response`	Enables the RF profile's band-select probe response.

Configuring 802.11n Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF**.

Step 2 Click **Add** to view the **Add RF Profile** window.

Step 3 In the **802.11** tab, proceed as follows:

a) Choose the required operational rates.

b) Select the required **802.11n MCS Rates** by checking the corresponding check boxes.

Step 4 Click **Save & Apply to Device**.

Configuring 802.11n Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {5ghz | 24ghz} dot11n** **Example:** `Device(config)# ap dot11 5ghz dot11n`	Enables 802.11n support on the network. The **no** form of this command disables the 802.11n support on the network.
Step 3	**ap dot11 {5ghz | 24ghz} dot11n mcs tx** *rtu* **Example:** `Device(config)# ap dot11 5ghz dot11n mcs tx 20`	Specifies the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. *rtu*-The valid range is between 0 and 23. The **no** form of this command disables the MCS rates that are configured.

Step 4	**wlan***wlan_profile_name wlan_ID SSID_network_name* **wmm require**
	Example:
	`Device(config)# wlan wlan1 25 ssid12`
	`Device(config-wlan)# wmm require`
		Enables WMM on the WLAN and uses the 802.11n data rates that you configured.
		The **require** keyword requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

Step 5	**ap dot11 {5ghz | 24ghz} shutdown** **Example:** `Device(config)# ap dot11 5ghz shutdown`	Disables the network.
Step 6	**{ap | no ap} dot11 {5ghz | 24 ghz} dot11n a-mpdu tx priority {all | 0-7}** **Example:** `Device(config)# ap dot11 5ghz dot11n a-mpdu tx priority all`	Specifies the aggregation method used for 802.11n packets. Aggregation is the process of grouping packet data frames together, rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). Both A-MPDU and A-MSDU are performed in the software. You can specify the aggregation method for various types of traffic from the access point to the clients. The list defines the priority levels (0-7) assigned per traffic type. • 0—Best effort

	Command or Action	Purpose
		• 1—Background • 2—Spare • 3—Excellent effort • 4—Controlled load • 5—Video, less than 100-ms latency and jitter • 6—Voice, less than 100-ms latency and jitter • 7—Network control You can configure each priority level independently, or you can use the all the parameters to configure all the priority levels at once. You can configure priority levels so that the traffic uses either A-MPDU transmission or A-MSDU transmission. • When you use the **ap** command along with the other options, the traffic associated with that priority level uses A-MPDU transmission. • When you use the **no ap** command along with the other options, the traffic associated with that priority level uses A-MSDU transmission. Configure the priority levels to match the aggregation method used by the clients. By default, A-MPDU is enabled for priority level 0, 4, and 5, and the rest are disabled. By default, A-MPDU is enabled for all priorities except 6 and 7.
Step 7	**no ap dot11 {5ghz | 24ghz} shutdown** **Example:** `Device(config)# no ap dot11 5ghz shutdown`	Re-enables the network.
Step 8	**ap dot11 {5ghz | 24ghz} dot11n guard-interval {any | long}** **Example:** `Device(config)# ap dot11 5ghz dot11n guard-interval long`	Configures the guard interval for the network.

	Command or Action	Purpose
Step 9	**ap dot11 {5ghz | 24ghz} dot11n rifs rx** **Example:** `Device(config)# ap dot11 5ghz dot11n rifs rx`	Configures the Reduced Interframe Space (RIFS) for the network.
Step 10	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring 802.11h Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap dot11 5ghz shutdown** **Example:** `Device(config)# ap dot11 5ghz shutdown`	Disables the 802.11 network.
Step 2	**{ap | no ap} dot11 5ghz channelswitch mode** *switch_mode* **Example:** `Device(config)# ap dot11 5ghz channelswitch mode 0`	Enables or disables the access point to announce when it is switching to a new channel. *switch_mode*--Enter 0 or 1 to specify whether transmissions are restricted until the actual channel switch (**0**) or are not restricted (**1**). The default value is disabled.
Step 3	**ap dot11 5ghz power-constraint** *value* **Example:** `Device(config)# ap dot11 5ghz power-constraint 200`	Configures the 802.11h power constraint value in dB. The valid range is from 0 to 255. The default value is 3.
Step 4	**no ap dot11 5ghz shutdown** **Example:** `Device(config)# no ap dot11 5ghz shutdown`	Re-enables the 802.11a network.

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

Verifying Configuration Settings Using Band Selection and 802.11 Bands Commands

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

Table 10: Monitoring Configuration Settings Using Band Selection and 802.11 Band Commands

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

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

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

802.11a Operational Rates
  802.11a 6M : Mandatory
  802.11a 9M : Supported
  802.11a 12M : Mandatory
  802.11a 18M : Supported
  802.11a 24M : Mandatory
  802.11a 36M : Supported
  802.11a 48M : Supported
  802.11a 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
```

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

```
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

Example: Viewing the Configuration Settings for the 2.4-GHz Band

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

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

```
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
  Priority 6 : Disabled
    Priority 7 : Disabled
  Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable Mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 11
Default Tx Power Level : 1
DTPC Status : true
Call Admission Limit : 105
G711 CU Quantum : 15
ED Threshold : -50
Fragmentation Threshold : 2346
PBCC Mandatory : Disabled
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
RTS Threshold : 2347
Short Preamble Mandatory : Enabled
Short Retry Limit : 7
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

Example: Viewing the status of 802.11h Parameters

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

Example: Verifying the Band-Selection Settings

The following example displays a band-select configuration:

```
Device# show wireless band-select

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

The following example displays an AP RF profile details:

```
Device# show ap rf-profile name vid detail

Description                          :
RF Profile Name                      : vid
Band                                 : 2.4 GHz
802.11n client only                  : Disabled
Transmit Power Threshold v1          : -70 dBm
Min Transmit Power                   : -10 dBm
Max Transmit Power                   : 30 dBm
Operational Rates
  802.11b 1M Rate                    : Mandatory
  802.11b 2M Rate                    : Mandatory
  802.11b 5.5M Rate                  : Mandatory
  802.11b 11M Rate                   : Mandatory
  802.11b 6M Rate                    : Supported
  802.11b 9M Rate                    : Supported
  802.11b 12M Rate                   : Supported
  802.11b 18M Rate                   : Supported
  802.11b 24M Rate                   : Supported
  802.11b 36M Rate                   : Supported
  802.11b 48M Rate                   : Supported
  802.11b 54M Rate                   : Supported
Max Clients                          : 200
Trap Threshold
  Clients                            : 12 clients
  Interference                       : 10%
  Noise                              : -80 dBm
  Utilization                        : 10%
Multicast Data Rate                  : auto
Rx SOP Threshold                     : auto
Band Select
  Probe Response                     :  Disabled
  Cycle Count                        :  2 cycles
  Cycle Threshold                    :  200 milliseconds
  Expire Suppression                 :  20 seconds
  Expire Dual Band                   :  60 seconds
  Client RSSI                        :  -80 dBm
  Client Mid RSSI                    :  -80 dBm
High Speed Roam
  hsr mode                           :  Disabled
  hsr neighbor timeout               :  5
Load Balancing
  Window                             :  5 clients
  Denial                             :  3 count
Coverage Data
  Data                               : -62 dBm
  Voice                              : -80 dBm
```

```
  Minimum Client Level            : 12 clients
  Exception Level                 : 48%
DCA Channel List                  : 1,6,11
Unused Channel List               : 2,3,4,5,7,8,9,10
DCA Foreign AP Contribution       : Enabled
802.11n MCS Rates
  MCS  0                          : Enabled
  MCS  1                          : Enabled
  MCS  2                          : Enabled
  MCS  3                          : Enabled
  MCS  4                          : Enabled
  MCS  5                          : Enabled
  MCS  6                          : Enabled
  MCS  7                          : Enabled
  MCS  8                          : Enabled
  MCS  9                          : Enabled
  MCS 10                          : Enabled
  MCS 11                          : Enabled
  MCS 12                          : Enabled
  MCS 13                          : Enabled
  MCS 14                          : Enabled
  MCS 15                          : Enabled
  MCS 16                          : Enabled
  MCS 17                          : Enabled
  MCS 18                          : Enabled
  MCS 19                          : Enabled
  MCS 20                          : Enabled
  MCS 21                          : Enabled
  MCS 22                          : Enabled
  MCS 23                          : Enabled
  MCS 24                          : Enabled
  MCS 25                          : Enabled
  MCS 26                          : Enabled
  MCS 27                          : Enabled
  MCS 28                          : Enabled
  MCS 29                          : Enabled
  MCS 30                          : Enabled
  MCS 31                          : Enabled
State                             : Up
Client Network  Preference        : connectivity
```

Configuration Examples for Band Selection, 802.11 Bands, and Parameters

Examples: Band Selection Configuration

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

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

This example shows how to set the suppression expiry time to the band select:

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

This example shows how to set the dual-band expiry time for the band select:

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

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

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

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

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

Examples: 802.11 Bands Configuration

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

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

Examples: 802.11n Configuration

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

```
Device# configure terminal
Device(config)# ap dot11 5ghz dot11n
Device(config)# ap dot11 5ghz dot11n mcs tx 20
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# wmm require\
Device(config-wlan)# exit
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz dot11n a-mpdu tx priority all
```

```
Device(config)# no ap dot11 5ghz shutdown
Device(config)#exit
```

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

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

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

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

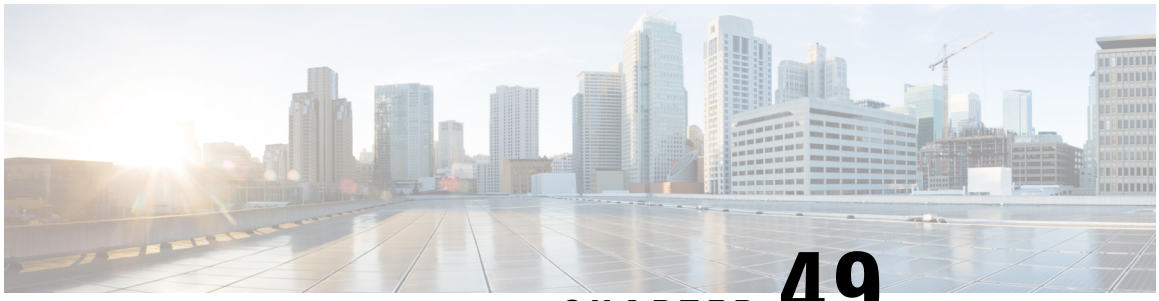
Examples: 802.11h Configuration

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

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

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

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



CHAPTER 49

Predownloading an Image to an Access Point

- Information About Predownloading an Image to an Access Point, on page 391
- Restrictions for Predownloading an Image to an Access Point, on page 391
- Predownloading an Image to Access Points (CLI), on page 392
- Monitoring the Access Point Predownload Process, on page 393

Information About Predownloading an Image to an Access Point

To minimize network outages, download an upgrade image to an access point from the device without resetting the access point or losing network connectivity. Previously, you could download an upgrade image to the device and reset it, causing the access point to go into discovery mode. After the access point discovered the controller with the new image, the access point would download the new image, reset it, go into discovery mode, and rejoin the device.

You can now download the upgrade image to the controller. When the controller is up with the upgrade image, the AP joins the controller and moves to Registered state, because the AP image has been predownloaded to the AP.

Restrictions for Predownloading an Image to an Access Point

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

- The maximum number of concurrent predownloads are limited to 100 per wncd instance (25 for 9800-L) in the controller. However, the predownloads are triggered in sets of 16 per wncd instance at the start, and is repeated every 60 seconds.
- Access points with 16-MB total available memory may not have enough free memory to download an upgrade image and may automatically delete crash information files, radio files, and backup images, if any, to free up space. However, this limitation does not affect the predownload process because the predownload image replaces backup image, if any, on the access point.
- All of the primary, secondary, and tertiary controllers should run the same images. Otherwise, the feature will not be effective.
- At the time of reset, you must make sure that all of the access points have downloaded the image.
- An access point can store only 2 software images.

- The Cisco Wave 1 APs may download the image twice while moving from Cisco AireOS Release 8.3 to Cisco IOS XE Gibraltar 16.10.1. This increases the AP downtime during migration.
- The **show ap image** command displays cumulative statistics regarding the AP images in the controller. We recommend that you clear the statistics using the **clear ap predownload statistics** command, before using the show ap image command, to ensure that correct data is displayed.
- AP image predownload will not work if you upgrade the controller from the web UI
- Cisco Catalyst 9800-CL Wireless Controller supports only self-signed certificates and does not support Cisco certificates. When you move the access points between Cisco Catalyst 9800-CL Wireless Controllers, and if the AP join failure occurs on the Cisco Catalyst 9800-CL controller, execute the **capwap ap erase all** command to remove the hash string stored on the APs.
- During AP image pre-download, the WNCD CPU may rise to 99 percent, which is normal and doesn't cause a crash or client or AP disconnect problems.

Predownloading an Image to Access Points (CLI)

Before you begin

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

- Predownloading can be done only when the device is booted in the install mode.
- You can copy the new image either from the TFTP server, flash image, or USB.
- If the latest upgrade image is already present in the AP, predownload will not be triggered. Check whether the primary and backup image versions are the same as the upgrade image, using the **show ap image** command.
- The **show ap image** command displays cumulative statistics regarding the AP images in the controller. We recommend that you clear the statistics using the **clear ap predownload statistics** command, before using the **show ap image** command, to ensure that correct data is displayed.
- AP continues to be in predownloading state, if AP flaps post SSO during AP predownload. We recommended that you issue the **ap image predownload abort** command and then the **clear ap predownload stats** command only then the predownload can be intiated again.

Procedure

	Command or Action	Purpose
Step 1	**install add file bootflash:***file-name* **Example:** `Device# install add file bootflash:image.bin`	The controller software image is added to the flash and expanded.
Step 2	**ap image predownload** or **ap name** *ap-name* **image predownload** **Example:**	Downloads the new image to all the access points or a specific access point connected to the device.

	Command or Action	Purpose
	`Device# ap image predownload` `Device# ap name ap1 image predownload`	
Step 3	**show ap image** **Example:** `Device# show ap image`	Verifies the access point's predownload status. This command initially displays the status as Predownloading and then moves to Completed, when download is complete.
Step 4	**show ap name** *ap-name* **image** **Example:** `Device# show ap name ap1 image`	Provides image details of a particular AP.
Step 5	**ap image swap** `or`**ap name** *ap-name* **image swap** `or`**ap image swap completed** **Example:** `Device# ap image swap`	Swaps the images of the APs that have completed predownload. **Note** You can swap the AP images using **ap image swap** command even without pre-downloading a new image to the AP and there are no restrictions or prerequisites to swap the image.
Step 6	**install activate** **Example:** `Device# install activate`	Runs compatibility checks, installs the package, and updates the package status details. For a restartable package, the command triggers the appropriate post-install scripts to restart the necessary processes, and for non-restartable packages it triggers a reload. **Note** This step reloads the complete controller stack (both primary and secondary controllers, if HA is used).
Step 7	**install commit** **Example:** `Device# install commit`	Commits the activation changes to be persistent across reloads. The commit can be done after activation while the system is up, or after the first reload. If the package is activated but not committed, it remains active after the first reload, but not after the second reload.

Monitoring the Access Point Predownload Process

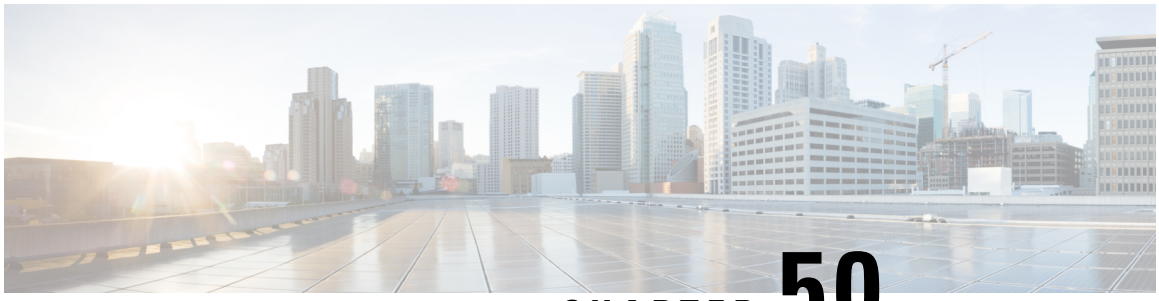
This section describes the commands that you can use to monitor the access point predownload process.

While downloading an access point predownload image, enter the **show ap image** command to verify the predownload progress on the corresponding access point:

```
Device# show ap image
Total number of APs  : 1

Number of APs
       Initiated                : 1
       Predownloading           : 1
       Completed predownloading   : 0
       Not Supported            : 0
       Failed to Predownload      : 0

AP Name                         Primary Image   Backup Image    Predownload Status
Predownload Ver...  Next Retry Time    Retry Count
-------------------------------------------------------------------------------------
AP1                             10.0.1.66       10.0.1.66       Predownloading
10.0.1.67           NA                          0


Device# show ap image

Total number of APs  : 1

Number of APs
       Initiated                : 1
       Predownloading           : 0
       Completed predownloading   : 1
       Not Supported            : 0
       Failed to Predownload      : 0

AP Name                         Primary Image   Backup Image    Predownload Status
Predownload Ver...  Next Retry Time    Retry Count
-------------------------------------------------------------------------------------
AP1                             10.0.1.66       10.0.1.67       Complete
10.0.1.67           NA
                         0
```

Use the following command to view the image details of a particular AP:

```
Device# show ap name APe4aa.5dd1.99b0 image

AP Name : APe4aa.5dd1.99b0
Primary Image : 16.6.230.46
Backup Image : 3.0.51.0
Predownload Status : None
Predownload Version : 000.000.000.000
Next Retry Time : N/A
Retry Count : 0
```



CHAPTER 50

Efficient Image Upgrade

- Efficient Image Upgrade, on page 395
- Enable Pre-Download (GUI), on page 395
- Enable Pre-Download (CLI), on page 396
- Configuring a Site Tag (CLI), on page 396
- Attaching Policy Tag and Site Tag to an AP (CLI), on page 397
- Trigger Predownload to a Site Tag, on page 398

Efficient Image Upgrade

Efficient Image upgrade is an optimized method of predownloading images to FlexConnect APs. For each Site Tag with FlexConnect APs joined, one AP per model in that Site Tag is selected as the primary AP, and downloads its image from the controller through the WAN link. Once the primary AP has the downloaded image, the APs in that Site Tag start downloading the image from the primary AP, via TFTP. At most three subordinate APs can download simultaneously from the primary. This reduces load on the WAN link.

Note Make sure that all APs joined via a Site Tag are at the same location, before enabling this feature.

Enable Pre-Download (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Access Points** page, expand the **All Access Points** section and click the name of the AP to edit.

Step 3 In the **Edit AP** page, click the **Advanced** tab and from the **AP Image Management** section, click **Predownload**.

Step 4 Click **Update & Apply to Device**.

Enable Pre-Download (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex rr-xyz-flex-profile`	Configures a flex profile and enters the flex profile configuration mode.
Step 3	**predownload** **Example:** `Device(config-wireless-flex-profile)# predownload`	Enables predownload of the image.
Step 4	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits the configuration mode and returns to privileged EXEC mode.

Configuring a Site Tag (CLI)

Follow the procedure given below to configure a site tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site rr-xyz-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**flex-profile** *flex-profile-name* **Example:**	Configures a flex profile.

	Command or Action	Purpose
	`Device(config-site-tag)# flex-profile rr-xyz-flex-profile`	**Note** You cannot remove the flex profile configuration from a site tag if local site is configured on the site tag. **Note** The **no local-site** command needs to be used to configure the Site Tag as Flexconnect, otherwise the Flex profile config does not take effect.
Step 4	**description** *site-tag-name* **Example:** `Device(config-site-tag)# description "default site tag"`	Adds a description for the site tag.
Step 5	**end** **Example:** `Device(config-site-tag)# end`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.
Step 6	**show wireless tag site summary** **Example:** `Device# show wireless tag site summary`	(Optional) Displays the number of site tags. **Note** To view detailed information about a site, use the **show wireless tag site detailed** *site-tag-name* command. **Note** The output of the **show wireless loadbalance tag affinity wncd** *wncd-instance-number* command displays default tag (site-tag) type, if both site tag and policy tag are not configured.

Attaching Policy Tag and Site Tag to an AP (CLI)

Follow the procedure given below to attach a policy tag and a site tag to an AP:

Procedure

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

	Command or Action	Purpose
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures a Cisco AP and enters AP profile configuration mode. **Note** The *mac-address* should be a wired mac address.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag rr-xyz-policy-tag`	Maps a policy tag to the AP.
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag rr-xyz-site`	Maps a site tag to the AP.
Step 5	**rf-tag** *rf-tag-name* **Example:** `Device(config-ap-tag)# rf-tag rf-tag1`	Associates the RF tag.
Step 6	**end** **Example:** `Device(config-ap-tag)# end`	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.
Step 7	**show ap tag summary** **Example:** `Device# show ap tag summary`	(Optional) Displays AP details and the tags associated to it.
Step 8	**show ap name** <*ap-name*> **tag info** **Example:** `Device# show ap name ap-name tag info`	(Optional) Displays the AP name with tag information.
Step 9	**show ap name** <*ap-name*> **tag detail** **Example:** `Device# show ap name ap-name tag detail`	(Optional) Displays the AP name with tag detals.

Trigger Predownload to a Site Tag

Follow the procedure given below to trigger image download to the APs:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> configure terminal`	Enters the privileged EXEC mode.
Step 2	**ap image predownload site-tag** *site-tag* **start** **Example:** `Device# ap image predownload site-tag rr-xyz-site start`	Instructs the primary APs to start image predownload.
Step 3	**show ap master list** **Example:** `Device# show ap master list`	Displays the list of primary APs per AP model per site tag.
Step 4	**show ap image** **Example:** `Device# show ap image`	Displays the predownloading state of primary and subordinate APs . **Note** To check if Flexefficient image upgrade is enabled in the AP, use the **show capwap client rcb** command on the AP console.

The following sample outputs display the functioning of the Efficient Image Upgrade feature:

The following output displays the primary AP.

```
Device# show ap master list
AP Name                          WTP Mac          AP Model          Site Tag
-------------------------------------------------------------------------------------
AP0896.AD9D.3124                 f80b.cb20.2460   AIR-AP2802I-D-K9 ST1
```

The following output shows that the primary AP has started predownloading the image.

```
Device# show ap image
Total number of APs: 6

AP Name             Primary Image   Backup Image  Predownload Status   Predownload Version
  Next Retry Time   Retry Count
-----------------------------------------------------------------------------------------
APE00E.DA99.687A    16.6.230.37     0.0.0.0       None                 0.0.0.0
  N/A               0
AP188B.4500.4208    16.6.230.37     8.4.100.0     None                 0.0.0.0
  N/A               0
AP188B.4500.4480    16.6.230.37     0.0.0.0       None                 0.0.0.0
  N/A               0
AP188B.4500.5E28    16.6.230.37     16.4.230.35   None                 0.0.0.0
  N/A               0
AP0896.AD9D.3124    16.6.230.37     8.4.100.0     Predownloading       16.6.230.36
  0                 0
AP2C33.1185.C4D0    16.6.230.37     8.4.100.0     None                 0.0.0.0
  N/A               0
```

The following output shows that the primary AP has completed predownload and the predownload has been initiated in the subordinate AP.

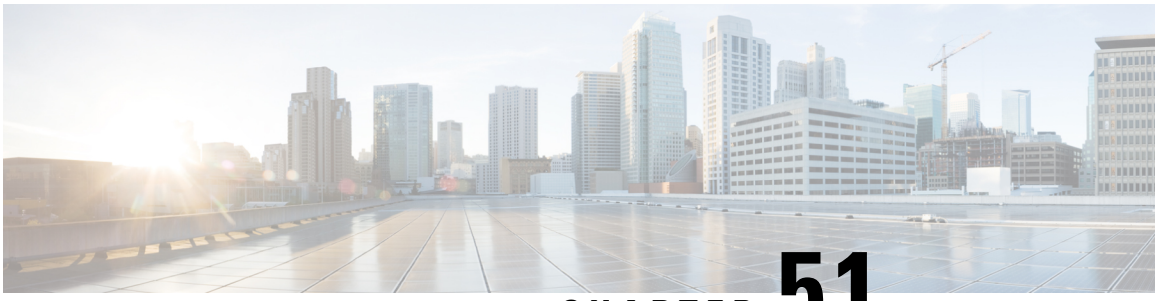
```
Device# show ap image

Total number of APs: 6
AP Name             Primary Image   Backup Image  Predownload Status   Predownload Version
  Next Retry Time   Retry Count
------------------------------------------------------------------------------------------------
APE00E.DA99.687A    16.6.230.37     0.0.0.0       Initiated            16.6.230.36
  N/A               0
AP188B.4500.4208    16.6.230.37     8.4.100.0     None                 0.0.0.0
  N/A               0
AP188B.4500.4480    16.6.230.37     0.0.0.0       None                 0.0.0.0
  N/A               0
AP188B.4500.5E28    16.6.230.37     16.4.230.35   None                 0.0.0.0
  N/A               0
AP0896.AD9D.3124    16.6.230.37     8.4.100.0     Complete             16.6.230.36
  0                 0
AP2C33.1185.C4D0    16.6.230.37     8.4.100.0     Initiated            16.6.230.36
  0                 0
```

The following output shows image status of a particular AP.

```
Device# show ap name APe4aa.5dd1.99b0 image
AP Name : APe4aa.5dd1.99b0
Primary Image : 16.6.230.46
Backup Image : 3.0.51.0
Predownload Status : None
Predownload Version : 000.000.000.000
Next Retry Time : N/A
Retry Count : 0
```

The following output shows predownload completion on all APs.

```
Device# show ap image
Total number of APs: 6

Number of APs
        Initiated                : 0
        Predownloading           : 0
        Completed predownloading   : 3
        Not Supported            : 0
        Failed to Predownload      : 0

AP Name             Primary Image   Backup Image  Predownload Status   Predownload Version
  Next Retry Time   Retry Count
------------------------------------------------------------------------------------------------
APE00E.DA99.687A    16.6.230.37     16.6.230.36   Complete             16.6.230.36
  N/A               0
AP188B.4500.4208    16.6.230.37     8.4.100.0     None                 0.0.0.0
  N/A               0
AP188B.4500.4480    16.6.230.37     0.0.0.0       None                 0.0.0.0
  N/A               0
AP188B.4500.5E28    16.6.230.37     16.4.230.35   None                 0.0.0.0
  N/A               0
AP0896.AD9D.3124    16.6.230.37     16.6.230.36   Complete             16.6.230.36
  0                 0
AP2C33.1185.C4D0    16.6.230.37     16.6.230.36   Complete             16.6.230.36
  0                 0
```



CHAPTER 51

N+1 Hitless Rolling AP Upgrade

- N+1 Hitless Rolling AP Upgrade, on page 401
- Configuring Hitless Upgrade, on page 402
- Verifying Hitless Upgrade, on page 403

N+1 Hitless Rolling AP Upgrade

The existing CAPWAP implementation on the Cisco Catalyst 9800 Series Wireless Controller requires that the controller and all its associated APs have the same software version. It is possible to upgrade a set of APs using the N+1 Hitless Rolling AP Upgrade feature. However, all the APs cannot be upgraded at the same time without network downtime.

You can upgrade wireless networks without network downtime when the same version skew is supported between the controller and the APs. This enables the APs to be upgraded in a staggered manner, while still being connected to the same controller. The version skew method can avoid upgrade downtime even for N+1 networks by using N+1 Hitless Rolling AP Upgrade feature and a spare controller.

The following is the workflow for the N+1 Hitless Rolling AP Upgrade feature:

1. Establish a mobility tunnel from the controller (WLC1) to a mobility member (WLC2).
2. Upgrade the controller software (WLC1) using the command **install add file bootflash:***new_version.bin* .
3. Optionally, you can also upgrade the AP image. For more information, see Predownloading an Image to an Access Point chapter.
4. Use the **ap image upgrade destination** *controller-name controller-ip report-name* privileged EXEC command to upgrade and move all the APs from WLC1 (source) to WLC2 (destination).
5. Activate the new image in WLC1 using the **install activate** command.
6. Commit the changes using the **install commit** command.
7. Move the APs back to WLC1 from WLC2 using the **ap image move destination** *controller-name controller-ip report-name* command.

Note The **ap image upgrade destination** command does not work without an image pre-download. If you do not perform an image pre-download, use the **ap image move** command to move the APs. When APs download the image and join the destination controller, you must set the iteration time as high. Also, you can customise the iteration time by configuring the **ap upgrade staggered iteration timeout** command.

Configuring Hitless Upgrade

Follow the procedure given below to achieve a zero downtime network upgrade in an N+1 deployment.

Before you begin

- Ensure that the hostname and wireless management IP of the destination controller is provided in the privileged EXEC command.
- Ensure that access points are predownloaded with the image running on the destination controller.

Procedure

	Command or Action	Purpose
Step 1	**ap image upgrade destination** *wlc-name wlc-ip* **Example:** `Device# ap image upgrade destination wlc2 10.7.8.9`	Moves APs to the specified destination controller with the swap and reset command. After this, the parent controller activates new image, and reloads with the new image. After the mobility tunnel comes up, APs are moved back to the parent controller without a swap and reset. **Note** Ensure that you establish a mobility tunnel from controller (WLC1) to a mobility member (WLC2) before image upgrade.
Step 2	**ap image upgrade destination** *wlc-name wlc-ip* **Example:** `Device# ap image upgrade destination wlc2 10.7.8.9`	(Optional) Moves APs to the specified destination controller with a swap and reset command. **Note** Perform Steps 2 to 4 only if you are not performing Step 1.
Step 3	**ap image move destination** *wlc-name wlc-ip* **Example:** `Device# ap image move destination wlc1 10.7.8.6`	Move the APs back to the parent controller.
Step 4	**ap image upgrade destination** *wlc-name wlc-ip* [**fallback**]	(Optional) Moves APs to the specified destination controller with a swap and reset command. After that, APs are moved back to

	Command or Action	Purpose
	Example: `Device# ap image upgrade destination wlc2 10.7.8.9 fallback`	the parent controller (without a swap and reset) after manual install activate of the new image and reloading of the parent controller.

Verifying Hitless Upgrade

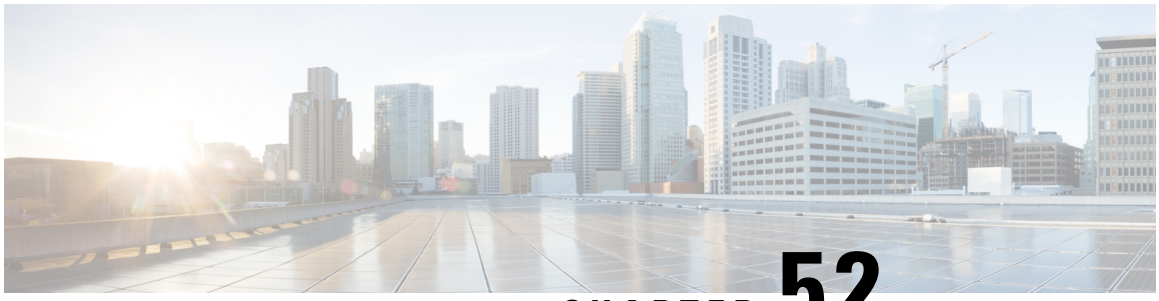
Use the following **show** commands to verify hitless upgrade.

To view all the upgrade report names, use the following command:

```
Device# show ap upgrade summary

Report Name      Start time
-----------------------------------------------------------------------------------------------
AP_upgrade_from_VIGK_CSR_2042018171639 05/20/2018 17:16:39 UTC
```

To view AP upgrade information based on the upgrade report name, use the following command:

```
Device# show ap upgrade name test-report

AP upgrade is complete
From version: 16.10.1.4
To version: 16.10.1.4
Started at: 05/20/2018 17:16:39 UTC
Percentage complete: 100
End time: 05/20/2018 17:25:39 UTC
Progress Report
---------------
Iterations
----------
Iteration Start time End time AP count
-----------------------------------------------------------------------------------------------------
0 05/20/2018 17:16:39 UTC 05/20/2018 17:16:39 UTC 0
1 05/20/2018 17:16:39 UTC 05/20/2018 17:25:39 UTC 1
Upgraded
--------
Number of APs: 1
AP Name Ethernet MAC Iteration Status
-----------------------------------------------------------------------------------------
AP-SIDD-CLICK 70db.9848.8f60 1 Joined
In Progress
-----------
Number of APs: 0
AP Name Ethernet MAC
-------------------------------------------------
Remaining
---------
Number of APs: 0
AP Name Ethernet MAC
-------------------------------------------------
```



CHAPTER 52

Wireless Sub-Package for Switch

- Introduction to Wireless Sub-package, on page 405
- Booting in Install Mode, on page 406
- Installing Sub-Package in a Single Step (GUI), on page 407
- Installing Sub-Package in a Single Step, on page 407
- Multi-step Installation of Sub-Package, on page 408
- Installing on a Stack, on page 409
- Upgrading to a Newer Version of Wireless Package, on page 409
- Deactivating the Wireless Package, on page 409
- Enabling or Disabling Auto-Upgrade, on page 410

Introduction to Wireless Sub-package

Wireless-only Fabric uses fabric constructs to garner the benefits of a fabric. In this architecture, a fabric is built on top of existing traditional network designs such as multi-tier, Routed Access, and VSS network. It uses a LISP control plane together with VXLAN encapsulation for the overlay data plane traffic. The wireless control plane remains intact with CAPWAP tunnels initiating on the APs and terminating on a Cisco Catalyst 9800 Series Wireless Controller or AireOS controller. The Cisco Catalyst 9800 Series Wireless Controller controller can function in a dedicated appliance, directly in a switch, or in a VM.

Cisco Catalyst 9800 Wireless Controller for Switch delivers all the benefits of a centralized control and management plane (easy to configure, upgrade, troubleshoot, etc) and the maximum throughput or performance of a distributed forwarding plane. The distributed data plane allows services such as AVC to scale. In this new model, the wireless control plane is not split between MC and MA. The switch is detached from the wireless control plane and the controller takes care of the wireless function and the traffic switching is done by the Cisco Access Switch.

Since the wireless functionality is required to be enabled only on few nodes of the network, you can install Cisco Catalyst 9800 Series Wireless Controller as a separate package on the switch on a need basis. The sub-package is installed on top of the base image and a reload is required to activate the sub-package.

Note The sub-package is an optional binary that contains the entire Cisco Catalyst 9800 Series Wireless Controller software.

Note Cisco Catalyst 9800 Wireless Controller software on the Cisco Catalyst 9300 switches must be provisioned and deployed on the switch using Cisco DNA Center, and it cannot be configured as a standalone controller. For mode details, see the Cisco Catalyst 9300 Series Switches Hardware Installation Guide.

Note SNMP is not supported on Catalyst 9800 Embedded Wireless Controller for Switch.

How to Install Wireless Package

1. Install the base image (without wireless) on the switch.
2. Install the wireless package on the switch.
3. Upgrade the AP image.
4. Reload the switch.
5. Enable wireless on the switch using the **wireless-controller** configuration command, and configure wireless features.

How to Remove Wireless Package

1. Uninstall the wireless package from the switch.
2. Reload the switch.
3. Run the **write** command. This removes the wireless configuration from the startup-configuration.

Upgrading to a Newer Version of Wireless Package

1. Install the base image (without wireless) on the switch.
2. Install the updated wireless package.
3. Reload the switch.
4. Commit the installation.

Booting in Install Mode

Use the procedure given below to boot the switch in install-mode:

Before you begin

The sub-package does not work in bundle-mode. Use the **show version** command to verify the boot mode.

Procedure

Step 1 **install add file** *image.bin location* **activate commit**.

This command moves the switch from bundle-mode to install-mode. Note that *image.bin* is the base image.

Step 2 Click **yes** to all the prompts.

Step 3 **reload**

Reloads the switch. Ensure that you boot from *flash:packages.conf*. After the reload, the switch will be in install-mode.

Note During Install mode image upgrade/downgrade, “Install add file” with flash:<file_name> command is not supported. Instead of that “bootflash:<filename”> needs to be used.

```
Install add file bootflash:<file_name>  activate commit
```

What to do next

Verify the boot mode using the **show version** command.

Installing Sub-Package in a Single Step (GUI)

Procedure

Step 1 Choose **Administration** > **Software Management** > **Software Upgrade**.

Step 2 Choose the upgrade mode from the **Upgrade Mode** drop-down list, the transport type from the **Transport Type** drop-down list and enter the **Server IP Address (IPv4/IPv6)**, the **File System** and choose the location from the **Source File Path** drop-down list.

Step 3 Click **Download & Install**.

Installing Sub-Package in a Single Step

Use the procedure given below to install sub-package in a single step:

Before you begin

- Ensure that the switch is in install-mode.
- Ensure that you boot only from *flash:packages.conf*.

Procedure

Step 1 **install add file** *flash:<controller>.bin* **activate commit**

Installs the Cisco Catalyst 9800 Wireless Controller for Switch sub-package.

Note The sub-package (flash:<controller>.bin) is available on www.cisco.com. You can also install the sub-package directly from TFTP server.

Step 2 Click **yes** to all the prompts.

What to do next

Use the **show install summary** command to verify the installed image or package.

Multi-step Installation of Sub-Package

Use the procedure given below to install sub-package:

Before you begin

- Ensure that the switch is in install-mode.
- Ensure that you boot only from *flash:packages.conf*.

Procedure

Step 1 **install add file** *flash:<controller>.bin*

The sub-package is added to the flash and expanded.

Step 2 **install activate file** *flash:<controller>.bin*

Installs the sub-package.

Step 3 **install commit**

Completes the installation by writing the files.

What to do next

Use the **show install summary** command to verify the installed image or package.

Installing on a Stack

You can install the package on a stack using either Installing Sub-Package in a Single Step or Multi-step Installation of Sub-Package, on page 408.

If a new member joins the stack, the two possible scenarios are:

- **If auto-upgrade is enabled**: The required software is installed on to the new member. It will match the version of software running on the stack as well as the wireless package.
- **If auto-upgrade is disabled**: As the software version is not the same as in the stack, the new member will remain in version mismatch state and it will not join the stack. You have to manually run the **install autoupgrade** command in EXEC mode to initiate the auto-upgrade procedure.

Upgrading to a Newer Version of Wireless Package

Use the procedure given below to upgrade to a newer version of wireless package:

Procedure

Step 1 **install add file** *flash:<base-image>.bin*

The base image (without wireless) is added to the flash and expanded.

Step 2 **install add file** *flash:<controller-sub-package>.bin*

The sub-package is added to the flash and expanded.

Step 3 **install active**

Installs the base image and sub-package and triggers a reload. However, you can also rollback to the previous state after the reload.

Step 4 **install commit**

Completes the installation by writing the files.

Deactivating the Wireless Package

Follow the procedure given below to deactivate the wireless sub-package:

Procedure

	Command or Action	Purpose
Step 1	**install deactivate file** *flash:<controller>.bin* **Example:**	Removes the package and forces the switch to reboot.

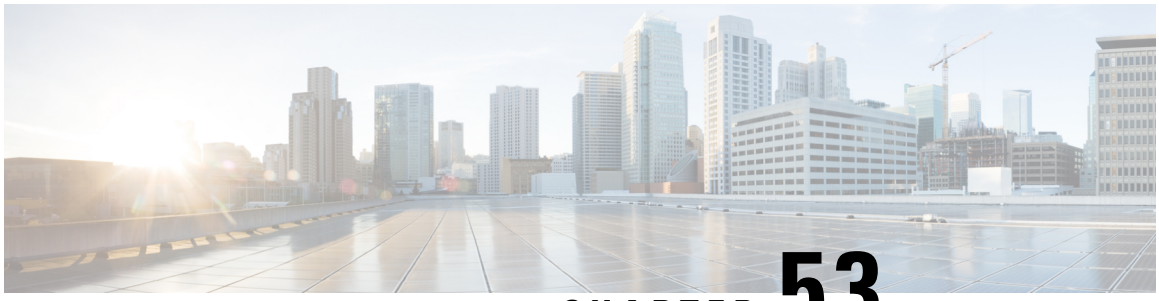
	Command or Action	Purpose
	`Device# install deactivate file flash:<controller>.bin`	
Step 2	**install commit** **Example:** `Device# install commit`	Commits the switch without wireless package.

Enabling or Disabling Auto-Upgrade

Follow the procedure given below to enable or disable auto-upgrade:

Procedure

	Command or Action	Purpose
Step 1	**software auto-upgrade enable** **Example:** `Device(config)# software auto-upgrade enable`	Enables software auto-upgrade.
Step 2	**no software auto-upgrade enable** **Example:** `Device(config)# no software auto-upgrade enable`	Disables software auto-upgrade.



CHAPTER 53

NBAR Protocol Discovery

- Introduction to NBAR Protocol Discovery, on page 411
- Configuring NBAR Protocol Discovery, on page 411
- Verifying Protocol Discovery Statistics, on page 412

Introduction to NBAR Protocol Discovery

The NBAR Protocol Discovery feature provides an easy way of discovering the application protocols passing through an interface. Network Based Application Recognition (NBAR) determines which protocols and applications are currently running on the network. With Protocol Discovery, you can discover any protocol traffic that is supported by NBAR and obtain statistics that are associated with that protocol.

NBAR provides several classification features that identify applications and protocols from Layer 4 through Layer 7. NBAR is also used in Cisco Application Visibility and Control (AVC). With AVC, NBAR provides better application performance through better QoS and policing, and provides finer visibility about the network that is being used.

Configuring NBAR Protocol Discovery

Follow the procedure given below to enable protocol discovery:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy nbar-proto-policy`	Configures a WLAN policy profile and enters wireless policy configuration mode.

	Command or Action	Purpose
Step 3	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures the wireless policy profile for central switching. **Note** NBAR Protocol Discovery is supported in local mode (central switching) and in FlexConnect (central switching) mode.
Step 4	**ip nbar protocol-discovery** **Example:** `Device(config-wireless-policy)# ip nbar protocol-discovery`	Enables application recognition on the wireless policy profile by activating the NBAR2 engine.

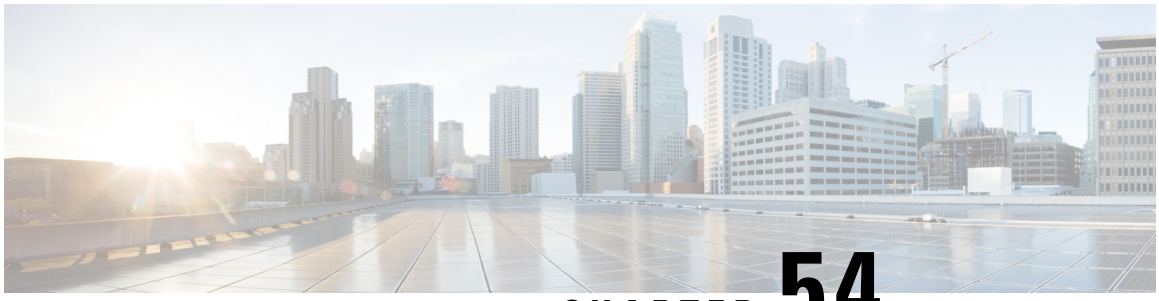
Verifying Protocol Discovery Statistics

To view protocol discovery statistics, use the following command:

```
Device# show ip nbar protocol-discovery wlan wlan-profile-name

wlan_profile_name (iif_id 0xF0400002)

Last clearing of "show ip nbar protocol-discovery" counters 00:07:12


                           Input                     Output
                           -----                     ------
   Protocol                Packet Count              Packet Count
                           Byte Count                Byte Count
                           5min Bit Rate (bps)       5min Bit Rate (bps)
                           5min Max Bit Rate (bps)   5min Max Bit Rate (bps)
   ------------------------ ------------------------ ------------------------
   unknown                 22                        0
                           4173                      0
                           0                         0
                           2000                      0
   dhcp                    3                         2
                           1166                      724
                           0                         0
                           0                         0
   ping                    2                         2
                           204                       236
                           0                         0
                           0                         0
   Total                   27                        4
                           5543                      960
                           0                         0
                           2000                      0
```

To clear protocol discovery statistics, use the following command:

```
Device# clear ip nbar protocol-discovery wlan wlan-profile-name
```



CHAPTER 54

NBAR Dynamic Protocol Pack Upgrade

- NBAR Dynamic Protocol Pack Upgrade, on page 413
- Upgrading the NBAR2 Protocol Pack, on page 414

NBAR Dynamic Protocol Pack Upgrade

Protocol packs are software packages that update the Network-Based Application Recognition (NBAR) engine protocol support on a device without replacing the Cisco software on the device. A protocol pack contains information on applications that are officially supported by NBAR, and are compiled and packed together. In each application, the protocol pack includes information on application signatures and application attributes. Each software release has a built-in protocol pack bundled with it.

The Application Visibility and Control (AVC) feature (used for deep-packet inspection [DPI]) supports wireless products using a distributed approach that benefits from NBAR running on the access points (AP) or controller whose goal is to run DPI and report the result using NetFlow messages.

The AVC DPI technology supports the ability to update recognized traffic and to define the custom type of traffic (known as custom applications). The NBAR runs on the controller in local mode, and on the APs in Flex and Fabric modes. In local mode, all the traffic coming from the APs are tunneled towards the wireless controller.

Note

- Although NBAR is supported in all the modes, upgrade of NBAR protocol packs is supported only in local mode (central switching) and in FlexConnect mode (central switching).
- Custom applications are available only in local mode (central switching) and in FlexConnect mode (central switching).
- When you upgrade the AVC protocol pack, copy the protocol pack to both RPs (active and standby). Otherwise, the protocol pack on the standby upgrade will fail and cause the synchronization failure crash.

Protocol packs provide the following features:

- They can be loaded easily and quickly.
- They can be upgraded to a later version protocol pack or revert to an earlier version protocol pack.
- Device reload is not required.

- They do not disrupt any service.

Protocol Pack Upgrade

Using protocol pack upgrades, you can update the NBAR engine to recognize new types of protocols or traffic without updating the entire switch or appliance image. It also eliminates the need to restart the entire system.

NBAR protocol packs are available for download from Cisco Software Center: https://software.cisco.com/download/navigator.html

Custom Applications

Using custom applications, you can force the NBAR engine to recognize traffic based on a set of custom rules, for example, destination IP, hostname, URL, and so on.

The custom application names then appear in the web UI or in the NetFlow collector.

Upgrading the NBAR2 Protocol Pack

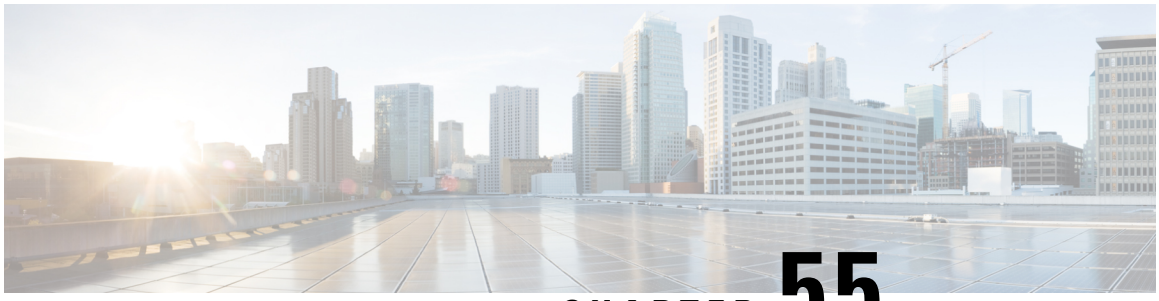
Follow the procedure given below to upgrade the NBAR2 protocol pack:

Before you begin

Download the protocol pack from Software Download page and copy it into the bootflash.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip nbar protocol-pack bootflash:***pack-name* **Example:** `Device(config)# ip nbar protocol-pack bootflash:mypp.pack`	Loads the protocol pack.



CHAPTER 55

Conditional Debug, Radioactive Tracing, and Packet Tracing

- Introduction to Conditional Debugging, on page 415
- Introduction to Radioactive Tracing, on page 416
- Conditional Debugging and Radioactive Tracing, on page 416
- Location of Tracefiles, on page 417
- Configuring Conditional Debugging (GUI), on page 417
- Configuring Conditional Debugging, on page 418
- Radioactive Tracing for L2 Multicast, on page 419
- Recommended Workflow for Trace files, on page 419
- Copying Tracefiles Off the Box, on page 420
- Configuration Examples for Conditional Debugging, on page 420
- Verifying Conditional Debugging, on page 421
- Example: Verifying Radioactive Tracing Log for SISF, on page 421
- Information About Packet Tracing, on page 422
- Configuring Conditional Debugging Packet Tracing, on page 423
- Configuring Conditional Debugging Packet Tracing per AP, on page 424
- Configuring Conditional Debugging Packet Tracing per Client (GUI), on page 425
- Configuring Conditional Debugging Packet Tracing per Client, on page 425
- Verifying Conditional Debugging Packet Tracing Configuration, on page 425

Introduction to Conditional Debugging

The Conditional Debugging feature allows you to selectively enable debugging and logging for specific features based on the set of conditions you define. This feature is useful in systems where a large number of features are supported.

The Conditional debug allows granular debugging in a network that is operating at a large scale with a large number of features. It allows you to observe detailed debugs for granular instances within the system. This is very useful when we need to debug only a particular session among thousands of sessions. It is also possible to specify multiple conditions.

A condition refers to a feature or identity, where identity could be an interface, IP Address, or a MAC address and so on.

This is in contrast to the general debug command, that produces its output without discriminating on the feature objects that are being processed. General debug command consumes a lot of system resources and impacts the system performance.

Introduction to Radioactive Tracing

Radioactive tracing (RA) provides the ability to stitch together a chain of execution for operations of interest across the system, at an increased verbosity level. This provides a way to conditionally print debug information (up to DEBUG Level or a specified level) across threads, processes and function calls.

Note

- The radioactive tracing supports First-Hop Security (FHS).

  For more information on First Hop Security features, see *System Management > Wireless Multicast > Information About Wireless Multicast > Information About IPv6 Snooping*.

- The radioactive tracing filter does not work, if the certificate is not valid.
- For effective debugging of issues on mesh features, ensure that you add both Ethernet and Radio MAC address as conditional MAC for RA tracing, while collecting logs.
- To enable debug for wireless IPs, use the **debug platform condition feature wireless ip** *ip-address* command.

Table 11: Components Supporting Radio Active Tracing

Components	Details
SISF or FHS	The first-hop security features, includes IPv6 Address Glean and IPv6 Device Tracking. For more information, see *Information About IPv6 Snooping*.
LISP	Locator or ID Separation Protocol.

Conditional Debugging and Radioactive Tracing

Radioactive Tracing when coupled with Conditional Debugging, enable us to have a single debug CLI to debug all execution contexts related to the condition. This can be done without being aware of the various control flow processes of the feature within the box and without having to issue debugs at these processes individually.

Note Use the **clear platform condition all** command to remove the debug conditions applied to the platform.

Location of Tracefiles

By default the tracefile logs will be generated for each process and saved into either the **/tmp/rp/trace** or **/tmp/fp/trace** directory. In this temp directory, the trace logs are written to files, which are of 1 MB size each. You can verify these logs (per-process) using the **show platform software trace message** *process_name* **chassis active R0** command. The directory can hold up to a maximum of 25 such files for a given process. When a tracefile in the **/tmp** directory reaches its 1MB limit or whatever size was configured for it during the boot time, it is rotated out to an archive location in the **/crashinfo** partition under **tracelogs** directory.

The **/tmp** directory holds only a single tracefile for a given process. Once the file reaches its file size limit it is rotated out to **/crashinfo/tracelogs**. In the archive directory, up to 25 files are accumulated, after which the oldest one is replaced by the newly rotated file from **/tmp**. File size is process dependent and some processes uses larger file sizes (upto 10MB). Similarly, the number of files in the **tracelogs** directory is also decided by the process. For example, WNCD process uses a limit of 400 files per instance, depending on the platform.

The tracefiles in the crashinfo directory are located in the following formats:

1. Process-name_Process-ID_running-counter.timestamp.gz

   Example: IOSRP_R0-0.bin_0.14239.20151101234827.gz

2. Process-name_pmanlog_Process-ID_running-counter.timestamp.bin.gz

   Example: wncmgrd_R0-0.27958_1.20180902081532.bin.gz

Configuring Conditional Debugging (GUI)

Procedure

Step 1	Choose **Troubleshooting** > **Radioactive Trace**.
Step 2	Click **Add**.
Step 3	Enter the **MAC/IP Address**.
Step 4	Click **Apply to Device**.
Step 5	Click **Start** to start or **Stop** to stop the conditional debug.
Step 6	Click **Generate** to create a radioactive trace log.
Step 7	Click the radio button to set the time interval.
Step 8	Click the **Download Logs** icon that is displayed next to the trace file name, to download the logs to your local folder.
Step 9	Click the **View Logs** icon that is displayed next to the trace file name, to view the log files on the GUI page. Click **Load More** to view more lines of the log file.
Step 10	Click **Apply to Device**.

Configuring Conditional Debugging

Follow the procedure given below to configure conditional debugging:

Procedure

	Command or Action	Purpose
Step 1	**debug platform condition feature wireless mac** {*mac-address*} **Example:** `Device# debug platform condition feature wireless mac b838.61a1.5433`	Configures conditional debugging for a feature using the specified MAC address. **Note** This is supported with AP or client MAC/IP and also on CMX IP address and mobility peer IP.
Step 2	**debug platform condition start** **Example:** `Device# debug platform condition start`	Starts conditional debugging (this will start radioactive tracing if there is a match on one of the conditions above). **Note** This is supported with AP or client MAC/IP and also on CMX IP address and mobility peer IP.

Step 3	**show platform condition** OR **show debug**
	Example:
	`Device# show platform condition`
	`Device# show debug`
		Displays the current conditions set.

Step 4	**debug platform condition stop** **Example:** `Device# debug platform condition stop`	Stops conditional debugging (this will stop radioactive tracing). **Note** This is supported with AP or client MAC/IP and also on CMX IP address and mobility peer IP.
Step 5	**show logging profile wireless** [**counter** | **[last]**{*x days/hours*} | **filter mac**{<*mac address*>} **[to-file]**{<*destination*>} **Example:** `Device# show logging profile wireless start last 20 minutes to-file bootflash:logs.txt`	Displays the logs from the latest wireless profile. **Note** You can use either the *show logging profile wireless* command or *show logging process* command to collect the logs.
Step 6	**show logging process** <*process name*> **Example:** `Device# show logging process wncd to-file flash:wncd.txt`	Displays the logs collection specific to the process.

	Command or Action	Purpose
Step 7	**clear platform condition all** **Example:** `Device# clear platform condition all`	Clears all conditions.

What to do next

Note The command **request platform software trace filter-binary wireless** {*mac-address*} generates 3 flash files:

- *collated_log_<.date..>*
- *mac_log <..date..>*
- *mac_database .. file*

Of these, *mac_log <..date..>* is the most important file, as it gives the messages for the MAC address we are debugging. The command **show platform software trace filter-binary** also generates the same flash files, and also prints the mac_log on the screen.

Radioactive Tracing for L2 Multicast

To identify a specific multicast receiver, specify the MAC address of the joiner or the receiver client, Group Multicast IP address and Snooping VLAN. Additionally, enable the trace level for the debug. The debug level will provide detailed traces and better visibility into the system.

debug platform condition feature multicast controlplane mac *client-mac-addr* **ip** *group-ip-addr* **vlan** *id* **level** *debug level*

Recommended Workflow for Trace files

The Recommended Workflow for Trace files is listed below:

1. To request the tracelogs for a specific time period.

   EXAMPLE 1 day.

   Use the command:

   Device#**show logging process wncd to-file flash:wncd.txt**

2. The system generates a text file of the tracelogs in the location /flash:
3. Copy the file off the switchdevice. By copying the file, the tracelogs can be used to work offline. For more details on copying files, see section below.
4. Delete the tracelog file (.txt) file from /flash: location. This will ensure enough space on the switchdevice for other operations.

Copying Tracefiles Off the Box

An example of the tracefile is shown below:

```
Device# dir crashinfo:/tracelogs
Directory of crashinfo:/tracelogs/

50664 -rwx 760 Sep 22 2015 11:12:21 +00:00 plogd_F0-0.bin_0.gz
50603 -rwx 991 Sep 22 2015 11:12:08 +00:00 fed_pmanlog_F0-0.bin_0.9558.20150922111208.gz
50610 -rw- 11 Nov 2 2015 00:15:59 +00:00 timestamp
50611 -rwx 1443 Sep 22 2015 11:11:31 +00:00
auto_upgrade_client_sh_pmanlog_R0-.bin_0.3817.20150922111130.gz
50669 -rwx 589 Sep 30 2015 03:59:04 +00:00 cfgwr-8021_R0-0.bin_0.gz
50612 -rwx 1136 Sep 22 2015 11:11:46 +00:00 reflector_803_R0-0.bin_0.1312.20150922111116.gz
50794 -rwx 4239 Nov 2 2015 00:04:32 +00:00 IOSRP_R0-0.bin_0.14239.20151101234827.gz
50615 -rwx 131072 Nov 2 2015 00:19:59 +00:00 linux_iosd_image_pmanlog_R0-0.bin_0
```

The trace files can be copied using one of the various options shown below:

```
Device# copy crashinfo:/tracelogs ?
  crashinfo: Copy to crashinfo: file system
  flash: Copy to flash: file system
  ftp: Copy to ftp: file system
  http: Copy to http: file system
  https: Copy to https: file system
  null: Copy to null: file system
  nvram: Copy to nvram: file system
  rcp: Copy to rcp: file system
  running-config Update (merge with) current system configuration
  scp: Copy to scp: file system
  startup-config Copy to startup configuration
  syslog: Copy to syslog: file system
  system: Copy to system: file system
  tftp: Copy to tftp: file system
  tmpsys: Copy to tmpsys: file system
```

The general syntax for copying onto a TFTP server is as follows:

```
Device# copy source: tftp:
Device# copy crashinfo:/tracelogs/IOSRP_R0-0.bin_0.14239.20151101234827.gz tftp:
Address or name of remote host []? 2.2.2.2
Destination filename [IOSRP_R0-0.bin_0.14239.20151101234827.gz]?
```

Note It is important to clear the generated report or archive files off the switch in order to have flash space available for tracelog and other purposes.

Configuration Examples for Conditional Debugging

The following is an output example of the *show platform condition* command.

```
Device# show platform condition
Conditional Debug Global State: Stop
Conditions Direction
------------------------------------------------------------------------------------------|---------
MAC Address 0024.D7C7.0054 N/A
Feature Condition Type Value
----------------------|----------------------|--------------------------------
Device#
```

The following is an output example of the *show debug* command.

```
Device# show debug
IOSXE Conditional Debug Configs:
Conditional Debug Global State: Start
Conditions Direction
------------------------------------------------------------------------------------------|---------
MAC Address 0024.D7C7.0054 N/A
Feature Condition Type Value
----------------------|----------------------|--------------------------------
Packet Infra debugs:
Ip Address Port
------------------------------------------------------|----------
Device#
```

Verifying Conditional Debugging

The table shown below lists the various commands that can be used to verify conditional debugging:

Command	Purpose
show platform condition	Displays the current conditions set.
show debug	Displays the current debug conditions set.
show platform software trace filter-binary	Displays logs merged from the latest tracefile.
request platform software trace filter-binary	Displays historical logs of merged tracefiles on the system.

Example: Verifying Radioactive Tracing Log for SISF

The following is an output example of the *show platform software trace message ios chassis active R0 | inc sisf* command.

```
Device# show platform software trace message ios chassis active R0 | inc sisf

2017/10/26 13:46:22.104 {IOSRP_R0-0}{1}: [parser]: [5437]:  UUID: 0, ra: 0 (note):  CMD:
'show platform software trace message ios switch active R0 | inc sisf' 13:46:22 UTC Thu Oct
 26 2017
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
   FF8E802918 semaphore system unlocked
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Unlocking, count is now 0
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
   FF8E802918 semaphore system unlocked
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Unlocking, count is now 1
```

```
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Setting State to 2
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Start timer 0
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc  Timer value/granularity for 0 :299998/1000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Updated Mac Timer : 299998
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Before Timer :  350000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Timer 0, default value is 350000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
   Allocating timer wheel for 0
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc No timer running
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Granularity for timer MAC_T1  is 1000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Current State :MAC-STALE, Req Timer : MAC_T1  Current Timer
 MAC_T1
```

Information About Packet Tracing

The Packet tracing feature cover details on how to perform data plane packet tracing for Cisco Catalyst 9800 Series Wireless Controller for Cloud software.

This feature identifies the following issues:

- Misconfiguration
- Capacity overload
- Software bugs while troubleshooting

This feature identifies what happens to a packet in your system. The conditional debugging packet tracing feature is used for accounting and capturing per-packet processing details for user-defined conditions.

You can trace packets on the controller using the following steps:

1. Enable conditional debugging on selected packets or traffic you want to trace on the controller.
2. Enable packet tracing (per-AP or per-Client).

Note You need to use per AP conditional debugging with MAC address as a filter when AP and controllers are in the same VLAN. If they are not in the same VLAN, the per AP packet tracing with MAC address does not capture packets as MAC address varies.

Limitation of Conditional Debugging Packet Tracing

MAC or IP filter only applies to the outer Ethernet or IP header, so if a packet is CAPWAP encapsulated, the MAC or IP does not apply to the inner 802.11 MAC or IP.

Configuring Conditional Debugging Packet Tracing

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged **EXEC** mode. Enter your password, if prompted.
Step 2	**debug platform packet-trace packet** *packet-count* **circular fia-trace data-size** *data-size* **Example:** `Device# debug platform packet-trace packet 8192 circular fia-trace data-size 2048`	Configures packet tracing to capture the last set of packets. Here, *packet-count*—Valid range is from 16 to 8192. *data-size*—Valid range is from 2048 to 16384 bytes.
Step 3	**debug platform packet-trace copy packet both size** *packet-size* **Example:** `Device# debug platform packet-trace copy packet both size 2048`	Configures packet tracing for a copy of packet data. Here, *packet-size*—Valid range is from 16 to 2048 bytes.
Step 4	**debug platform condition interface** {*intf-name* | **cpp**} {**mac** | **ipv4** | **match**} {**both** | **ingress** | **egress**} **Example:** Enables conditional debugging for TenGigabitEthernet 0/0/0 and match packets whose source and destination MAC is 0001.0001.0001: `Device# debug platform condition interface TenGigabitEthernet 0/0/0 mac 0001.0001.0001 both`	Enables conditional debugging for an interface, MAC, or IP filter. An interface refers to any physical port, port channel, internal vlan, SVI, or wireless client.
Step 5	**debug platform condition start** **Example:** `Device# debug platform condition start`	Starts conditional debugging packet tracing.
Step 6	**debug platform condition stop** **Example:** `Device# debug platform condition stop`	Stops conditional debugging packet tracing.
Step 7	**show platform hardware chassis active qfp feature packet-trace packet all | redirect bootflash:packet_trace.txt**	Redirects all traced packets to bootflash.

	Command or Action	Purpose
	Example: `Device# show platform hardware chassis active qfp feature packet-trace packet all | redirect bootflash:packet_trace.txt`	Converts the packet_trace.txt to pcap and downloads the pcap files. You can do so using the following link: http://wwwin-dharton-dev.cisco.com/pactrac2pcap.html

Configuring Conditional Debugging Packet Tracing per AP

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged **EXEC** mode. Enter your password, if prompted.

Step 2	**debug platform condition interface** {*intf-name* | **cpp**} {**mac** [**mac-address** | **access-list** *acl-name*] | **ipv4** | **match**} {**both** | **ingress** | **egress**}
	Example:
	`Device# debug platform condition interface TenGigabitEthernet 0/0/0 mac 0001.0001.0001 both`
	`Device# debug platform condition interface TenGigabitEthernet 0/0/0 mac access-list mac-acl-name both`
		Enables conditional debugging with MAC filter.
		Herein, the CLI matches the packets whose source or destination MAC address is 0001.0001.0001.

Step 3	**debug platform condition interface TenGigabitEthernet** *intf-number* **match mac** {**H.H.H** | **any** | **host**} {**both** | **ingress** | **egress**} **Example:** `Device# debug platform condition interface TenGigabitEthernet 0/0/0 match mac 0001.0001.0001 both`	Enables conditional debugging with inline MAC ACL.

Step 4	**debug platform condition interface TenGigabitEthernet** *intf-number* **ipv4** {*A.B.C.D/nn* | **access-list** *acl-name* | **both** | **egress** | **ingress**} {**both** | **egress** | **ingress**}
	Example:
	`Device# debug platform condition interface TenGigabitEthernet 0/0/0 ipv4 192.168.1.2/32 both`
	`Device# debug platform condition interface TenGigabitEthernet 0/0/0 ipv4 access-list ip-acl-name both`
		Enables conditional debugging with IP filter.
		Here,
		intf-number—Is the GigabitEthernet interface number.Valid range is from 1 to 32.

	Command or Action	Purpose
	`Device# debug platform condition interface TenGigabitEthernet 0/0/0 match ipv4 192.168.1.2/32 both`	

Configuring Conditional Debugging Packet Tracing per Client (GUI)

Procedure

Step 1 Choose **Troubleshooting** > **Radioactive Trace**.

Step 2 Click **Add**.

Step 3 In the Add MAC/IP Address window, enter the **MAC/IP Address**.

Step 4 Click **Apply to Device**.

Configuring Conditional Debugging Packet Tracing per Client

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged **EXEC** mode. Enter your password, if prompted.
Step 2	**debug platform condition interface** {*intf-name* | **cpp** *cpp-handle-index*} {**mac** | **ipv4** | **match** [**ipv4** | **ipv6** | **mac**]} {**both** | **ingress** | **egress**} **Example:** `Device# debug platform condition interface cpp 0xa0000001 match ipv4 protocol icmp host 192.168.1.100 host 192.168.1.1 both`	Enables conditional debugging for a wireless client interface. Here, *cpp-handle-index*—Valid range is from 1 to 4294967295.

Verifying Conditional Debugging Packet Tracing Configuration

To view the summary of the traced packet, use the following command:

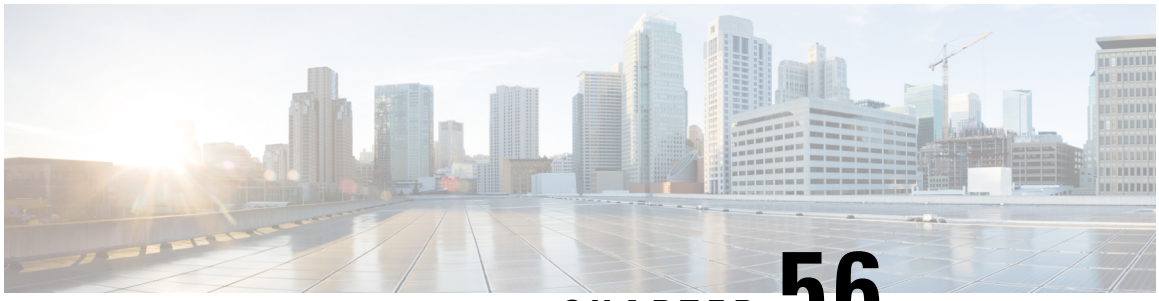
```
Device# show platform packet-trace summary
```

To view a specific traced packet, use the following command:

```
Device# show platform packet-trace packet packet-number
```

To view the wireless client interface handle, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
mac-address client-mac details
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
mac-address 8825.93b0.b51f details
Client Details for client cpp_if_handle: 0x34
Name : WLCLIENT-IF-0x00a0000001
Mac Addr : 8825.93b0.b51f
pal_if_handle : 0xa0000001
Mobility State : LOCAL
Multicast Action : FORWARD
Auth State : RUN
```



CHAPTER 56

Aggressive Client Load Balancing

- Information About Aggressive Client Load Balancing, on page 427
- Enabling Aggressive Client Load Balancing (GUI), on page 428
- Configuring Aggressive Client Load Balancing (GUI), on page 428
- Configuring Aggressive Client Load Balancing (CLI), on page 429

Information About Aggressive Client Load Balancing

The Aggressive Client Load Balancing feature allows lightweight access points to load balance wireless clients across access points.

When a wireless client attempts to associate to a lightweight access point, the associated response packets are sent to a client with an 802.11 response packet including status code 17. This code 17 indicates that the corresponding AP is busy. The AP does not respond with the response '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 hears the client request.

For example, if the number of clients on AP1 is more than the number of clients on AP2 and the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, the client 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 attempts to associate 11 times, it will 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 A voice client does not authenticate when delay is configured to more than 300 ms. To avoid this, configure a central-authentication, local-switching WLAN with Cisco Centralized Key Management (CCKM), configure a pagent router between an AP and WLC with a delay of 600 ms (300 ms UP and 300 ms DOWN), and try associating the voice client.

Note For a FlexConnect AP, the association is locally handled. The load-balancing decisions are taken at the controller. A FlexConnect AP sends an initial response to the client before knowing the result of the calculations in the controller. Load-balancing does not take effect when the FlexConnect AP is in standalone mode.

A FlexConnect AP does not send (re)association response with status 17 for load balancing the way local-mode APs do; instead, it first sends (re)association with status 0 (success) and then deauth with reason 5.

Note This feature is not supported on the APs joined on default-site-tag.

This feature is not supported on the APs across different named site-tags.

This feature is supported only on the APs within a named-site-tag.

Enabling Aggressive Client Load Balancing (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > WLANs > Wireless Networks**.

Step 2 Select a **WLAN** to view the **Edit WLAN** window.

Step 3 Click **Advanced** tab.

Step 4 Select the **Load Balance** check box to enable the feature.

Step 5 Click **Update & Apply to Device**.

Configuring Aggressive Client Load Balancing (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Advanced**.

The **Load Balancing** window is displayed.

Step 2 In the **Aggressive Load Balancing Window (clients)** field, enter the number of clients for the aggressive load balancing client window.

Step 3 In the **Aggressive Load Balancing Denial Count** field, enter the load balancing denial count.

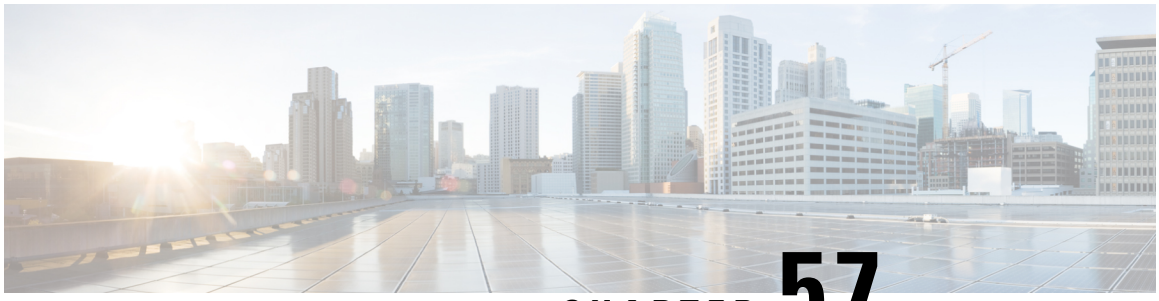
Step 4 Click **Apply**.

Configuring Aggressive Client Load Balancing (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wlan** *wlan-name* **Example:** `Device(config)# wlan test-wlan`	Specifies the WLAN name.
Step 4	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Disables the WLAN.
Step 5	**load-balance** **Example:** `Device(config-wlan)# load-balance`	Configures a guest controller as mobility controller, in order to enable client load balance to a particular WLAN. Configure the WLAN security settings as the WLAN requirements.
Step 6	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables WLAN.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 8	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 9	**ap dot11** {**24ghz** | **5ghz**} **load-balancingdenial** *count* **Example:** `Device(config)# ap dot11 5ghz load-balancing denial 10`	Configures the load balancing denial count.

	Command or Action	Purpose
Step 10	**ap dot11** {**24ghz** | **5ghz**} **load-balancingwindow** *clients* **Example:** `Device(config)# ap dot11 5ghz load-balancing denial 10`	Configures the number of clients for the aggressive load balancing client window.
Step 11	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.
Step 12	**show running-config | section** *wlan-name* **Example:** `Device# show running-config | section test-wlan`	Displays a filtered section of the current configuration.



CHAPTER 57

Accounting Identity List

- Configuring Accounting Identity List (GUI), on page 431
- Configuring Accounting Identity List (CLI), on page 431
- Configuring Client Accounting (GUI), on page 432
- Configuring Client Accounting (CLI), on page 432

Configuring Accounting Identity List (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA**.

Step 2 In the **AAA Method List** tab, go to the **Accounting** section, and click **Add**.

Step 3 In the **Quick Setup: AAA Accounting** window that is displayed, enter a name for your method list.

Step 4 Choose the type of authentication as identity, in the **Type** drop-down list.

Step 5 Choose the server groups you want to use to authenticate access to your network, from the **Available Server Groups** list and click > icon to move them to the **Assigned Server Groups** list.

Step 6 Click **Save & Apply to Device**.

Configuring Accounting Identity List (CLI)

Accounting is the process of logging the user actions and keeping track of their network usage. 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.

Follow the procedure given below to configure accounting identity list.

Before you begin

Configure the RADIUS server and AAA group server.

Procedure

	Command or Action	Purpose
Step 1	**aaa accounting identity** *named-list* **start-stop group** *server-group-name* **Example:** `Device(config)# aaa accounting identity user1 start-stop group aaa-test`	Enables accounting to send a start-record accounting notice when a client is authorized and a stop-record at the end. **Note** You can also use the default list, instead of a named list.

Whenever there is a change in the client attribute, for example, change in IP address, client roaming, and so on, an accounting interim update is sent to the RADIUS server.

Configuring Client Accounting (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the **Policy Profile Name** and in the **Edit Policy Profile** window, go to the **Advanced** tab.

Step 3 From the **Accounting List** drop-down, select the appropriate accounting list for this policy profile. This will ensure that the policy profile undergoes that type of accounting you want to perform, before allowing it access to the network.

Step 4 Click **Save & Apply to Device**.

Configuring Client Accounting (CLI)

Follow the procedure given below to configure client accounting.

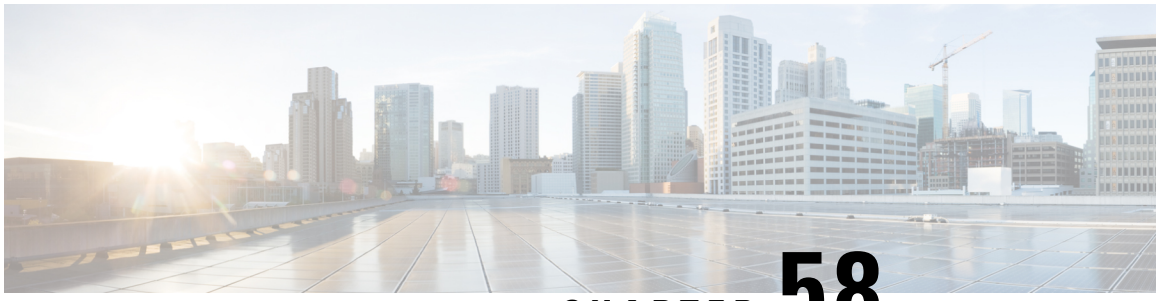
Before you begin

Ensure that RADIUS accounting is configured.

Procedure

	Command or Action	Purpose
Step 1	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 2	**shutdown** **Example:**	Disables the policy profile.

	Command or Action	Purpose
	`Device(config-wireless-policy)# shutdown`	
Step 3	**accounting-list** *list-name* **Example:** `Device(config-wireless-policy)# accounting-list user1`	Sets the accounting list.
Step 4	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the policy profile.



CHAPTER 58

Wireless Multicast

- Information About Wireless Multicast, on page 435
- Prerequisites for Configuring Wireless Multicast, on page 438
- Restrictions on Configuring Wireless Multicast, on page 439
- Configuring Wireless Multicast, on page 439
- IPv6 Multicast-over-Multicast, on page 441
- Directed Multicast Service, on page 443
- Wireless Broadcast, Non-IP Multicast and Multicast VLAN, on page 446
- Multicast Filtering, on page 452

Information About Wireless Multicast

If the network supports packet multicasting, the multicast method that the controller uses can be configured. The controller performs multicast routing in two modes:

- Unicast mode: The controller unicasts every multicast packet to every access point associated to the controller. This mode is inefficient and generates a lot of extra traffic in the device and the network, but is required on networks that do not support multicast routing (needed if the APs are on different subnets than the device's wireless management interface).
- Multicast mode: The controller sends multicast packets to a CAPWAP multicast group. This method reduces the overhead on the controller processor and shifts the work of packet replication to the network, which is much more efficient than the unicast method.

The flexconnect mode has two submodes: local switching and central switching. In local switching mode, the data traffic is switched at the AP level and the controller does not see any multicast traffic. In central switching mode, the multicast traffic reaches the controller. However, IGMP snooping takes place at the AP.

When the multicast mode is enabled 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 VLAN for sending multicast packets. Access points in the multicast group receive the packet and forward it to all the BSSIDs mapped to the VLAN on which clients receive multicast traffic.

The controller supports all the capabilities of IGMP v1, including Multicast Listener Discovery (MLD) v1 snooping, but the IGMP v2 and IGMP v3 capabilities are limited. This feature keeps track of and delivers IPv6 multicast flows to the clients that request them. To support IPv6 multicast, global multicast mode should be enabled.

Internet Group Management Protocol (IGMP) snooping is introduced to better direct multicast packets. When this feature is enabled, the controller snooping gathers IGMP reports from the clients, processes them, creates unique multicast group IDs (MGIDs) based on the Layer 3 multicast address and the VLAN number, and sends the IGMP reports to the IGMP querier. The controller then updates the access-point MGID table on the corresponding 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 VLAN.

MGID is a 14-bit value filled in the 16-bit reserved field of wireless information in the CAPWAP header. The remaining two bits should be set to zero.

Multicast Optimization

Multicast optimization enables you to create a multicast VLAN that can be used for multicast traffic. One of the VLANs in the device can be configured as a multicast VLAN where multicast groups are registered. The clients are allowed to listen to a multicast stream on the multicast VLAN. The MGID is generated using the mulicast VLAN and multicast IP addresses. If multiple clients on different VLANs of the same WLAN are listening to a single multicast IP address, a single MGID is generated. The device makes sure that all the multicast streams from the clients on this VLAN group always go out on the multicast VLAN to ensure that the upstream router has one entry for all the VLANs of the VLAN group. Only one multicast stream hits the VLAN group even if the clients are on different VLANs. Therefore, the multicast packets that are sent out over the network is just one stream.

Note When VLAN groups are defined and uses multicast communication, then you need to enable the multicast VLAN.

IPv6 Global Policies

IPv6 global policies provide storage and access policy database services. IPv6 ND inspection and IPv6 RA guard are IPv6 global policies features. Every time an ND inspection is configured globally, the policy attributes are stored in the software policy database. The policy is then applied to an interface, and the software policy database entry is updated to include this interface to which the policy is applied.

IPv6 RA guard is enabled by default on the controller. RA from the wired side should be forwarded to the wireless clients if the Stateless Address Auto-Configuration (SLAAC) is deployed in the network.

Information About IPv6 Snooping

The following sections provide information about IPv6 snooping.

IPv6 Neighbor Discovery Inspection

The IPv6 Neighbor Discovery Inspection, or IPv6 snooping feature bundles several Layer 2 IPv6 first-hop security features, including IPv6 Address Glean and IPv6 Device Tracking. IPv6 neighbor discovery (ND) inspection operates at Layer 2, or between Layer 2 and Layer 3, and provides IPv6 features with security and scalability. This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism,

such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables and analyzes ND messages in order to build a trusted binding table. IPv6 ND messages that do not have valid bindings are dropped. An ND message is considered trustworthy if its IPv6-to-MAC mapping is verifiable. This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

When IPv6 ND inspection is configured on a target (which varies depending on platform target support and may include device ports, switch ports, Layer 2 interfaces, Layer 3 interfaces, and VLANs), capture instructions are downloaded to the hardware to redirect the ND protocol and Dynamic Host Configuration Protocol (DHCP) for IPv6 traffic up to the switch integrated security features (SISF) infrastructure in the routing device. For ND traffic, messages such as NS, NA, RS, RA, and REDIRECT are directed to SISF. For DHCP, UDP messages sourced from port 546 or 547 are redirected.

IPv6 ND inspection registers its "capture rules" to the classifier, which aggregates all rules from all features on a given target and installs the corresponding ACL down into the platform-dependent modules. Upon receiving redirected traffic, the classifier calls all entry points from any registered feature (for the target on which the traffic is being received), including the IPv6 ND inspection entry point. This entry point is the last to be called, so any decision (such as drop) made by another feature supersedes the IPv6 ND inspection decision.

IPv6 Device Tracking

IPv6 device tracking provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears.

IPv6 First-Hop Security Binding Table

The IPv6 First-Hop Security Binding Table recovery mechanism feature enables the binding table to recover in the event of a device reboot. A database table of IPv6 neighbors connected to the device is created from information sources such as ND snooping. This database, or binding, table is used by various IPv6 guard features to validate the link-layer address (LLA), the IPv4 or IPv6 address, and prefix binding of the neighbors to prevent spoofing and redirect attacks.

This mechanism enables the binding table to recover in the event of a device reboot. The recovery mechanism will block any data traffic sourced from an unknown source; that is, a source not already specified in the binding table and previously learned through ND or DHCP gleaning. This feature recovers the missing binding table entries when the resolution for a destination address fails in the destination guard. When a failure occurs, a binding table entry is recovered by querying the DHCP server or the destination host, depending on the configuration.

Recovery Protocols and Prefix Lists

The IPv6 First-Hop Security Binding Table Recovery Mechanism feature introduces the capability to provide a prefix list that is matched before the recovery is attempted for both DHCP and NDP.

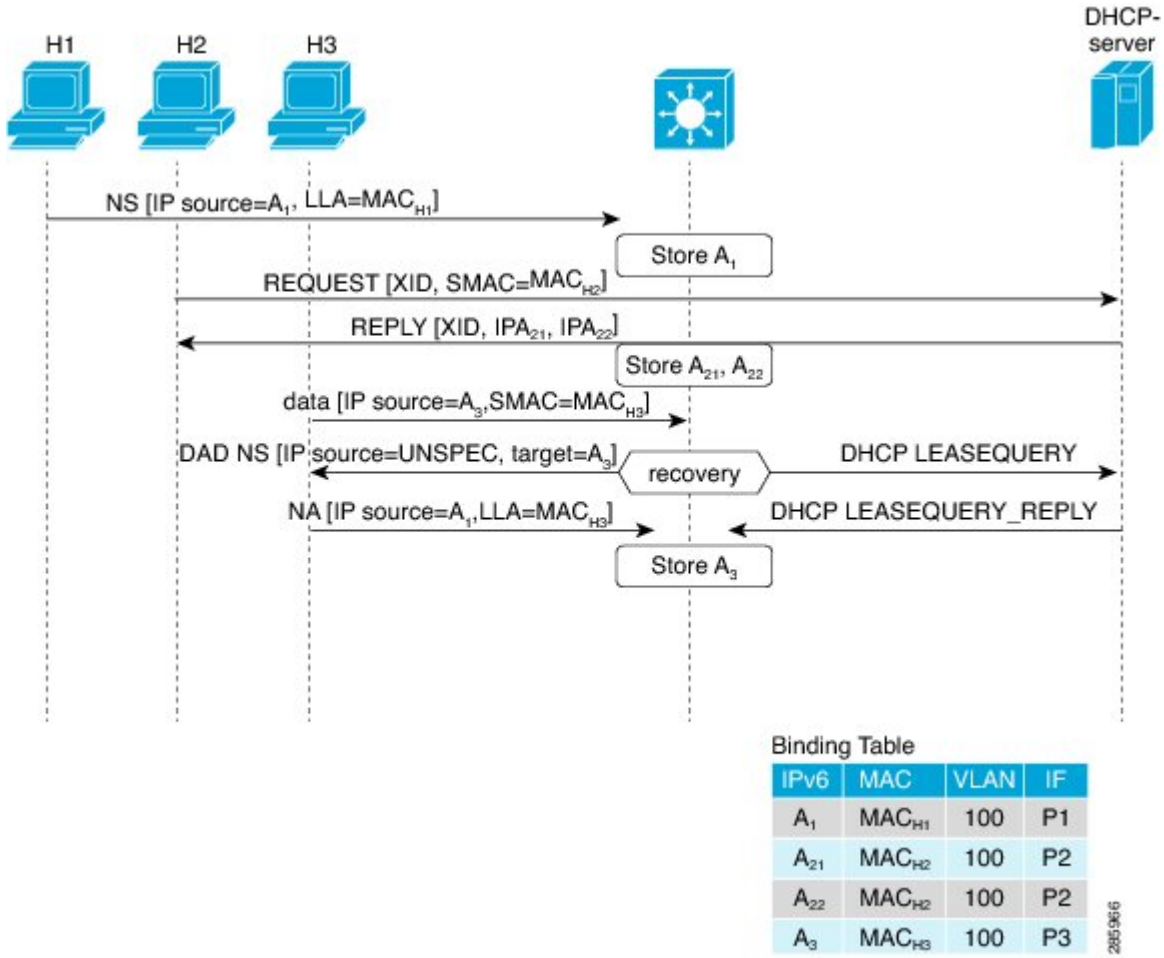
If an address does not match the prefix list associated with the protocol, then the recovery of the binding table entry will not be attempted with that protocol. The prefix list should correspond to the prefixes that are valid for address assignment in the Layer 2 domain using the protocol. The default is that there is no prefix list, in which case the recovery is attempted for all addresses. The command to associate a prefix list to a protocol is **protocol** {**dhcp** | **ndp**} [**prefix-list** *prefix-list-name*].

IPv6 Address Glean

IPv6 address glean is the foundation for many other IPv6 features that depend on an accurate binding table. It inspects ND and DHCP messages on a link to glean addresses, and then populates the binding table with these addresses. This feature also enforces address ownership and limits the number of addresses any given node is allowed to claim.

The following figure shows how IPv6 address glean works.

Figure 6: IPv6 Address Glean



Prerequisites for Configuring Wireless Multicast

- To participate in IP multicasting, the multicast hosts, routers, and multilayer switches must have IGMP operating.
- When enabling multicast mode on the controller, a CAPWAP multicast group address should also be configured. Access points listen to the CAPWAP multicast group using IGMP.

Restrictions on Configuring Wireless Multicast

The following are the restrictions for configuring IP multicast forwarding:

- Access points 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.
- Multicast routing should not be enabled for the management interface.
- Multicast with VLAN group is only supported in local mode AP.
- Multicast traffic from wireless clients in non-multicast VLAN should be routed by the uplink switch.
- Multicast traffic on an AAA overridden VLAN is not supported.

Restrictions for IPv6 Snooping

The IPv6 snooping feature is not supported on Etherchannel ports.

Configuring Wireless Multicast

The following sections provide information about the various wireless multicast configuration tasks:

Configuring Wireless Multicast-MCMC Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**wireless multicast***ip-addr* **Example:** `Device(config)# wireless multicast 231.1.1.1`	Enables multicast-over-multicast. Use the **no** form of this command to disable the feature.
Step 2	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Configuring Wireless Multicast-MCUC Mode

Note The wireless multicast to unicast (MCUC) mode is only supported in 9800-CL small template.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless multicast** **Example:** `Device(config)# wireless multicast`	Enables the multicast traffic for wireless clients.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Configuring Multicast Listener Discovery Snooping (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **Multicast**.

Step 2 Click **MLD Snooping**.

Step 3 In the **MLD Snooping** section, click the toggle button to enable or disable MLD snooping.

Step 4 Enter the **MLD Query Interval**, in milliseconds. The value range is between 100 ms and 32767 ms. The default value is 1000 ms.

Step 5 Move the required VLAN IDs listed in the **Disabled** section to the **Enabled** section. (By default, this feature is disabled on the VLAN.)

You can also search for a VLAN ID using the search field. You can click **Disable All** to move all the VLAN IDs from the **Enabled** list to the **Disabled** list, or click **Enable All** to move all the VLAN IDs from the **Disabled** list to the **Enabled** list.

Step 6 Click **Apply to Device**.

Configuring IPv6 MLD Snooping

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# ipv6 mld snooping`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ipv6 mld snooping** **Example:** `Device(config)# ipv6 mld snooping`	Enables MLD snooping.

Verifying the Multicast VLAN Configuration

To view the multicast VLAN associated with a policy profile along with the VLAN assigned to that profile, use the following command:

```
Device# show wireless profile policy detail default-policy-profile

Policy Profile Name           : default-policy-profile
Description                   : default policy profile
Status                        : ENABLED
VLAN                          : vlan-pool1
Multicast VLAN        : 84
Client count                  : 0
Passive Client                : DISABLED
```

To view the multicast VLAN associated with a client, use the following command:

```
Device# show wireless client mac ac2b.6e4b.551e detail

Client MAC Address : ac2b.6e4b.551e
Client IPv4 Address : 84.84.0.20
…….
VLAN : 82
Access VLAN : 82
Multicast VLAN: 84
```

IPv6 Multicast-over-Multicast

IPv6 multicast allows a host to send a single data stream to a subset of all the hosts (group transmission) simultaneously. When IPv6 Multicast over Multicast is configured, all the APs join the IPv6 multicast address, and the multicast traffic from the wireless controller to the AP flows over the IPv6 multicast tunnel.

In mixed deployments (IPv4 and IPv6), the APs might join the wireless controller over IPv4 or IPv6. To enable Multicast over Multicast in mixed deployments, configure both IPv4 and IPv6 multicast tunnels. The IPv4 APs have a unicast IPv4 CAPWAP tunnel and join the IPv4 multicast group. The IPv6 APs will have a unicast IPv6 CAPWAP tunnel and joins the IPv6 multicast group.

Note Mixed mode of Multicast over Unicast and Multicast over Multicast over IPv4 and IPv6 is not supported in Cisco IOS XE Gibraltar 16.10.1.

Table 12: Multicast Support Per Platform

Platform	Multicast Support - Multicast over Unicast	Multicast Support - Multicast over Multicast
Cisco Catalyst 9800-40 Wireless Controller	No	Yes
Cisco Catalyst 9800-80 Wireless Controller	No	Yes
Cisco Catalyst 9800 Wireless Controller for Cloud - Small Template	Yes	Yes
Cisco Catalyst 9800 Wireless Controller for Cloud - Medium Template	No	Yes
Cisco Catalyst 9800 Wireless Controller for Cloud - Large Template	No	Yes
Cisco Catalyst 9800-L Wireless Controller	Yes	Yes

Configuring IPv6 Multicast-over-Multicast (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **Multicast**.

Step 2 From the **AP Capwap Multicast** drop-down list, select **Multicast**.

Step 3 Enter the **AP Capwap IPv6 Multicast group Address**.

Step 4 Click **Apply**.

Configuring IPv6 Multicast-over-Multicast

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless multicast** {*ipv4-address* | **ipv6** *ipv6-address*) **Example:** `Device(config)# wireless multicast ipv6 ff45:1234::86`	Configures IPv6 multicast-over-multicast address.

Verifying IPv6 Multicast-over-Multicast

To verify the IPv6 multicast-over-multicast configuration, use the following commands:

```
Device# show wireless multicast

Multicast : Enabled
AP Capwap Multicast : Multicast
AP Capwap IPv4 Multicast group Address : 231.1.1.1
AP Capwap IPv6 Multicast group Address : ff45:1234::86
Wireless Broadcast : Disabled
Wireless Multicast non-ip-mcast : Disabled


Device# show running-configuration | inc multicast

show run | inc multicast:--

wireless multicast
wireless multicast ipv6 ff45:1234::86
wireless multicast 231.1.1.1
```

Verifying the Multicast Connection Between the Controller and the AP

Cisco Catalyst 9800 Series Wireless Controller initiates a ping request that passes through the CAPWAP multicast tunnel onto the CAPWAP multicast receiver, which is the AP. In response, the AP pings the packets for CAPWAP multicast group IP address, and sends back the response to the controller. You can view the statistics on the AP for transmitted and received traffic to analyse the data that are sent and received through the multicast tunnel. Alternatively, you can also verify by enhancing the existing statistics on the AP for transmitted and received traffic to explicitly list the joins, leaves, data packets transmitted and received through the multicast tunnel.

To confirm if the APs receive multicast to multicast (mom) traffic sent by the controller, use the following command

```
Device# show ap multicast mom

AP Name                     MOM-IP     TYPE MOM- STATUS
-----------------------------------------------------
SS-E-1                      IPv4            Up
SS-E-2                      IPv4            Up
9130E-r3-sw2-g1012          IPv4            Up
9115i-r3-sw2-te1-0-38       IPv4            Up
AP9120-r3-sw3-Gi1-0-46      IPv4            Up
ap3800i-r2-sw1-te2-0-2      IPv4            Up
```

Directed Multicast Service

The Directed Multicast Service (DMS) feature allows a client to request access points (AP) to transmit multicast packets as unicast frames. After receiving this request, an AP buffers the multicast traffic for a client and transmits it as a unicast frame when the client wakes up. This allows the client to receive the multicast packets that were ignored while in sleep mode (to save battery power) and also ensures Layer 2 reliability. The unicast frames are 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 saving more battery power. Without DMS, the client has to wake up at each Delivery Traffic Indication Map (DTIM) interval to receive multicast traffic.

Configuring Directed Multicast Service(GUI)

Procedure

Step 1 Choose **Configuration > Wireless > WLANs > Wireless Networks**.

Step 2 Select a **WLAN** to view the **Edit WLAN** window.

Step 3 Click **Advanced** tab.

Step 4 Check the **Directed Multicast Service** check box to enable the feature.

Step 5 Click **Update & Apply to Device**.

Configuring Directed Multicast Service

Before you begin

- This feature is enabled on receiving a request from a client. Ensure that this feature is configured under WLAN.
- This feature is supported only on 802.11v-capable clients, such as Apple iPad and Apple iPhone.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan test5`	Configures the WLAN profile and enters WLAN profile configuration mode.
Step 3	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Disables the WLAN profile.
Step 4	**dms** **Example:** `Device(config-wlan)# dms`	Configures DMS processing per WLAN.
Step 5	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN profile.

Verifying the Directed Multicast Service Configuration

To verify the status of the DMS configuration on the controller, use **show** commands below. The DMS status is displayed under *IEEE 802.11v Parameters*.

```
Device# show wlan id 5

WLAN Profile Name     : test
================================================
Identifier                                    : 5
Network Name (SSID)                           : test
Status                                        : Disabled
Broadcast SSID                                : Enabled
Universal AP Admin                            : Disabled
Max Associated Clients per WLAN               : 0
Max Associated Clients per AP per WLAN        : 0
Max Associated Clients per AP Radio per WLAN  : 200
!
.
.
.
Assisted-Roaming
    Neighbor List                             : Disabled
    Prediction List                           : Disabled
    Dual Band Support                         : Disabled

! DMS status is displayed below.

IEEE 802.11v parameters
    Directed Multicast Service                : Enabled
    BSS Max Idle                              : Disabled
        Protected Mode                        : Disabled
    Traffic Filtering Service                 : Disabled
    BSS Transition                            : Enabled
        Disassociation Imminent               : Disabled
            Optimised Roaming Timer           : 40
            Timer                             : 200
    WNM Sleep Mode                            : Disabled
802.11ac MU-MIMO                              : Disabled
802.11ax paramters
    OFDMA Downlink                            : unknown
    OFDMA Uplink                              : unknown
    MU-MIMO Downlink                          : unknown
    MU-MIMO Uplink                            : unknown
    BSS Color                                 : unknown
    Partial BSS Color                         : unknown
    BSS Color Code
```

To verify the status of the DMS configuration on the controller for clients, use the following command:

```
Device# show wireless client mac-address 6c96.cff2.83a0 detail | inc 11v

11v BSS Transition : implemented
11v DMS Capable : Yes
```

To verify the DMS request and response statistics, use the following command:

```
Device# show wireless stats client detail | inc DMS

Total DMS requests received in action frame      : 0
Total DMS responses sent in action frame         : 0
Total DMS requests received in Re-assoc Request  : 0
Total DMS responses sent in Re-assoc Response    : 0
```

To verify the DMS configuration Cisco Aironet 2700 and 3700 Series APs, use the following command:

```
AP# show controllers dot11Radio 0/1 | begin Global DMS

Global DMS - requests:0 uc:0 drop:408
DMS enabled on WLAN(s): dms-open
 test-open
```

To verify the DMS configuration on the Cisco Aironet 2800, 3800, and 4800 Series APs, use the following command:

```
AP# show multicast dms all

 vapid    client               dmsid        TClas
 0       1C:9E:46:7C:AF:C0     1    mask:0x55, version:4, proto:0x11, dscp:0x0, sport:0,
dport:9, sip:0.0.0.0, dip:224.0.0.251
```

Wireless Broadcast, Non-IP Multicast and Multicast VLAN

Restrictions

- Wireless broadcast does not support VLAN groups.
- When a VLAN pool is mapped to the WLAN profile, support for forwarding non-IPv4 multicast and broadcast is unavailable.
- Non-IPv4 multicasts and broadcasts are restricted to clients on the VLAN mapped to the WLAN and are not forwarded on VLANs returned by AAA override.

Configuring Non-IP Wireless Multicast (CLI)

Before you begin

- The non-IP Multicast feature is disable globally, by default.
- For non-IP multicast, global wireless multicast must be enabled for traffic to pass.
- This feature is not supported in Fabric or Flex deployments.

Procedure

	Command or Action	Purpose
Step 1	**wireless multicast non-ip** **Example:** `Device(config)# wireless multicast non-ip`	Enables non-IP multicast in all the VLANs. By default, the non-IP multicast in all the VLANs is in Disabled state. Wireless multicast must be enabled for the traffic to pass. Use the **no** form of this command to disable non-IP multicast in all the VLANs.

	Command or Action	Purpose
Step 2	**wireless multicast non-ip vlan** *vlanid* **Example:** `Device(config)# wireless multicast non-ip vlan 5`	Enables non-IP multicast per VLAN. By default, non-IP multicast per VLAN is in Disabled state. Both wireless multicast and wireless multicast non-IP must be enabled for traffic to pass. Use the **no** form of this command to disable non-IP multicast per VLAN.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Configuring Wireless Broadcast (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **Multicast**.

Step 2 In the Multicast page, change the status of the **Wireless Broadcast** to enabled to broadcast packets for wireless clients.

The default value is disabled.

Step 3 From the Disabled VLAN table, click the arrow adjecent to the VLAN ID in the **Disabled** state to the **Enabled** state to enable broadcast packets for a VLAN.

The default value is disabled.

Step 4 Save the configuration.

Configuring Wireless Broadcast (CLI)

Before you begin

- This feature is applicable only to non-ARP and DHCP broadcast packets.
- This feature is disable globally, by default.
- This feature is not supported in Fabric or Flex deployments.

Procedure

	Command or Action	Purpose
Step 1	**wireless broadcast** **Example:** `Device(config)# wireless broadcast`	Enables broadcast packets for wireless clients. By default, the broadcast packets for wireless clients is in Disabled state. Enabling **wireless broadcast** enables broadcast traffic for each

	Command or Action	Purpose
		VLAN. Use the **no** form of this command to disable broadcasting packets.
Step 2	**wireless broadcast vlan** *vlanid* **Example:** `Device(config)# wireless broadcast vlan 3`	Enables broadcast packets for single VLAN. By default, the Broadcast Packets for a Single VLAN feature is in Disabled state. Wireless broadcast must be enabled for broadcasting. Use the **no** form of this command to disable broadcast traffic for each VLAN.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Configuring Multicast-over-Multicast for AP Multicast Groups (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap capwap multicast** *IP address* **Example:** `Device(config)# ap capwap multicast 239.4.4.4`	Configures an all-AP multicast group to send a single packet to all the APs.
Step 2	**wireless multicast** *IP address* **Example:** `Device(config)# wireless multicast 239.4.4.4`	Enables Multicast-over-Multicast for multicasting client multicast group traffic to all the APs through the underlying all-AP multicast group. *IP address*—Multicast-over-multicast IP address.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Verifying Wireless Multicast

Table 13: Commands for Verifying Wireless Multicast

Command	Description
show wireless multicast	Displays the multicast status and IP multicast mode, and each VLAN's broadcast and non-IP multicast status. Also displays the Multicast Domain Name System (mDNS) bridging state.

Command	Description
show wireless multicast group summary	Displays all (Group and VLAN) lists and the corresponding MGID values.
show wireless multicast [**source** *source*] **group** *group* **vlan** *vlanid*	Displays details of the specified (S,G,V) and shows all the clients associated with and their MC2UC status.
show ip igmp snooping wireless mcast-ipc-count	Displays the number of multicast IPCs per MGID sent to the wireless controller module.
show ip igmp snooping wireless mgid	Displays the MGID mappings.
show ip igmp snooping igmpv2-tracking	Displays the client-to-SGV mappings and the SGV-to-client mappings.
show ip igmp snooping querier vlan *vlanid*	Displays the IGMP querier information for the specified VLAN.
show ip igmp snooping querier detail	Displays the detailed IGMP querier information of all the VLANs.
show ipv6 mld snooping querier vlan *vlanid*	Displays the MLD querier information for the specified VLAN.
show ipv6 mld snooping wireless mgid	Displays MGIDs for the IPv6 multicast group.

Multicast Optimization

Multicast used to be based on the group of the multicast addresses and the VLAN as one entity, MGID. With the VLAN group, duplicate packets might increase. Using the VLAN group feature, every client listens to the multicast stream on a different VLAN. As a result, the device creates different MGIDs for each multicast address and the VLAN. Therefore, the upstream router sends a copy for each VLAN, which results in as many copies as the number of VLANs in the group. Because the WLAN remains the same for all the clients, multiple copies of the multicast packet are sent over the wireless network. To suppress the duplication of a multicast stream on the wireless medium between the device and the access points, the multicast optimization feature can be used.

Multicast optimization enables you to create a multicast VLAN that can be used for multicast traffic. One of the VLANs in the device can be configured as a multicast VLAN where multicast groups are registered. The clients are allowed to listen to a multicast stream on the multicast VLAN. The MGID is generated using the mulicast VLAN and multicast IP addresses. If multiple clients on different VLANs of the same WLAN are listening to a single multicast IP address, a single MGID is generated. The device makes sure that all the multicast streams from the clients on this VLAN group always go out on the multicast VLAN to ensure that the upstream router has one entry for all the VLANs of the VLAN group. Only one multicast stream hits the VLAN group even if the clients are on different VLANs. Therefore, the multicast packets that are sent out over the network is just one stream.

Configuring IP Multicast VLAN for WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** and **Description**.

Step 4 Enable the **Central Switching** and **Central Association** toggle buttons.

Step 5 In the **Access Policies** tab, under the **VLAN** settings, choose the vlans from the **VLAN/VLAN Group** drop-down list and enter the **Multicast VLAN**.

Step 6 Click **Apply to Device**.

Configuring IP Multicast VLAN for WLAN

Before you begin

- This feature is not supported in Fabric or Flex deployments.
- Multicast VLAN is used for both IPv4 and IPv6 multicast forwarding to APs.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**central association** **Example:** `Device(config-wireless-policy)# central association`	Configures central association for locally switched clients.
Step 4	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures WLAN for central switching.

	Command or Action	Purpose
Step 5	**description** *policy-profile-name* **Example:** `Device(config-wireless-policy)# description "test"`	(Optional) Adds a description for the policy profile.
Step 6	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan 32`	Assigns the profile policy to the VLAN.
Step 7	**multicast vlan** *vlan-id* **Example:** `Device(config-wireless-policy)# multicast vlan 84`	Configures multicast for the VLAN.
Step 8	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the profile policy.

Verifying the Multicast VLAN Configuration

To view the multicast VLAN associated with a policy profile along with the VLAN assigned to that profile, use the following command:

```
Device# show wireless profile policy detail default-policy-profile

Policy Profile Name           : default-policy-profile
Description                   : default policy profile
Status                        : ENABLED
VLAN                          : vlan-pool1
Multicast VLAN        : 84
Client count                  : 0
Passive Client                : DISABLED
```

To view the multicast VLAN associated with a client, use the following command:

```
Device# show wireless client mac ac2b.6e4b.551e detail

Client MAC Address : ac2b.6e4b.551e
Client IPv4 Address : 84.84.0.20
…….
VLAN : 82
Access VLAN : 82
Multicast VLAN: 84
```

Multicast Filtering

Information About Multicast Filtering

The Multicast Filtering feature is disabled by default.

Configuring Multicast Filtering

Perform the procedure given here to create a policy profile and then enable Multicast Filtering on a WLAN:

Before you begin

Create a WLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 3	**multicast filter** **Example:** `Device(config-wireless-policy)#multicast filter`	Configures a multicast filter. (Use the **no** form of this command to disable the feature.)

What to do next

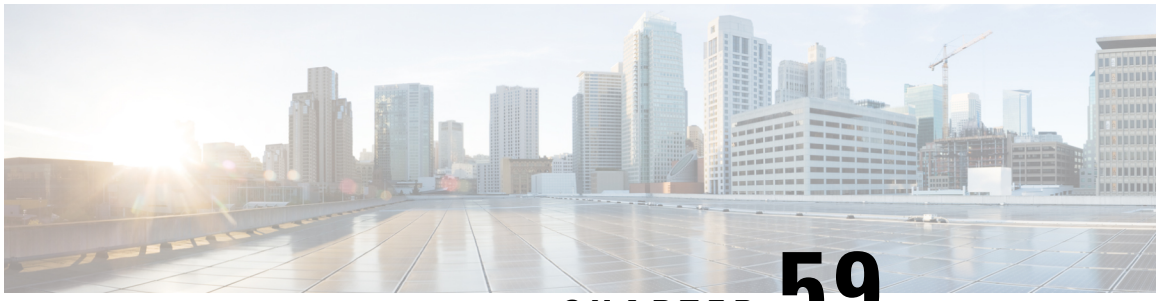
1. Create a policy tag. For more information about creating policy tags, see *Configuring a Policy Tag (CLI)*.
2. Map the policy tag to an AP. For more information about mapping a policy tag to an AP, see *Attaching a Policy Tag and Site Tag to an AP (CLI)*.

Verifying Multicast Filtering

To verify if multicast filtering is enabled, use the **show wireless profile policy detailed** *named-policy-profile* command:

```
Device# show wireless profile policy detailed named-policy-profile
Policy Profile Name                : named-policy-profile
Description                        :
Status                             : DISABLED
```

```
VLAN                                : 91
Multicast VLAN                      : 0
OSEN client VLAN                    :
Multicast Filter                    : ENABLED
```



CHAPTER 59

Map-Server Per-Site Support

- Information About Map Server Per Site Support, on page 455
- Configuring the Default Map Server (GUI), on page 456
- Configuring the Default Map Server (CLI), on page 456
- Configuring a Map Server Per Site (GUI), on page 457
- Configuring a Map Server Per Site (CLI), on page 457
- Creating a Map Server for Each VNID (GUI), on page 458
- Creating a Map Server for Each VNID, on page 458
- Creating a Fabric Profile and Associating a Tag and VNID (GUI), on page 459
- Creating a Fabric Profile and Associating a Tag and VNID (CLI), on page 459
- Verifying the Map Server Configuration, on page 460

Information About Map Server Per Site Support

The Map Server Per Site feature supports per-site map server and the selection of map server based on the client's subnet. This enables the controller to support multiple sites and to segregate each site's traffic.

This feature is applicable to both Enterprise and Guest map servers. For the Layer 2 virtual extensible LAN network identifier-based (L2VNID-based) map server, the appropriate map server should be selected based on the L2 VNID.

The following list shows the map server selection order for AP query and client registration:

- Per-L3 VNID map server
- Per site (ap-group) map server
- Default or global map server

Benefits

Some of the benefits of using Map Server Per Site feature are listed below:

- You can use a single large site with horizontal scaling of the map server and border nodes.
- You can share the controller across multiple sites, with each site can having its own map server and virtual network or VNID and still segment traffic from each site.
- You can share Guest map-server across multiple sites while keeping the Enterprise map-server separate.

- You can use the same SSID across different sites. Within a site, they can belong to a different virtual network domain.

Configuring the Default Map Server (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Fabric**.

Step 2 On the **Fabric** page, click the **Control Plane** tab.

Step 3 In the **Control Plane Name** list, click **default-control-plane**.

Step 4 In the **Edit Control Plane** window that is displayed, click **Add**.

Step 5 Enter the IP address of the map server.

Step 6 Set the **Password Type** as either **Unencrypted** or **AES**.

Step 7 Enter the **Pre Shared Key**.

Step 8 Click **Save**.

Step 9 Click **Update & Apply to Device**.

Configuring the Default Map Server (CLI)

Follow the procedure given below to configure the default map server.

Before you begin

- The global map server is the default map server that is used for both AP query (when an AP joins) as well as for client registration (when a client joins).
- We recommend that you configure map servers in pairs to ensure redundancy because s the LISP control-plane does not support redundancy inherently.
- To share a map server set, create a map server group, which can be shared across site profiles, fabric profiles, Layer 2 and Layer3 VNID, as well with the default map server.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless fabric control-plane** *control-plane-name*	Configures the control plane name.

	Command or Action	Purpose
	Example: `Device(config)# wireless fabric control-plane test-map`	If you do not provide a control plane name, the default-control-plane that is auto generated is used.
Step 3	**ip address** *ip-address* **key** *pre-shared-key* **Example:** `Device((config-wireless-cp)#ip address 10.12.13.14 key secret`	Configures IP address and the key for the control plane.

Configuring a Map Server Per Site (GUI)

Before you begin

Ensure that you have configured an AP Join Profile prior to configuring the primary and backup controllers.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join Profile** page, click the AP Join Profile name.

Step 3 In the **Edit AP Join Profile** window, click the **CAPWAP** tab.

Step 4 In the **High Availability** tab under **Backup Controller Configuration**, check the **Enable Fallback** check box.

Step 5 Enter the primary and secondary controller names and IP addresses.

Step 6 Click **Update & Apply to Device**.

Configuring a Map Server Per Site (CLI)

Follow the procedure given below to configure per-site MAP server under site-tag.

Before you begin

You can configure map server for each site or each AP group. . If a map server is not configured for each VNID or subnet, per-site map server is used for AP queries and client registration.

Procedure

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

	Command or Action	Purpose
Step 2	**wireless tag site** *site-tag* **Example:** `Device(config)# wireless tag site test-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**fabric control-plane** *map-server-name* **Example:** `Device(config-wireless-site)# fabric control-plane test-map`	Associates a fabric control plane name with a site tag.

Creating a Map Server for Each VNID (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless Plus** > **Fabric** > **Fabric Configuration**.
Step 2 In the **Profiles** tab, click **Add** to add a new Fabric Profile.
Step 3 In the **Add New Profile** window that is displayed, enter a name and description for the profile.
Step 4 Specify the L2 VNID and SGT Tag details.
Step 5 In the **Map Servers** section, specify the IP address and preshared key details for Server 1.
Step 6 Optionally, you can specify the IP address and preshared key details for Server 2.
Step 7 Click **Save & Apply to Device.**

Creating a Map Server for Each VNID

Follow the procedure given below to configure map server for each VNID in Layer 2 and Layer 3 or a map server for a client VNID.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	Choose one of the following: • **wireless fabric name** *vnid-map* **l2-vnid** *l2-vnid* **l3-vnid** *l3vnid* **ip** *network-ip subnet-mask* **control-plane** *control-plane-name*	Configures a map server for each VNID in Layer 2 and Layer 3 or a map server for a client VNID.

	Command or Action	Purpose

	• **wireless fabric name** *vnid-map* **l2-vnid** *l2-vnid* **control-plane** *control-plane-name*
	Example:
	`Device(config)# wireless fabric name test1 l2-vnid 12 l3-vnid 10 ip 10.8.6.2 255.255.255.236 control-plane cp1`
	Example:
	`Device(config)# wireless fabric name test1 l2-vnid 22 control-plane cp1`	

Creating a Fabric Profile and Associating a Tag and VNID (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless** > **Fabric**.

Step 2 In the **Profiles** tab on **Fabric Configuration** page, click **Add** to add a new profile.

Step 3 In the **Add New Profile** window that is displayed, enter a name and description for the profile.

Step 4 Specify the L2 VNID and SGT Tag details.

Step 5 Click **Save & Apply to Device**.

Creating a Fabric Profile and Associating a Tag and VNID (CLI)

Follow the procedure given below to create a fabric profile and associate the VNID to which the client belongs and the SGT tag to this profile.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile fabric** *fabric-profile-name* **Example:** `Device(config)# wireless profile fabric test-fabric`	Configures a fabric profile.
Step 3	**sgt-tag** *value* **Example:**	Configures an SGT tag.

	Command or Action	Purpose
	`Device(config-wireless-fabric)# sgt-tag 5`	
Step 4	**client-l2-vnid** *vnid* **Example:** `Device(config-wireless-fabric)# client-l2-vnid 10`	Configures a client Layer 2 VNID.

Verifying the Map Server Configuration

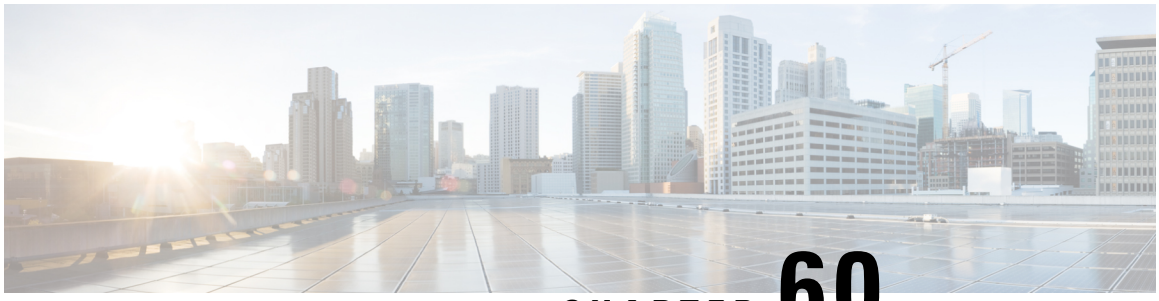
Use the following commands to verify the map server configuration:

```
Device# show wireless fabric summary

Fabric Status      : Enabled


Control-plane:
Name                              IP-address        Key                               Status
-------------------------------------------------------------------------------------------
test-map                          10.12.13.14       test1                             Down


Fabric VNID Mapping:
  Name               L2-VNID        L3-VNID        IP Address             Subnet
Control plane name
-------------------------------------------------------------------------------------------------------

  test1               12             10             10.6.8.9            255.255.255.236
 test2


Device# show wireless fabric vnid mapping

Fabric VNID Mapping:
  Name               L2-VNID        L3-VNID        IP Address             Subnet      Control
 Plane Name
-------------------------------------------------------------------------------------------------------

  fabric1             1              0              9.6.51.0            255.255.255.0
     map-server-name

Device# show wireless profile fabric detailed profile-name

Profile-name      : fabric-ap
VNID              : 1
SGT               : 500
Type              : Guest

Control Plane Name       Control-Plane IP   Control-Plane Key
------------------------------------------------------------------------------
 Ent-map-server           5.4.3.2                guest_1

Device# show ap name ap-name config general
```

```
Fabric status                                    : Enabled
RLOC                                             : 2.2.2.2
Control Plane Name  : ent-map-server
```

```
Device# show wireless client mac mac-address detail

Fabric status : Enabled
RLOC                  : 2.2.2.2
Control Plane Name  : ent-map-server
```

```
Device# show wireless tag site detailed site-tag

Site Tag Name        : default-site-tag
Description          : default site tag
---------------------------------------
AP Profile           : default-ap-profile
Local-site           : Yes
Fabric-control-plane: Ent-map-server
```



CHAPTER 60

Volume Metering

The Volume Metering feature allows you to configure the interval at which an access point (AP) updates client accounting statistics to the controller and in turn to the RADIUS server. Currently, the report is sent from an AP to the controller every 90 seconds. With this feature, you can configure the time from 5 to 90 seconds. This helps reduce the delay in accounting data usage by a device.

• Configuring Volume Metering, on page 463

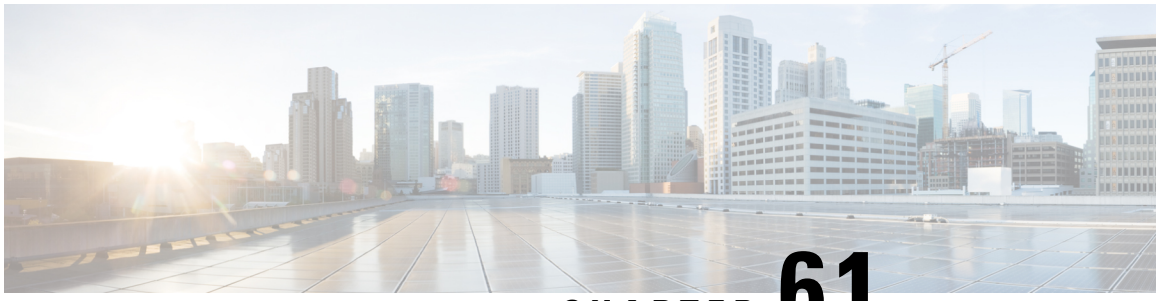
Configuring Volume Metering

Follow the procedure given below to configure volume metering:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile yy-ap-profile`	Configures an AP profile and enters ap profile configuration mode.
Step 3	**dot11 24ghz reporting-interval** *reporting-interval* **Example:** `Device(config-ap-profile)# dot11 24ghz reporting-interval 60`	Configures the dot11 parameters.
Step 4	**dot11 5ghz reporting-interval** *reporting-interval* **Example:** `Device(config-ap-profile)# dot11 5ghz reporting-interval 60`	Configures the dot11 parameters.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config-ap-profile)# exit`	Returns to global configuration mode.
Step 6	**aaa accounting update periodic** *interval-in-minutes* **Example:** `Device(config)# aaa accounting update periodic 75`	Sets the time interval (in minutes) at which the controller sends interim accounting updates of the client to the RADIUS server.
Step 7	**exit** **Example:** `Device(config)# exit`	Exits configuration mode and returns to privileged EXEC mode.



CHAPTER 61

Enabling Syslog Messages in Access Points and Controller for Syslog Server

- Information About Enabling Syslog Messages in Access Points and Controller for Syslog Server, on page 465
- Configuring Syslog Server for an AP Profile, on page 466
- Configuring Syslog Server for the Controller (GUI), on page 468
- Configuring Syslog Server for the Controller , on page 468
- Verifying Syslog Server Configurations, on page 470

Information About Enabling Syslog Messages in Access Points and Controller for Syslog Server

The Syslog server on access points and controller has many levels and facilities.

The following are the Syslog levels:

- Emergencies
- Alerts
- Critical
- Errors
- Warnings
- Notifications
- Informational
- Debugging

The following options are available for the Syslog facility:

- 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.

Configuring Syslog Server for an AP Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters the AP profile configuration mode.

	Command or Action	Purpose
Step 3	**syslog facility** **Example:** `Device(config-ap-profile)# syslog facility`	Configures the facility parameter for Syslog messages.
Step 4	**syslog host** *ip-address* **Example:** `Device(config-ap-profile)# syslog host 9.3.72.1`	Configures the Syslog server IP address and parameters.
Step 5	**syslog level** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**} **Example:** `Device(config-ap-profile)# syslog level`	Configures the Syslog server logging level. The following are the Syslog server logging levels: • **emergencies**—Signifies severity 0. Implies that the system is not usable. • **alerts**—Signifies severity 1. Implies that an immediate action is required. • **critical**—Signifies severity 2. Implies critical conditions. • **errors**—Signifies severity 3. Implies error conditions. • **warnings**—Signifies severity 4. Implies warning conditions. • **notifications**—Signifies severity 5. Implies normal but significant conditions. • **informational**—Signifies severity 6. Implies informational messages. • **debugging**—Signifies severity 7. Implies debugging messages. **Note** To know the number of Syslog levels supported, you need to select a Syslog level. Once a Syslog level is selected, all the levels below it are also enabled. If you enable *critical* Syslog level then all levels below it are also enabled. So, all three of them, namely, *critical*, *alerts*, and *emergencies* are enabled.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Syslog Server for the Controller (GUI)

Procedure

Step 1 Choose **Troubleshooting** > **Logs**.

Step 2 Click **Manage Syslog Servers** button.

Step 3 In **Log Level Settings**, from the **Syslog** drop-down list, choose a security level.

Step 4 From the **Message Console** drop-down list, choose a logging level.

Step 5 In **Message Buffer Configuration**, from the **Level** drop-down list, choose a server logging level.

Step 6 In **IP Configuration** settings, click **Add**.

Step 7 Choose the **Server Type**, from the **IPv4 / IPv6** or **FQDN** option.

Step 8 For Server Type **IPv4 / IPv6**, enter the **IPv4 / IPv6 Server Address**. For Server Type **FQDN**, enter the **Host Name**, choose the IP type and the appropriate **VRF Name** from the drop-down lists.

To delete a syslog server, click 'x' next to the appropriate server entry, under the **Remove** column.

Note When creating a host name, spaces are not allowed.

Step 9 Click **Apply to Device**.

Note When you click on **Apply to Device**, the changes are configured. If you click on **Cancel**, the configurations are discarded.

Configuring Syslog Server for the Controller

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**logging host** {*hostname* | *ipv6*} **Example:**	Enables Syslog server IP address and parameters.

	Command or Action	Purpose
	`Device(config)# logging host 124.3.52.62`	
Step 3	**logging facility** {**auth** | **cron** | **daemon** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **sys10** | **sys11** | **sys12** | **sys13** | **sys14** | **sys9** | **syslog** | **user** | **uucp**} **Example:** `Device(config)# logging facility syslog`	Enables facility parameter for the Syslog messages. You can enable the following facility parameter for the Syslog messages: • **auth**—Authorization system. • **cron**—Cron facility. • **daemon**—System daemons. • **kern**—Kernel. • **local0** to **local7**—Local use. • **lpr**—Line printer system. • **mail**—Mail system. • **news**—USENET news. • **sys10** to **sys14** and **sys9**—System use. • **syslog**—Syslog itself. • **user**—User process. • **uucp**—Unix-to-Unix copy system.
Step 4	**logging trap** {*severity-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**} **Example:** `Device(config)# logging trap 2`	Enables Syslog server logging level. *severity-level*- Refers to the logging severity level. The valid range is from 0 to 7. The following are the Syslog server logging levels: • **emergencies**—Signifies severity 0. Implies that the system is not usable. • **alerts**—Signifies severity 1. Implies that an immediate action is required. • **critical**—Signifies severity 2. Implies critical conditions. • **errors**—Signifies severity 3. Implies error conditions. • **warnings**—Signifies severity 4. Implies warning conditions. • **notifications**—Signifies severity 5. Implies normal but significant conditions.

	Command or Action	Purpose
		• **informational**—Signifies severity 6. Implies informational messages. • **debugging**—Signifies severity 7. Implies debugging messages. **Note** To know the number of Syslog levels supported, you need to select a Syslog level. Once a Syslog level is selected, all the levels below it are also enabled. If you enable *critical* Syslog level then all levels below it are also enabled. So, all three of them, namely, *critical*, *alerts*, and *emergencies* are enabled.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Syslog Server Configurations

Verifying Global Syslog Server Settings for all Access Points

To view the global Syslog server settings for all access points that joins the controller, use the following command:

```
Device# show ap config general
Cisco AP Name : APA0F8.4984.5E48
================================================

Cisco AP Identifier : a0f8.4985.d360
Country Code : IN
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-DN
AP Country Code : IN - India
AP Regulatory Domain
Slot 0 : -A
Slot 1 : -D
MAC Address : a0f8.4984.5e48
IP Address Configuration : DHCP
IP Address : 9.4.172.111
IP Netmask : 255.255.255.0
Gateway IP Address : 9.4.172.1
Fallback IP Address Being Used :
Domain :
Name Server :
CAPWAP Path MTU : 1485
Telnet State : Disabled
SSH State : Disabled
Jumbo MTU Status : Disabled
Cisco AP Location : default location
```

```
Site Tag Name : ST1
RF Tag Name : default-rf-tag
Policy Tag Name : PT3
AP join Profile : default-ap-profile
Primary Cisco Controller Name : WLC2
Primary Cisco Controller IP Address : 9.4.172.31
Secondary Cisco Controller Name : Not Configured
Secondary Cisco Controller IP Address : 0.0.0.0
Tertiary Cisco Controller Name : Not Configured
Tertiary Cisco Controller IP Address : 0.0.0.0
Administrative State : Enabled
Operation State : Registered
AP Certificate type : Manufacturer Installed Certificate
AP Mode : Local
AP VLAN tagging state : Disabled
AP VLAN tag : 0
CAPWAP Preferred mode : Not Configured
AP Submode : Not Configured
Office Extend Mode : Disabled
Remote AP Debug : Disabled
Logging Trap Severity Level : notification
Software Version : 16.10.1.24
Boot Version : 1.1.2.4
Mini IOS Version : 0.0.0.0
Stats Reporting Period : 180
LED State : Enabled
PoE Pre-Standard Switch : Disabled
PoE Power Injector MAC Address : Disabled
Power Type/Mode : PoE/Full Power (normal mode)
Number of Slots : 3
AP Model : AIR-AP1852I-D-K9
IOS Version : 16.10.1.24
Reset Button : Disabled
AP Serial Number : KWC212904UB
Management Frame Protection Validation : Disabled
AP User Mode : Automatic
AP User Name : Not Configured
AP 802.1X User Mode : Global
AP 802.1X User Name : Not Configured
Cisco AP System Logging Host : 9.4.172.116
AP Up Time : 11 days 1 hour 15 minutes 52 seconds
AP CAPWAP Up Time : 6 days 3 hours 11 minutes 6 seconds
Join Date and Time : 09/05/2018 04:18:52
Join Taken Time : 3 minutes 1 second
Join Priority : 1
Ethernet Port Duplex : Auto
Ethernet Port Speed : Auto
AP Link Latency : Disable
AP Lag Configuration Status : Disabled
AP Lag Operational Status : Disabled
Lag Support for AP : Yes
Rogue Detection : Enabled
Rogue Containment auto-rate : Disabled
Rogue Containment of standalone flexconnect APs : Disabled
Rogue Detection Report Interval : 10
Rogue AP minimum RSSI : -90
Rogue AP minimum transient time : 0
AP TCP MSS Adjust : Enabled
AP TCP MSS Size : 1250
AP IPv6 TCP MSS Adjust : Enabled
AP IPv6 TCP MSS Size : 1250
Hyperlocation Admin Status : Disabled
Retransmit count : 5
Retransmit interval : 3
```

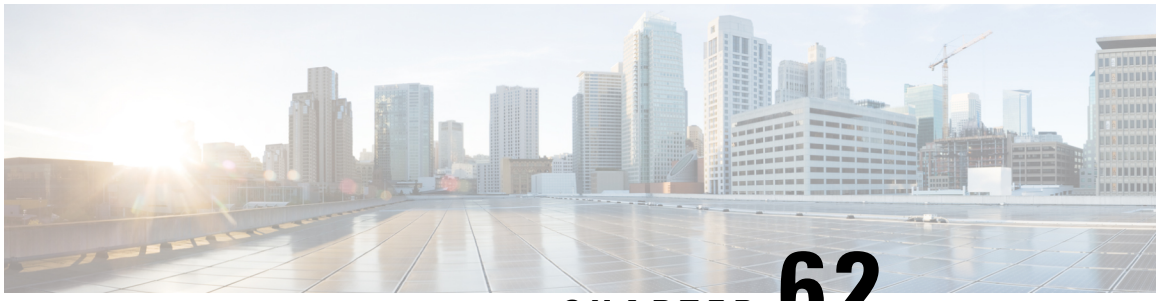
```
Fabric status : Disabled
FIPS status : Disabled
WLANCC status : Disabled
USB Module Type : USB Module
USB Module State : Enabled
USB Operational State : Disabled
USB Override : Disabled
Lawful-Interception Admin status : Disabled
Lawful-Interception Oper status : Disabled
```

Verifying Syslog Server Settings for a Specific Access Point

To view the Syslog server settings for a specific access point, use the following command:

```
Device# show ap name <ap-name> config general
show ap name APA0F8.4984.5E48 config general
Cisco AP Name : APA0F8.4984.5E48
================================================

Cisco AP Identifier : a0f8.4985.d360
Country Code : IN
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-DN
AP Country Code : IN - India
AP Regulatory Domain
Slot 0 : -A
Slot 1 : -D
MAC Address : a0f8.4984.5e48
IP Address Configuration : DHCP
IP Address : 9.4.172.111
IP Netmask : 255.255.255.0
Gateway IP Address : 9.4.172.1
Fallback IP Address Being Used :
Domain :
Name Server :
CAPWAP Path MTU : 1485
Telnet State : Disabled
SSH State : Disabled
Jumbo MTU Status : Disabled
Cisco AP Location : default location
Site Tag Name : ST1
RF Tag Name : default-rf-tag
Policy Tag Name : PT3
AP join Profile : default-ap-profile
Primary Cisco Controller Name : WLC2
Primary Cisco Controller IP Address : 9.4.172.31
Secondary Cisco Controller Name : Not Configured
Secondary Cisco Controller IP Address : 0.0.0.0
Tertiary Cisco Controller Name : Not Configured
Tertiary Cisco Controller IP Address : 0.0.0.0
Administrative State : Enabled
Operation State : Registered
AP Certificate type : Manufacturer Installed Certificate
AP Mode : Local
AP VLAN tagging state : Disabled
AP VLAN tag : 0
CAPWAP Preferred mode : Not Configured
AP Submode : Not Configured
Office Extend Mode : Disabled
Remote AP Debug : Disabled
Logging Trap Severity Level : notification
Software Version : 16.10.1.24
Boot Version : 1.1.2.4
Mini IOS Version : 0.0.0.0
Stats Reporting Period : 180
```

```
LED State : Enabled
PoE Pre-Standard Switch : Disabled
PoE Power Injector MAC Address : Disabled
Power Type/Mode : PoE/Full Power (normal mode)
Number of Slots : 3
AP Model : AIR-AP1852I-D-K9
IOS Version : 16.10.1.24
Reset Button : Disabled
AP Serial Number : KWC212904UB
Management Frame Protection Validation : Disabled
AP User Mode : Automatic
AP User Name : Not Configured
AP 802.1X User Mode : Global
AP 802.1X User Name : Not Configured
Cisco AP System Logging Host : 9.4.172.116
AP Up Time : 11 days 1 hour 15 minutes 52 seconds
AP CAPWAP Up Time : 6 days 3 hours 11 minutes 6 seconds
Join Date and Time : 09/05/2018 04:18:52
Join Taken Time : 3 minutes 1 second
Join Priority : 1
Ethernet Port Duplex : Auto
Ethernet Port Speed : Auto
AP Link Latency : Disable
AP Lag Configuration Status : Disabled
AP Lag Operational Status : Disabled
Lag Support for AP : Yes
Rogue Detection : Enabled
Rogue Containment auto-rate : Disabled
Rogue Containment of standalone flexconnect APs : Disabled
Rogue Detection Report Interval : 10
Rogue AP minimum RSSI : -90
Rogue AP minimum transient time : 0
AP TCP MSS Adjust : Enabled
AP TCP MSS Size : 1250
AP IPv6 TCP MSS Adjust : Enabled
AP IPv6 TCP MSS Size : 1250
Hyperlocation Admin Status : Disabled
Retransmit count : 5
Retransmit interval : 3
Fabric status : Disabled
FIPS status : Disabled
WLANCC status : Disabled
USB Module Type : USB Module
USB Module State : Enabled
USB Operational State : Disabled
USB Override : Disabled
Lawful-Interception Admin status : Disabled
Lawful-Interception Oper status : Disabled
```



CHAPTER 62

Software Maintenance Upgrade

- Introduction to Software Maintenance Upgrade, on page 475
- Information About AP Device Package, on page 480
- Information About Per Site or Per AP Model Service Pack (APSP), on page 483

Introduction to Software Maintenance Upgrade

Software Maintenance Upgrade (SMU) is a package that can be installed on a system to provide a patch fix or a security resolution to a released image. A SMU package is provided for each release and per component basis, and is specific to the corresponding platform.

A SMU provides a significant benefit over classic Cisco IOS software because it allows you to address the network issue quickly while reducing the time and scope of the testing required. The Cisco IOS XE platform internally validates the SMU compatibility and does not allow you to install noncompatible SMUs.

All the SMUs are integrated into the subsequent Cisco IOS XE software maintenance releases. A SMU is an independent and self-sufficient package and does not have any prerequisites or dependencies. You can choose which SMUs to install or uninstall in any order.

Note SMUs are supported only on Extended Maintenance releases and for the full lifecycle of the underlying software release.

Note You can activate the file used in the **install add file** command only from the filesystems of the active device. You cannot use the file from the standby or member filesystems; the **install add file** command will fail in such instances.

Note When the SMU file is deleted and a reboot is performed, the device may display the following error message:

```
--- Starting SMU Add operation ---
Performing SMU_ADD on all members
    FAILED: Improper State./bootflash/<previously-installed-smu-filename>.smu.bin not
present. Please restore file for stability.
Checking status of SMU_ADD on [1/R0]
SMU_ADD: Passed on []. Failed on [1/R0]
Finished SMU Add operation
FAILED: add_activate_commit /bootflash/<tobeinstalled-wlc-smu-filename>.smu.bin Wed Aug 02
 08:30:18 UTC 2023.
```

This error occurs because the previous SMU file was not properly removed from the controller. It may lead to functional errors, such as the inability to install new SMU or APSP files.

We recommend that you use the install remove file command to remove previous instances of APSP or SMU files from the bootflash.

SMU infrastructure can be used to meet the following requirements in the wireless context:

- Controller SMU: Controller bug fixes or Cisco Product Security Incident Response information (PSIRT).
- APSP: AP bug fixes, PSIRTs, or minor features that do not require any controller changes.
- APDP: Support for new AP models without introduction of new hardware or software capabilities.

Note The **show ap image** command displays cumulative statistics regarding the AP images in the controller. We recommend that you clear the statistics using the **clear ap predownload statistics** command, before using the **show ap image** command, to ensure that correct data is displayed.

SMU Workflow

The SMU process should be initiated with a request to the SMU committee. Contact your customer support to raise an SMU request. During the release, the SMU package is posted on the Cisco Software Download page and can be downloaded and installed.

SMU Package

An SMU package contains the metadata and fix for the reported issue the SMU is requested for.

SMU Reload

The SMU type describes the effect on a system after installing the corresponding SMU. SMUs can be nontraffic-affecting or can result in device restart, reload, or switchover.

A controller cold patch require a cold reload of the system during activation. A cold reload is the complete reload of the operating system. This action affects the traffic flow for the duration of the reload (~5 min). This reload ensures that all the processes are started with the correct libraries and files that are installed as part of the corresponding SMU.

Controller hot patching support allows the SMU to be effective immediately after activation, without reloading the system. After the SMU is committed, the activation changes are persistent across reloads. Hot patching

SMU packages contain metadata that lists all processes that need to be restarted in order to activate the SMU. During SMU activation, each process in this list will be restarted one at a time until the SMU is fully applied.

Installing a SMU (GUI)

Procedure

Step 1 Choose **Administration** > **Software Management** and click the **Software Maintenance Upgrade** tab.

Step 2 Click **Add** to add a SMU image.

Step 3 From the **Transport Type** drop-down list, choose the transfer type to transfer the software image to your device as TFTP, SFTP, FTP, Device, or Desktop (HTTP).

a) If you choose **TFTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **File path** and choose a **File System** from the drop-down list. For example, if the SMU file is at the root of the TFTP server you can enter `/C9800-universalk9_wlc.17.03.02a.CSCvw55275.SPA.smu.bin` in the **File path** field.

b) If you choose **SFTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **SFTP Username**, **SFTP Password**, **File path** and choose a **File System** from the drop-down list.

c) If you choose **FTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **FTP Username**, **FTP Password**, **File path**, and choose a **File System** from the drop-down list.

d) If you choose **Device** as the **Transport Type**, you need to enter the **File path** and choose a **File System** from the drop-down list. This is possible when the software is already present on the device due to an earlier download and activation, followed by a subsequent deactivation.

Note The File System depends upon the kind of device you are using. On physical controllers, you have the option to store the file to the bootflash or hard disk, whereas in case of virtual controllers, you can only store it in the bootflash.

e) If you choose **Desktop (HTTPS)** as the **Transport Type**, you need to choose a **File System** from the drop-down list and click **Select File** to navigate to the **Source File Path**.

Step 4 Enter the **File Name** and click **Add File**.

This operation copies the maintenance update package from the location you selected above to the device and performs a compatibility check for the platform and image versions and adds the SMU package for all the members. After a SMU is successfully added to the system, a message is displayed about the successful operation and that the SMU can be activated on the device. The message displays the name of the package (SMU) that is now available to be activated. It lists the SMU Details - Name, Version, State (active or inactive), Type (reload, restart, or non-reload) and other compatibility details. If SMU is of the Type - reload, then any operation (activate, deactivate or rollback) will cause the device to reload; restart involves only a process restart and if it is non reload- no change in process takes place.

Step 5 Select the SMU and click on **Activate** to activate the SMU on the system and install the package, and update the package status details.

Step 6 Select the SMU and click **Commit** to make the activation changes persistent across reloads.

The Commit operation creates commit points. These commit points are similar to snapshots using which you can determine which specific change you want to be activated or rolled back to, in case there is any issue with

the SMU. The commit can be done after activation when the system is up, or after the first reload. If a package is activated, but not committed, it remains active after the first reload, but not after the second reload.

Installing SMU

Procedure

	Command or Action	Purpose
Step 1	**install add file bootflash:** *filename* **Example:** `Device# install add file bootflash:<Filename>`	Copies the maintenance update package from a remote location to the device, and performs a compatibility check for the platform and image versions. This command runs base compatibility checks on a file to ensure that the SMU package is supported on the platform. It also adds an entry in the package/SMU.sta file, so that its status can be monitored and maintained.
Step 2	**install activate file bootflash:** *filename* **Example:** `Device# install activate file bootflash:<Filename>`	Runs compatibility checks, installs the package, and updates the package status details. For a restartable package, the command triggers the appropriate post-install scripts to restart the necessary processes, and for non-restartable packages it triggers a reload.
Step 3	**install commit** **Example:** `Device# install commit`	Commits the activation changes to be persistent across reloads. The commit can be done after activation while the system is up, or after the first reload. If a package is activated but not committed, it remains active after the first reload, but not after the second reload.
Step 4	**show version** **Example:** `Device# show version`	Displays the image version on the device.
Step 5	**show install summary** **Example:** `Device# show install summary`	Displays information about the active package. The output of this command varies according to the install commands that are configured.

Roll Back an Image (GUI)

Procedure

Step 1 Choose **Administration** > **Software Management**.
Step 2 Go to **SMU**, **APSP** or **APDP**.
Step 3 Click **Rollback**.
Step 4 In the **Rollback to** drop-down list, choose **Base**, **Committed** or **Rollback Point**.
Step 5 Click **Add File**.

Rollback SMU

Procedure

	Command or Action	Purpose
Step 1	**install rollback to** {**base** | **committed** | **id** | **committed** } *committed ID* **Example:** `Device(config)# install rollback to id 1234`	Returns the device to the previous installation state. After the rollback, a reload is required.
Step 2	**install commit** **Example:** `Device# install commit`	Commits the activation changes to be persistent across reloads.

Deactivate SMU

Procedure

	Command or Action	Purpose
Step 1	**install deactivate file bootflash:** *filename* **Example:** `Device# install deactivate file bootflash:<Filename>`	Deactivates an active package, updates the package status, and triggers a process to restart or reload.
Step 2	**install commit** **Example:** `Device# install commit`	Commits the activation changes to be persistent across reloads.

Configuration Examples for SMU

The following is sample of the SMU configuration, after the install add for the SMU is done:

```
Device#show install summary

[ Chassis 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------

IMG   C    16.8.1.0.39751

--------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------
```

Information About AP Device Package

The controller supports rolling out critical bug fixes using Software Maintenance Upgrade (SMU). Similarly, if any new AP hardware model is introduced, the AP models need to be connected to the existing wireless network.

Currently, when a new AP hardware model is introduced, those get shipped along with the corresponding controller related major software version. Then you need to wait for the release of a corresponding controller version relative to the new AP model and upgrade the entire network.

From 16.11.1 onwards, you can introduce the new AP model into your wireless network using the SMU infrastructure without the need to upgrade to the new controller version. This solution is termed as AP Device Package (APDP).

SMU Process or Workflow

The SMU process builds APDP to detect code changes and build APDP. It also supports addition of a new file (AP image file) to APDP and inclusion of those AP images into APDP.

The workflow is as follows:

- install add
- install prepare activate
- install activate
- install commit

For more details, see *Managing AP Device Package*.

Note To ensure completion of the APSP or APDP activation or deactivation process, ensure that you run the **install commit** command after the **install activate** or **install deactivate** command. Failing to do so within 6 hours of the deactivate operation terminates the deactivate operation and moves it back to the original commit position.

SMU Package

A SMU package contains the metadata that carry AP model and its capability related details.

AP Image Changes

When new AP models are introduced, there may or may not be corresponding new AP images. This means that AP images are mapped to the AP model families. If a new AP model belongs to an existing AP model family then you will have existing AP image entries (Example: ap3g3, ap1g5, and so on). For instance, if an AP model belongs to either ap3g3 or ap1g5, the respective image file is updated with the right AP image location. Also, the corresponding metadata file is updated with the new AP model capability information.

If a new AP model belongs to a new AP model family and new image file, the new image entry file is created in the right AP image location. Also, the corresponding metadata file is updated with the new AP model capability information.

During AP image bundling and packaging of APDP, the new AP model images and metadata file are packaged into APDP.

Note The APDP images must not be renamed to avoid impact on its functionality.

Installing AP Device Package (GUI)

Procedure

Step 1 Choose **Administration** > **Software Management**.

Step 2 Click **AP Device Package (APDP)** tab.

Step 3 Click **Add**.

Step 4 From the **Transport Type** drop-down list, choose the transfer type to transfer the software image to your device as TFTP, SFTP, FTP, Device, or Desktop (HTTP).

a) If you choose **TFTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **File path** and choose a **File System** from the drop-down list.

b) If you choose **SFTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **SFTP Username**, **SFTP Password**, **File path** and choose a **File System** from the drop-down list.

c) If you choose **FTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **FTP Username**, **FTP Password**, **File path**, and choose a **File System** from the drop-down list.

d) If you choose **Device** as the **Transport Type**, you need to enter the **File path** and choose a **File System** from the drop-down list.

e) If you choose **Desktop (HTTPS)** as the **Transport Type**, you need to choose a **File System** from the drop-down list and click **Select File** to navigate to the **Source File Path**.

Step 5 Enter the **File Name** and click **Add File**.

Step 6 From the **AP Upgrade Configuration** section, choose the percentage of APs to be included from the **AP Upgrade per iteration** drop-down list.

Step 7 Click **Apply**.

Installing AP Device Package (CLI)

Procedure

	Command or Action	Purpose
Step 1	**install add file bootflash:** *filename* **Example:** `Device# install add file bootflash:<Filename>`	Extracts AP images from APDP and places them in SMU or APDP specific mount location. **Note** Here, the SMU does not trigger the Wireless module.
Step 2	**install prepare activate file bootflash:** *filename* **Example:** `Device# install prepare activate file bootflash:<Filename>`	Prepares the AP software in APDP to the existing current active AP image list.
Step 3	**install activate file bootflash:** *filename* **Example:** `Device# install activate file bootflash:<Filename>`	Adds the AP software in APDP to the existing current active AP image list. Also, updates the capability information for the new AP models in the controller . **Note** Even if the new AP module supports new hardware capabilities, the controller recognizes only the capability information that its base version supports. At this point, the controller accepts the new connection from the new AP model. The new AP model then joins the controller .
Step 4	**install commit** **Example:** `Device# install commit`	Commits the new AP software to be persistent across reloads. The commit can be done after activation while the system is up, or after the first reload. If a package is activated but not committed, it remains active after the first reload, but not after the second reload.
Step 5	**install prepare deactivate file bootflash:** *filename* **Example:** `Device# install prepare deactivate file bootflash:<Filename>`	Prepares and deactivates an active APDP, and updates the package status.

	Command or Action	Purpose
Step 6	**install deactivate file bootflash:** *filename* **Example:** `Device# install deactivate file bootflash:<Filename>`	(Optional) Deactivates an active APDP, updates the package status, and triggers a process to restart or reload.
Step 7	**show version** **Example:** `Device# show version`	Displays the image version on the device.

Verifying APDP on the Controller

To verify the status of APDP packages on the controller , use the following command:

```
Device# show install summary

[ Chassis 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
APDP  I    bootflash:apdp_CSCvp12345.bin
IMG   C    17.1.0.0
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

Note The output of this command varies based on the packages, and the package states that are installed.

Information About Per Site or Per AP Model Service Pack (APSP)

The controller supports critical updates to the access points (APs) using Software Maintenance Update (SMU). Using the Per Site or Per AP Model Service Pack feature, you can roll out critical AP bug fixes to a subset of APs, on a site or group of sites, using SMU in a staggered manner.

This feature allows to control the propagation of a SMU in your network by selecting the sites, to be included in the SMU activation, using Per Site AP SMU rollout. However, all sites should be brought to the same SMU level before a new SMU can be rolled out to a subset of sites or for a subsequent image upgrade to be initiated on the system..

Using Per AP model SMU, you can limit the update to only certain AP models. The software is predownloaded and is activated only to certain AP models, within a site. Note that if a certain number of model images are included in a SMU, all the future updates must contain software images for those models.

This feature is supported in the flex-connect mode, local mode, and Software-Defined Access (SD-Access) wireless scenarios.

Note After applying the AP site filter for per site SMU upgrade, a new image installation will not be allowed without applying the site filter to all the other sites, or removing the existing site filter.

Workflow of AP SMU Upgrade

- Run a query to check whether there are ongoing activities, such as AP image predownload or AP rolling upgrade.
- Identify the site or sites to install the SMU in, and set up a site filter.
- Trigger the predownload of SMU to the sites in the site filter.
- Activate the SMU after the predownload is complete.
- Commit the update.

Note You can add more sites to a filter after setting up the filter. However, you have to apply the filter again using the **ap image site-filter file** *file-name* **apply** command. If you clear the site filter, the update is made on all the remaining sites. Deactivation and rollback of the images are not filtered per site, and are applicable to all the sites.

Rolling AP Upgrade

Rolling AP upgrade is a method of upgrading the APs in a staggered manner such that some APs are always up in the network and provide seamless coverage to clients, while the other APs are selected to be upgraded.

Note The AP images should be downloaded before the rolling upgrade is triggered, so that all the APs that are to be upgraded have the new image version.

Rolling AP Upgrade Process

Rolling AP upgrade is done on a per controller basis. The number of APs to be upgraded at a given time, is the percentage of the total number of APs that are connected to the controller. The percentage is capped at a user configured value. The default percentage is 15. The non-client APs will be upgraded before the actual upgrade of APs begin.

The upgrade process is as follows:

1. **Candidate AP Set Selection**

   In this stage, a set of AP candidates are selected based on neighbouring AP information. For example, if you identify an AP for upgrade, a certain number (N) of its neighbours are excluded from candidate selection. The N values are generated in the following manner:

   If the user configurable capped percentage is 25%, then N=6 (Expected number of iterations =5)

   If the user configurable capped percentage is 15%, then N=12 (Expected number of iterations=12)

If the user configurable capped percentage is 5%, then N=24 (Expected number of iterations =22)

If the candidates cannot be selected using the neighbouring AP information, select candidates from indirect neighbours. If you still are not able to select candidates, the AP will be upgraded successfully without any failure.

Note After the candidates are selected, if the number of candidates are more than the configured percentage value, the extra candidates are removed to maintain the percentage cap.

2. **Client Steering**

   Clients that are connected to the candidate APs are steered to APs that are not there in the candidate AP list, prior to rebooting the candidate APs. The AP sends out a request to each of its associated clients with a list of APs that are best suited for them. This does not include the candidate APs. The candidate APs are marked as unavailable for neighbour lists. Later, the markings are reset in the AP rejoin and reload process.

3. **AP Rejoin and Reload Process**

   After the client steering process, if the clients are still connected to the candidate AP, the clients are sent a de-authorization and the AP is reloaded and comes up with a new image. A three-minute timer is set for the APs to rejoin. When this timer expires, all the candidates are checked and marked if they have either joined the controller or the mobility peer. If 90% of the candidate APs have joined, the iteration is concluded; if not, the timer is extended to three more minutes. The same check is repeated after three minutes. After checking thrice, the iteration ends and the next iteration begins. Each iteration may last for about 10 minutes.

   For rolling AP upgrade, there is only one configuration that is required. It is the number of APs to be upgraded at a time, as a percentage of the total number of APs in the network.

   Default value will be 15.

```
Device (config)#ap upgrade staggered <25 | 15 | 5>
```

Use the following command to trigger the rolling AP upgrade:

```
Device#ap image upgrade [test]
```

Installing AP Service Package (GUI)

Procedure

Step 1 Choose **Administration** > **Software Management**.

Step 2 Click **AP Service Package (APSP)** tab.

Step 3 Click **Add**.

Step 4 From the **Transport Type** drop-down list, choose the transfer type to transfer the software image to your device as TFTP, SFTP, FTP, Device, or Desktop (HTTP).

a) If you choose **TFTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **File path** and choose a **File System** from the drop-down list.

b) If you choose **SFTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **SFTP Username**, **SFTP Password**, **File path** and choose a **File System** from the drop-down list.
c) If you choose **FTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **FTP Username**, **FTP Password**, **File path**, and choose a **File System** from the drop-down list.
d) If you choose **Device** as the **Transport Type**, you need to enter the **File path** and choose a **File System** from the drop-down list.
e) If you choose **Desktop (HTTPS)** as the **Transport Type**, you need to choose a **File System** from the drop-down list and click **Select File** to navigate to the **Source File Path**.

Step 5 Enter the **File Name** and click **Add File**.

Step 6 From the **AP Upgrade Configuration** section, choose the percentage of APs to be included from the **AP Upgrade per iteration** drop-down list.

Step 7 Click **Apply**.

Installing AP Service Package (CLI)

Use the following procedure to roll out critical bug fixes to a subset of APs using SMU.

Procedure

	Command or Action	Purpose
Step 1	**install add file** *file-name* **Example:** `Device# install add file flash:<file-name>`	Checks for ongoing activities, such as AP image predownload or AP rolling upgrade. If there are no such activities, populates the predownload directory to install a package file to the system.
Step 2	**ap image site-filter file** *file-name* **add** *site-tag* **Example:** `Device# ap image site-filter file flash:<file-name> add bgl18`	Adds a site tag to a site filter.
Step 3	**ap image site-filter file** *file-name* **remove** *site-tag* **Example:** `Device# ap image site-filter file flash:<file-name> remove bgl18`	(Optional) Removes a site tag from a site filter.
Step 4	**install prepare activate file** *file-name* **Example:** `Device# install prepare activate file flash:<file-name>`	Performs predownload of an AP image. This image predownload will be filtered by the site filter, set up in the previous step.
Step 5	**install activate file** *file-name* **Example:** `Device# install activate file flash:<file-name>`	Triggers the AP upgrade in rolling a staggered fashion for the APs added in site filter.

	Command or Action	Purpose
Step 6	**install commit** **Example:** `Device# install commit`	Commits the image update. During the commit, the mapping from file to site is saved in the persistent database so that it is available even after a reload.

Adding a Site to a Filter

Procedure

	Command or Action	Purpose
Step 1	**ap image site-filter file** *file-name* **add** *site-tag* **Example:** `Device# ap image site-filter file flash:<file-name> add bgl18`	Adds a site tag to a site filter. Repeat this step again to set up a multisite filter.
Step 2	**ap image site-filter file** *file-name* **apply** **Example:** `Device# ap image site-filter file flash:<file-name> apply`	Predownloads the image and upgrades the APs based on the site filter.
Step 3	**ap image site-filter file** *file-name* **clear** **Example:** `Device# ap image site-filter file flash:<file-name> clear`	Clears the site filter table and predownloads the image and does a rolling AP upgrade to all sites where it is not active.

Deactivating an Image

Procedure

	Command or Action	Purpose
Step 1	**install prepare deactivate file** *file-name* **Example:** `Device# install prepare deactivate file flash:C9800-CL-rpboot.1324.SSA.pkg`	Specifies the package to be prepared for deactivation and predownloads AP image to the affected APs.
Step 2	**install deactivate file flash** *file-name* **Example:** `Device# install deactivate file flash:<file-name>`	Performs rolling AP upgrade based on the AP models present in the prepare file. Deactivation is not filtered by site. Therefore, deactivation applies to all the sites.

	Command or Action	Purpose
		Note Action is taken if the APs in a site are not running the SMU that is being deactivated. Only internal tables are updated to remove the SMU.

Roll Back APSP

Procedure

	Command or Action	Purpose
Step 1	**install prepare rollback to** *rollback_id* **Example:** `Device# install prepare rollback to 1`	Prepares to roll back to a particular installation point.
Step 2	**install rollback to** *rollback_id* **Example:** `Device# install rollback to rollback_id1`	Performs rollback of the image for the affected AP models. The roll back action is not filtered by site. Therefore, rollback applies to all the sites. **Note** The APs that are in the base image or in a point before the rollback action takes effect are not affected.

Canceling the Upgrade

Procedure

	Command or Action	Purpose
Step 1	**install prepare abort** **Example:** `Device# install abort prepare`	Prepares the controller for canceling the current install operation.
Step 2	**install abort** **Example:** `Device# install abort`	Aborts the upgrade by resetting the APs in rolling fashion. **Note** The **install prepare abort** command must be followed up with the **install abort** command.

Verifying the Upgrade

To see the summary of the AP software install files, use the following command:

```
Device# show ap image file summary

AP Image Active List
============================
Install File Name: vwlc_apsp_16.11.1.0_74.bin
------------------------------
AP Image Type                Capwap Version
-------------                --------------
     ap1g1                    16.11.1.19

     ap1g2                    16.11.1.19

     ap1g3                    16.11.1.19

     ap1g4                    16.11.1.19

     ap1g5                    16.11.1.19

     ap1g6                    16.11.1.19

AP Image Prepare List**
============================
Install File Name: vwlc_apsp_16.11.1.0_74.bin
------------------------------
AP Image Type                Capwap Version
-------------                --------------
     ap1g1                    16.11.1.19

     ap1g2                    16.11.1.19

     ap1g3                    16.11.1.19

     ap1g4                    16.11.1.19

     ap1g5                    16.11.1.19

     ap1g6                    16.11.1.19


**Difference of Active and Prepare list gives images being predownloaded to Access Points.
```

To see the summary of the AP site-filtered upgrades, use the following command:

```
Device# show ap image site summary

Install File Name: vwlc_apsp_16.11.1.0_74.bin

Site Tag                                    Prepared         Activated        Committed

-------------------------------------------------------------------------------------------
bgl-18-1                                    Yes              Yes              Yes

bgl-18-2                                    Yes              Yes              Yes

bgl-18-3                                    Yes              Yes              Yes

default-site-tag                            Yes              Yes              Yes
```

To see the summary of AP upgrades, use the following command:

```
Device# show ap upgrade summary
```

To check the status of an APSP, use the following command:

```
Device# show install summary

[ Chassis 1 ] Installed Package(s) Information:

State (St): I - Inactive, U - Activated & Uncommitted,

C - Activated & Committed, D - Deactivated & Uncommitted

--------------------------------------------------------------------------------

Type St Filename/Version

--------------------------------------------------------------------------------

APSP I bootflash:vwlc_apsp_16.11.1.0_74.bin

IMG C 16.11.1.0.1249


--------------------------------------------------------------------------------

Auto abort timer: inactive

--------------------------------------------------------------------------------
```

Verifying of AP Upgrade on the Controller

Use the following **show** command to verify the AP upgrade on the controller:

```
Device #show ap upgrade

AP upgrade is in progress
From version: 8 16.9.1.6
To version: 9 16.9.1.30
Started at: 03/09/2018 21:33:37 IST
Percentage complete: 0
Expected time of completion: 03/09/2018 22:33:37 IST
Progress Report
---------------
Iterations
----------
Iteration Start time End time AP count
-------------------------------------------------------------------------
0 03/09/2018 21:33:37 IST 03/09/2018 21:33:37 IST 0
1 03/09/2018 21:33:37 IST ONGOING 0
Upgraded
--------
Number of APs: 0
AP Name Ethernet MAC Iteration Status
-------------------------------------------------------------------------
In Progress
-----------
Number of APs: 1
AP Name Ethernet MAC
-------------------------------------------------
APf07f.06a5.d78c f07f.06cf.b910
Remaining
```

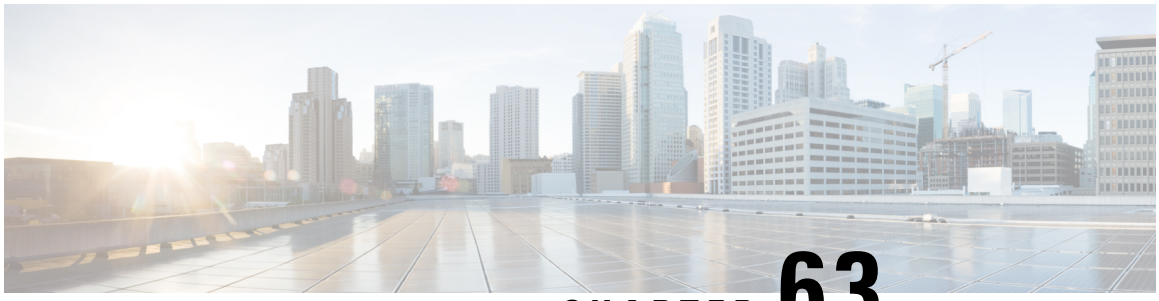
```
---------
Number of APs: 3
AP Name Ethernet MAC
-------------------------------------------------
APCC16.7EDB.6FA6 0081.c458.ab30
AP38ED.18CA.2FD0 38ed.18cb.25a0
AP881d.fce7.5ee4 d46d.50ee.33a0
```

PART VI

Security

- IPv4 ACLs , on page 495
- DNS-Based Access Control Lists, on page 523
- Allowed List of Specific URLs, on page 541
- Web-Based Authentication , on page 545
- Central Web Authentication, on page 581
- ISE Simplification and Enhancements, on page 595
- Authentication and Authorization Between Multiple RADIUS Servers, on page 609
- AAA Dead-Server Detection, on page 619
- RADIUS Server Load Balancing, on page 623
- Secure LDAP, on page 627
- RADIUS DTLS, on page 635
- Internet Protocol Security, on page 647
- MAC Filtering, on page 663
- IP Source Guard, on page 669
- Managing Rogue Devices, on page 671
- Classifying Rogue Access Points, on page 691
- Configuring Secure Shell , on page 701
- Private Shared Key, on page 709
- Multi-Preshared Key, on page 717
- Multiple Authentications for a Client, on page 725
- Cisco TrustSec, on page 737
- SGT Inline Tagging and SXPv4, on page 751
- Locally Significant Certificates, on page 757
- Cisco Umbrella WLAN, on page 771

• FIPS, on page 781



CHAPTER 63

IPv4 ACLs

- Information about Network Security with ACLs, on page 495
- Restrictions for Configuring IPv4 Access Control Lists, on page 503
- How to Configure ACLs, on page 504
- Configuration Examples for ACLs, on page 517
- Monitoring IPv4 ACLs, on page 521

Information about Network Security with ACLs

This chapter describes how to configure network security on the switch by using access control lists (ACLs), which in commands and tables are also referred to as access lists.

ACL Overview

Packet filtering can help limit network traffic and restrict network use by certain users or devices. ACLs filter traffic as it passes through a controller and permit or deny packets crossing specified interfaces. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. One by one, it tests packets against the conditions in an access list. The first match decides whether the controller accepts or rejects the packets. Because the controller stops testing after the first match, the order of conditions in the list is critical. If no conditions match, the controller rejects the packet. If there are no restrictions, the controller forwards the packet; otherwise, the controller drops the packet. The controller can use ACLs on all packets it forwards. There is implcit any host deny deny rule.

You configure access lists on a controller to provide basic security for your network. If you do not configure ACLs, all packets passing through the switch could be allowed onto all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at router interfaces. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic.

Access Control Entries

An ACL contains an ordered list of access control entries (ACEs). Each ACE specifies *permit* or *deny* and a set of conditions the packet must satisfy in order to match the ACE. The meaning of *permit* or *deny* depends on the context in which the ACL is used.

Note The maximum number of ACEs that can be applied under an access policy (ACL) for central switching is 256 ACEs. The maximum number of ACEs applicable for Flex Mode or Local Switching is 64 ACEs.

ACL Supported Types

The switch supports IP ACLs and Ethernet (MAC) ACLs:

- IP ACLs filter IPv4 traffic, including TCP, User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), and Internet Control Message Protocol (ICMP).
- Ethernet ACLs filter non-IP traffic.

This switch also supports quality of service (QoS) classification ACLs.

Supported ACLs

The controller supports three types of ACLs to filter traffic:

- Port ACLs access-control traffic entering a Layer 2 interface. You can apply port ACLs to a Layer 2 interface in each direction to each access list type — IPv4 and MAC.
- Router ACLs access-control routed traffic between VLANs and are applied to Layer 3 interfaces in a specific direction (inbound or outbound).
- FQDN ACL: FQDN ACL is encoded along with IPv6 ACL and sent to AP. FQDN ACL is always a custom ACL. AP does DNS snooping and sends the IPv4 and IPv6 addresses to the controller.

ACL Precedence

When Port ACLs, and router ACLs are configured on the same switch, the filtering precedence, from greatest to least for ingress traffic is port ACL, and then router ACL. For egress traffic, the filtering precedence is router ACL, and then port ACL.

The following examples describe simple use cases:

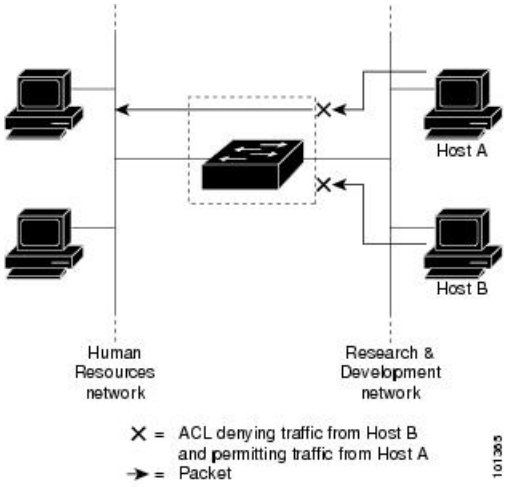
- When an input router ACL and input port ACL exist in a switch virtual interface (SVI), incoming packets received on ports to which a port ACL is applied are filtered by the port ACL. Incoming routed IP packets received on ports are filtered by the router ACL. Other packets are not filtered.
- When an output router ACL and input port ACL exist in an SVI, incoming packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IP packets are filtered by the router ACL. Other packets are not filtered.

Port ACLs

- Standard IP access lists using source addresses
- Extended IP access lists using source and destination addresses and optional protocol type information
- MAC extended access lists using source and destination MAC addresses and optional protocol type information

The switch examines ACLs on an interface and permits or denies packet forwarding based on how the packet matches the entries in the ACL. In this way, ACLs control access to a network or to part of a network.

Figure 7: Using ACLs to Control Traffic in a Network



This is an example of using port ACLs to control access to a network when all workstations are in the same VLAN. ACLs applied at the Layer 2 input would allow Host A to access the Human Resources network, but prevent Host B from accessing the same network. Port ACLs can only be applied to Layer 2 interfaces in the inbound direction.

When you apply a port ACL to a trunk port, the ACL filters traffic on all VLANs present on the trunk port. When you apply a port ACL to a port with voice VLAN, the ACL filters traffic on both data and voice VLANs.

With port ACLs, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC addresses. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP access list and a MAC access list to the interface.

Note You can't apply more than one IP access list and one MAC access list to a Layer 2 interface. If an IP access list or MAC access list is already configured on a Layer 2 interface and you apply a new IP access list or MAC access list to the interface, the new ACL replaces the previously configured one.

Router ACLs

You can apply router ACLs on switch virtual interfaces (SVIs), which are Layer 3 interfaces to VLANs; on physical Layer 3 interfaces; and on Layer 3 EtherChannel interfaces. You apply router ACLs on interfaces for specific directions (inbound or outbound). You can apply one router ACL in each direction on an interface.

The switch supports these access lists for IPv4 traffic:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses and optional protocol type information for matching operations.

As with port ACLs, the switch examines ACLs associated with features configured on a given interface. As packets enter the switch on an interface, ACLs associated with all inbound features configured on that interface are examined. After packets are routed and before they are forwarded to the next hop, all ACLs associated with outbound features configured on the egress interface are examined.

ACLs permit or deny packet forwarding based on how the packet matches the entries in the ACL, and can be used to control access to a network or to part of a network.

ACEs and Fragmented and Unfragmented Traffic

IP packets can be fragmented as they cross the network. When this happens, only the fragment containing the beginning of the packet contains the Layer 4 information, such as TCP or UDP port numbers, ICMP type and code, and so on. All other fragments are missing this information.

Some access control entries (ACEs) do not check Layer 4 information and therefore can be applied to all packet fragments. ACEs that do test Layer 4 information cannot be applied in the standard manner to most of the fragments in a fragmented IP packet. When the fragment contains no Layer 4 information and the ACE tests some Layer 4 information, the matching rules are modified:

- Permit ACEs that check the Layer 3 information in the fragment (including protocol type, such as TCP, UDP, and so on) are considered to match the fragment regardless of what the missing Layer 4 information might have been.

Note For TCP ACEs with L4 Ops, the fragmented packets will be dropped per RFC 1858.

- Deny ACEs that check Layer 4 information never match a fragment unless the fragment contains Layer 4 information.

ACEs and Fragmented and Unfragmented Traffic Examples

Consider access list 102, configured with these commands, applied to three fragmented packets:

```
Device(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Device(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Device(config)# access-list 102 permit tcp any host 10.1.1.2
Device(config)# access-list 102 deny tcp any any
```

Note In the first and second ACEs in the examples, the *eq* keyword after the destination address means to test for the TCP-destination-port well-known numbers equaling Simple Mail Transfer Protocol (SMTP) and Telnet, respectively.

- Packet A is a TCP packet from host 10.2.2.2., port 65000, going to host 10.1.1.1 on the SMTP port. If this packet is fragmented, the first fragment matches the first ACE (a permit) as if it were a complete packet because all Layer 4 information is present. The remaining fragments also match the first ACE, even though they do not contain the SMTP port information, because the first ACE only checks Layer 3 information when applied to fragments. The information in this example is that the packet is TCP and that the destination is 10.1.1.1.

- Packet B is from host 10.2.2.2, port 65001, going to host 10.1.1.2 on the Telnet port. If this packet is fragmented, the first fragment matches the second ACE (a deny) because all Layer 3 and Layer 4 information is present. The remaining fragments in the packet do not match the second ACE because they are missing Layer 4 information. Instead, they match the third ACE (a permit).

  Because the first fragment was denied, host 10.1.1.2 cannot reassemble a complete packet, so packet B is effectively denied. However, the later fragments that are permitted will consume bandwidth on the network and resources of host 10.1.1.2 as it tries to reassemble the packet.

- Fragmented packet C is from host 10.2.2.2, port 65001, going to host 10.1.1.3, port ftp. If this packet is fragmented, the first fragment matches the fourth ACE (a deny). All other fragments also match the fourth ACE because that ACE does not check any Layer 4 information and because Layer 3 information in all fragments shows that they are being sent to host 10.1.1.3, and the earlier permit ACEs were checking different hosts.

Standard and Extended IPv4 ACLs

This section describes IP ACLs.

An ACL is a sequential collection of permit and deny conditions. One by one, the switch tests packets against the conditions in an access list. The first match determines whether the switch accepts or rejects the packet. Because the switch stops testing after the first match, the order of the conditions is critical. If no conditions match, the switch denies the packet.

The software supports these types of ACLs or access lists for IPv4:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses for matching operations and optional protocol-type information for finer granularity of control.

Note Only extended ACLs are supported while the standard ACLs are not supported.

IPv4 ACL Switch Unsupported Features

Configuring IPv4 ACLs on the switch is the same as configuring IPv4 ACLs on other Cisco switches and routers.

The following ACL-related features are not supported:

- Non-IP protocol ACLs
- IP accounting
- Reflexive ACLs, URL Redirect ACLs and Dynamic ACLs are not supported.

Access List Numbers

The number you use to denote your ACL shows the type of access list that you are creating.

This lists the access-list number and corresponding access list type and shows whether or not they are supported in the switch. The switch supports IPv4 standard and extended access lists, numbers 1 to 199 and 1300 to 2699.

Table 14: Access List Numbers

Access List Number	Type	Supported
1–99	IP standard access list	Yes
100–199	IP extended access list	Yes
200–299	Protocol type-code access list	No
300–399	DECnet access list	No
400–499	XNS standard access list	No
500–599	XNS extended access list	No
600–699	AppleTalk access list	No
700–799	48-bit MAC address access list	No
800–899	IPX standard access list	No
900–999	IPX extended access list	No
1000–1099	IPX SAP access list	No
1100–1199	Extended 48-bit MAC address access list	No
1200–1299	IPX summary address access list	No
1300–1999	IP standard access list (expanded range)	Yes
2000–2699	IP extended access list (expanded range)	Yes

In addition to numbered standard and extended ACLs, you can also create standard and extended named IP ACLs by using the supported numbers. That is, the name of a standard IP ACL can be 1 to 99; the name of an extended IP ACL can be 100 to 199. The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

Numbered Standard IPv4 ACLs

When creating an ACL, remember that, by default, the end of the ACL contains an implicit deny statement for all packets that it did not find a match for before reaching the end. With standard access lists, if you omit the mask from an associated IP host address ACL specification, 0.0.0.0 is assumed to be the mask.

The switch always rewrites the order of standard access lists so that entries with **host** matches and entries with matches having a *don't care* mask of 0.0.0.0 are moved to the top of the list, above any entries with non-zero *don't care* masks. Therefore, in **show** command output and in the configuration file, the ACEs do not necessarily appear in the order in which they were entered.

After creating a numbered standard IPv4 ACL, you can apply it to terminal lines (virtual teletype (VTY) lines), or to interfaces.

Numbered Extended IPv4 ACLs

Although standard ACLs use only source addresses for matching, you can use extended ACL source and destination addresses for matching operations and optional protocol type information for finer granularity of control. When you are creating ACEs in numbered extended access lists, remember that after you create the ACL, any additions are placed at the end of the list. You cannot reorder the list or selectively add or remove ACEs from a numbered list.

The switch does not support dynamic or reflexive access lists. It also does not support filtering based on the type of service (ToS) minimize-monetary-cost bit.

Some protocols also have specific parameters and keywords that apply to that protocol.

You can define an extended TCP, UDP, ICMP, IGMP, or other IP ACL. The switch also supports these IP protocols:

These IP protocols are supported:

- Authentication Header Protocol (**ahp**)
- Encapsulation Security Payload (**esp**)
- Enhanced Interior Gateway Routing Protocol (**eigrp**)
- generic routing encapsulation (**gre**)
- Internet Control Message Protocol (**icmp**)
- Internet Group Management Protocol (**igmp**)
- any Interior Protocol (**ip**)
- IP in IP tunneling (**ipinip**)
- KA9Q NOS-compatible IP over IP tunneling (**nos**)
- Open Shortest Path First routing (**ospf**)
- Payload Compression Protocol (**pcp**)
- Protocol-Independent Multicast (**pim**)
- Transmission Control Protocol (**tcp**)
- User Datagram Protocol (**udp**)

Named IPv4 ACLs

You can identify IPv4 ACLs with an alphanumeric string (a name) rather than a number. You can use named ACLs to configure more IPv4 access lists in a router than if you were to use numbered access lists. If you identify your access list with a name rather than a number, the mode and command syntax are slightly different. However, at times, not all commands that use IP access lists accept a named access list.

Note The name you give to a standard or extended ACL can also be a number in the supported range of access list numbers. That is, the name of a standard IP ACL can be 1 to 99 and . The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

Consider these guidelines before configuring named ACLs:

- Numbered ACLs are also available.
- A standard ACL and an extended ACL cannot have the same name.

ACL Logging

The controller software can provide logging messages about packets permitted or denied by a standard IP access list. That is, any packet that matches the ACL causes an informational logging message about the packet to be sent to the console. The level of messages logged to the console is controlled by the **logging console** commands controlling the syslog messages.

Note Because routing is done in hardware and logging is done in software, if a large number of packets match a *permit* or *deny* ACE containing a **log** keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

The first packet that triggers the ACL causes a logging message right away, and subsequent packets are collected over 5-minute intervals before they appear or logged. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval.

Note The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

Hardware and Software Treatment of IP ACLs

ACL processing is performed in hardware. If the hardware reaches its capacity to store ACL configurations, all packets on that interface are dropped.

The ACL scale for controllers is as follows:

- Cisco Catalyst 9800-40 Wireless Controller, Cisco Catalyst 9800-L Wireless Controller, Cisco Catalyst 9800-CL Wireless Controller (small and medium) support 128 ACLs with 128 Access List Entries (ACEs).
- Cisco Catalyst 9800-80 Wireless Controller and Cisco Catalyst 9800-CL Wireless Controller (large) support 256 ACLs and 256 ACEs.
- FlexConnect and Fabric mode APs support 96 ACLs.

Note If an ACL configuration cannot be implemented in the hardware due to an out-of-resource condition on the controller, then only the traffic in that VLAN arriving on that controller is affected.

When you enter the **show ip access-lists** privileged EXEC command, the match count displayed does not account for packets that are access controlled in hardware. Use the privileged EXEC command to obtain some basic hardware ACL statistics for switched and routed packets.

IPv4 ACL Interface Considerations

For inbound ACLs, after receiving a packet, the controller checks the packet against the ACL. If the ACL permits the packet, the controller continues to process the packet. If the ACL rejects the packet, the controller discards the packet.

For outbound ACLs, after receiving and routing a packet to a controlled interface, the controller checks the packet against the ACL. If the ACL permits the packet, the controller sends the packet. If the ACL rejects the packet, the controller discards the packet.

If an undefined ACL has nothing listed in it, it is an empty access list.

Restrictions for Configuring IPv4 Access Control Lists

The following are restrictions for configuring network security with ACLs:

General Network Security

The following are restrictions for configuring network security with ACLs:

- A standard ACL and an extended ACL cannot have the same name.
- Though visible in the command-line help strings, **AppleTalk** is not supported as a matching condition for the **deny** and **permit** MAC access-list configuration mode commands.
- DNS traffic is permitted by default with or without ACL entries for clients that are awaiting web authentication.

IPv4 ACL Network Interfaces

The following restrictions apply to IPv4 ACLs to network interfaces:

- When controlling access to an interface, you can use a named or numbered ACL.
- You do not have to enable routing to apply ACLs to Layer 2 interfaces.

MAC ACLs on a Layer 2 Interface

After you create a MAC ACL, you can apply it to a Layer 2 interface to filter non-IP traffic coming in that interface. When you apply the MAC ACL, consider these guidelines:

- You can apply no more than one IP access list and one MAC access list to the same Layer 2 interface. The IP access list filters only IP packets, and the MAC access list filters non-IP packets.
- A Layer 2 interface can have only one MAC access list. If you apply a MAC access list to a Layer 2 interface that has a MAC ACL configured, the new ACL replaces the previously configured one.

Note The **mac access-group** interface configuration command is only valid when applied to a physical Layer 2 interface. You cannot use the command on EtherChannel port channels.

IP Access List Entry Sequence Numbering

- This feature does not support dynamic, reflexive, or firewall access lists.

How to Configure ACLs

Configuring IPv4 ACLs (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **ACL**.

Step 2 Click **Add**.

Step 3 In the **Add ACL Setup** dialog box, enter the following parameters.

- **ACL Name:** Enter the name for the ACL.
- **ACL Type:** IPv4 Standard.
- **Sequence:** Enter the sequence number.
- **Action:** Choose **Permit** or **Deny** the packet flow from the drop-down list.
- **Source Type:** Choose **any**, **Host** or **Network** from which the packet is sent.
- **Log:** Enable or disable logging.

Step 4 Click **Add**.

Step 5 Add the rest of the rules and click **Apply to Device**.

Configuring IPv4 ACLs

Follow the procedure given below to use IP ACLs on the switch:

Procedure

Step 1 Create an ACL by specifying an access list number or name and the access conditions.

Step 2 Apply the ACL to interfaces or terminal lines..

Creating a Numbered Standard ACL (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **ACL**.

Step 2 On the **ACL** page, click **Add**.

Step 3 In the **Add ACL Setup** window, enter the following parameters.

- **ACL Name:** Enter the name for the ACL.
- **ACL Type:** IPv4 Standard.
- **Sequence:** Enter the sequence number.
- **Action:** Choose **Permit** or **Deny** access from the drop-down list.
- **Source Type:** Choose **any**, **Host** or **Network**
- **Log:** Enable or disable logging, this is limited to ACLs associated to Layer 3 interface only.

Step 4 Click **Add**.

Step 5 Click **Save & Apply to Device**.

Creating a Numbered Standard ACL (CLI)

Follow the procedure given below to create a numbered standard ACL:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} *source source-wildcard*] **Example:** `Device(config)# access-list 2 deny`	Defines a standard IPv4 access list by using a source address and wildcard. The *access-list-number* is a decimal number from 1 to 99 or 1300 to 1999.

	Command or Action	Purpose
	`your_host`	Enter **deny** or **permit** to specify whether to deny or permit access if conditions are matched. The *source* is the source address of the network or host from which the packet is being sent specified as: • The 32-bit quantity in dotted-decimal format. • The keyword **any** as an abbreviation for *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard. • The keyword **host** as an abbreviation for source and *source-wildcard* of *source* 0.0.0.0. (Optional) The *source-wildcard* applies wildcard bits to the source. **Note** Logging is supported only on ACLs attached to Layer 3 interfaces.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Device# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Creating a Numbered Extended ACL (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **ACL**.

Step 2 On the **ACL** page, click **Add**.

Step 3 In the **Add ACL Setup** window, enter the following parameters.

- **ACL Name:** Enter the name for the ACL.
- **ACL Type:** IPv4 Extended.
- **Sequence:** Enter the sequence number.
- **Action:** Choose **Permit** or **Deny** the packet flow from the drop-down list.
- **Source Type:** Choose **any**, **Host** or **Network** from which the packet is sent.
- **Destination Type:** Choose **any**, **Host** or **Network** to which the packet is sent.
- **Protocol:** Choose a protocol from the drop-down list.
- **Log:** Enable or disable logging.
- **DSCP:** Enter to match packets with the DSCP value

Step 4 Click **Add**.

Step 5 Click **Save & Apply to Device**.

Creating a Numbered Extended ACL (CLI)

Follow the procedure given below to create a numbered extended ACL:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** tos] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*]	Defines an extended IPv4 access list and the access conditions. The *access-list-number* is a decimal number from 100 to 199 or 2000 to 2699.

	Command or Action	Purpose
	Example: `Device(config)# access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log`	Enter **deny** or **permit** to specify whether to deny or permit the packet if conditions are matched. For *protocol*, enter the name or number of an P protocol: **ahp**, **eigrp**, **esp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **pcp**, **pim**, **tcp**, or **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword **ip**. **Note** This step includes options for most IP protocols. For additional specific parameters for TCP, UDP, ICMP, and IGMP, see the following steps. The *source* is the number of the network or host from which the packet is sent. The *source-wildcard* applies wildcard bits to the source. The *destination* is the network or host number to which the packet is sent. The *destination-wildcard* applies wildcard bits to the destination. Source, source-wildcard, destination, and destination-wildcard can be specified as: • The 32-bit quantity in dotted-decimal format. • The keyword **any** for 0.0.0.0 255.255.255.255 (any host). • The keyword **host** for a single host 0.0.0.0. The other keywords are optional and have these meanings: • **precedence**—Enter to match packets with a precedence level specified as a number from 0 to 7 or by name: **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5), **internet** (6), **network** (7). • **fragments**—Enter to check non-initial fragments. • **tos**—Enter to match by type of service level, specified by a number from 0 to 15

	Command or Action	Purpose
		or a name: **normal** (0), **max-reliability** (2), **max-throughput** (4), **min-delay** (8). • **time-range**—Specify the time-range name. • **dscp**—Enter to match packets with the DSCP value specified by a number from 0 to 63, or use the question mark (?) to see a list of available values. **Note** Your controller must support the ability to: • Mark DCSP • Mark UP • Map DSCP and UP For more information on **DSCP-to-UP Mapping**, see: https://tools.ietf.org/html/draft-ietf-tsvwg-ieee-802-11-01 **Note** If you enter a **dscp** value, you cannot enter **tos** or **precedence**. You can enter both a **tos** and a **precedence** value with no **dscp**.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} **tcp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] [*flag*] **Example:** `Device(config)# access-list 101 permit tcp any any eq 500`	Defines an extended TCP access list and the access conditions. The parameters are the same as those described for an extended IPv4 ACL, with these exceptions: (Optional) Enter an *operator* and *port* to compare source (if positioned after *source source-wildcard*) or destination (if positioned after *destination destination-wildcard*) port. Possible operators include **eq** (equal), **gt** (greater than), **lt** (less than), **neq** (not equal), and **range** (inclusive range). Operators require a port number (range requires two port numbers separated by a space). Enter the *port* number as a decimal number (from 0 to 65535) or the name of a TCP port. Use only TCP port numbers or names when filtering TCP.

	Command or Action	Purpose
		The other optional keywords have these meanings: • *flag*—Enter one of these flags to match by the specified TCP header bits: **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize), or **urg** (urgent).
Step 4	**access-list** *access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] **Example:** `Device(config)# access-list 101 permit udp any any eq 100`	(Optional) Defines an extended UDP access list and the access conditions. The UDP parameters are the same as those described for TCP except that the [operator [port]] port number or name must be a UDP port number or name, and the **flag** not valid for UDP.
Step 5	**access-list** *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] **Example:** `Device(config)# access-list 101 permit icmp any any 200`	Defines an extended ICMP access list and the access conditions. The ICMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings: • *icmp-type*—Enter to filter by ICMP message type, a number from 0 to 255. • *icmp-code*—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255. • *icmp-message*—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name.
Step 6	**access-list** *access-list-number* {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] **Example:** `Device(config)# access-list 101 permit igmp any any 14`	(Optional) Defines an extended IGMP access list and the access conditions. The IGMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with this optional parameter. *igmp-type*—To match IGMP message type, enter a number from 0 to 15, or enter the message name: **dvmrp**, **host-query**, **host-report**, **pim**, or **trace**.

	Command or Action	Purpose
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Creating Named Standard ACLs (GUI)

Procedure

Step 1 Click **Configuration** > **Security** > **ACL**.

Step 2 Click **Add** to create a new ACL setup.

Step 3 In the **Add ACL Setup** window, enter the following parameters.

- **ACL Name:** Enter the name for the ACL
- **ACL Type:** IPv4 Standard
- **Sequence:** The valid range is between 1 and 99 or 1300 and 1999
- **Action:** Choose **Permit** or **Deny** access from the drop-down list.
- **Source Type:** Choose **any**, **Host** or **Network**
- **Log:** Enable or disable logging, this is limited to ACLs associated to Layer 3 interface only.

Step 4 Click **Add** to add the rule.

Step 5 Click **Save & Apply to Device**.

Creating Named Standard ACLs

Follow the procedure given below to create a standard ACL using names:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**ip access-list standard** *name* **Example:** `Device(config)# ip access-list standard 20`	Defines a standard IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 1 to 99.

Step 4	Use one of the following:
	• **deny** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**]
	• **permit** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**]
	Example:
	`Device(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255`
	or
	`Device(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0`
		In access-list configuration mode, specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.
		• **host** *source*—A source and source wildcard of *source* 0.0.0.0.
		• **any**—A source and source wildcard of 0.0.0.0 255.255.255.255.

Step 5	**end** **Example:** `Device(config-std-nacl)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Device# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Creating Extended Named ACLs (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **ACL**.

Step 2 Click **Add**.

Step 3 In the **Add ACL Setup** window, enter the following parameters.

- **ACL Name:** Enter the name for the ACL.
- **ACL Type:** IPv4 Extended.
- **Sequence:** Enter the sequence number.
- **Action:** Choose **Permit** or **Deny** the packet flow from the drop-down list.
- **Source Type:** Choose **any**, **Host** or **Network** from which the packet is sent.
- **Destination Type:** Choose **any**, **Host** or **Network** to which the packet is sent.
- **Protocol:** Choose a protocol from the drop-down list.
- **Log:** Enable or disable logging.
- **DSCP:** Enter to match packets with the DSCP value

Step 4 Click **Add**.

Step 5 Add the rest of the rules and click **Apply to Device**.

Creating Extended Named ACLs

Follow the procedure given below to create an extended ACL using names:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip access-list extended** *name* **Example:** `Device(config)# ip access-list extended 150`	Defines an extended IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 100 to 199.
Step 4	{**deny** | **permit**} *protocol* {*source* [*source-wildcard*] | **host** *source* | **any**} {*destination* [*destination-wildcard*] | host *destination* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] **Example:** `Device(config-ext-nacl)# permit 0 any any`	In access-list configuration mode, specify the conditions allowed or denied. Use the **log** keyword to get access list logging messages, including violations. • **host** *source*—A source and source wildcard of *source* 0.0.0.0. • **host** *destintation*—A destination and destination wildcard of *destination* 0.0.0.0. • **any**—A source and source wildcard or destination and destination wildcard of 0.0.0.0 255.255.255.255.
Step 5	**end** **Example:** `Device(config-ext-nacl)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Device# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

When you are creating extended ACLs, remember that, by default, the end of the ACL contains an implicit deny statement for everything if it did not find a match before reaching the end. For standard ACLs, if you omit the mask from an associated IP host address access list specification, 0.0.0.0 is assumed to be the mask.

After you create an ACL, any additions are placed at the end of the list. You cannot selectively add ACL entries to a specific ACL. However, you can use **no permit** and **no deny** access-list configuration mode commands to remove entries from a named ACL.

Being able to selectively remove lines from a named ACL is one reason you might use named ACLs instead of numbered ACLs.

What to do next

After creating a named ACL, you can apply it to interfaces or to VLANs.

Applying an IPv4 ACL to an Interface (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **ACL**.

Step 2 Click **Associating Interfaces**.

Step 3 Choose the interface from the **Available Interfaces** list to view its ACL details on the right-hand side. You can change the ACL details, if required.

Step 4 Click **Save & Apply to Device**.

Applying an IPv4 ACL to an Interface (CLI)

This section describes how to apply IPv4 ACLs to network interfaces.

Beginning in privileged EXEC mode, follow the procedure given below to control access to an interface:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Device(config)#`	Identifies a specific interface for configuration, and enter interface configuration mode. The interface can be a Layer 2 interface (port ACL), or a Layer 3 interface (router ACL).
Step 3	**ip access-group** {*access-list-number* | *name*} {**in** | **out**} **Example:** `Device(config-if)# ip access-group 2 in`	Controls access to the specified interface.
Step 4	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-if)# end`	
Step 5	**show running-config** **Example:** `Device# show running-config`	Displays the access list configuration.
Step 6	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Applying ACL to Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, click **Add**.

Step 3 In the **Add Policy Profile** window, click **Access Policies** tab.

Step 4 In the **WLAN ACL** area, choose the IPv4 ACL from the **IPv4 ACL** drop-down list.

Step 5 Click **Apply to Device**.

Applying ACL to Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy profile-policy`	Configures a WLAN policy profile and enters wireless policy configuration mode.

	Command or Action	Purpose
Step 3	**ipv4 acl** *acl-name* **Example:** `Device(config-wireless-policy)# ipv4 acl test-acl`	Configures an IPv4 ACL.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuration Examples for ACLs

Examples: Including Comments in ACLs

You can use the **remark** keyword to include comments (remarks) about entries in any IP standard or extended ACL. The remarks make the ACL easier for you to understand and scan. Each remark line is limited to 100 characters.

The remark can go before or after a permit or deny statement. You should be consistent about where you put the remark so that it is clear which remark describes which permit or deny statement. For example, it would be confusing to have some remarks before the associated permit or deny statements and some remarks after the associated statements.

To include a comment for IP numbered standard or extended ACLs, use the **access-list** *access-list number* **remark** *remark* global configuration command. To remove the remark, use the **no** form of this command.

In this example, the workstation that belongs to Jones is allowed access, and the workstation that belongs to Smith is not allowed access:

```
Device(config)# access-list 1 remark Permit only Jones workstation through
Device(config)# access-list 1 permit 171.69.2.88
Device(config)# access-list 1 remark Do not allow Smith through
Device(config)# access-list 1 deny 171.69.3.13
```

For an entry in a named IP ACL, use the **remark** access-list configuration command. To remove the remark, use the **no** form of this command.

In this example, the Jones subnet is not allowed to use outbound Telnet:

```
Device(config)# ip access-list extended telnetting
Device(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Device(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

Examples: Applying an IPv4 ACL to a Policy Profile in a Wireless Environment

This example shows how to apply an IPv4 ACL to a Policy Profile in a Wireless environment.

Note All IPv4 ACLs must be associated to a policy profile.

This example uses extended ACLs to permit TCP traffic.

1. Creating an IPv4 ACL.

```
Device(config)# ip access-list extended <acl-name>
Device(config-ext-nacl)# 10 permit ip any 10.193.48.224 0.0.0.31
Device (config-ext-nacl)# 20 permit ip any any
```

2. Applying the IPv4 ACL to a policy profile.

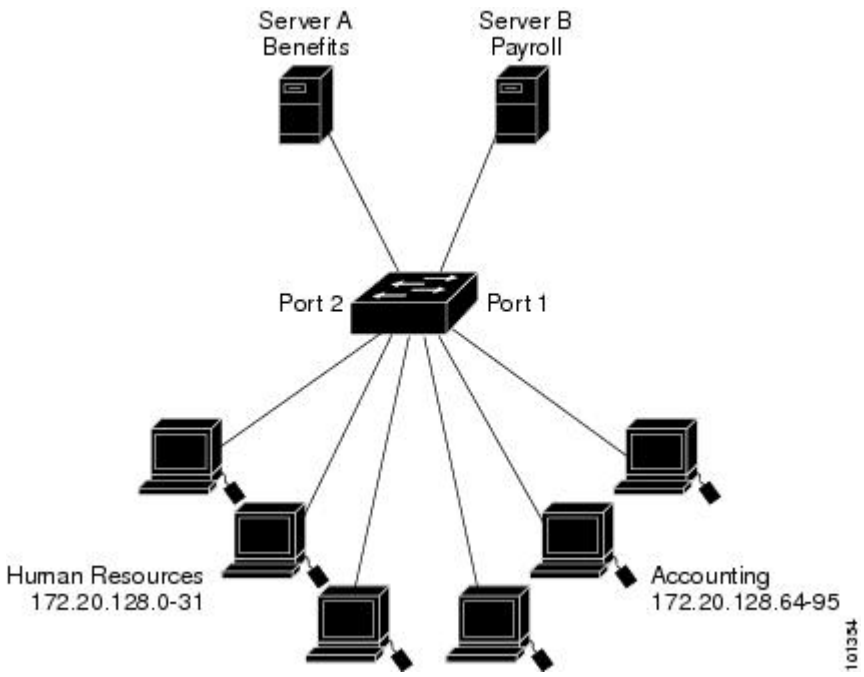
```
Device(config)# wireless profile policy <policy-profile-name>
Device(config-wireless-policy)# shutdown
Device(config-wireless-policy)# ipv4 acl <acl-name>
Device(config-wireless-policy)# no shutdown
```

IPv4 ACL Configuration Examples

This section provides examples of configuring and applying IPv4 ACLs. For detailed information about compiling ACLs, see the *Cisco IOS Security Configuration Guide, Release 12.4* and to the Configuring IP Services" section in the "IP Addressing and Services" chapter of the *Cisco IOS IP Configuration Guide, Release 12.4.*

ACLs in a Small Networked Office

Figure 8: Using Router ACLs to Control Traffic



This shows a small networked office environment with routed Port 2 connected to Server A, containing benefits and other information that all employees can access, and routed Port 1 connected to Server B, containing confidential payroll data. All users can access Server A, but Server B has restricted access.

Use router ACLs to do this in one of two ways:

- Create a standard ACL, and filter traffic coming to the server from Port 1.
- Create an extended ACL, and filter traffic coming from the server into Port 1.

Examples: ACLs in a Small Networked Office

This example uses a standard ACL to filter traffic coming into Server B from a port, permitting traffic only from Accounting's source addresses 172.20.128.64 to 172.20.128.95. The ACL is applied to traffic coming out of routed Port 1 from the specified source address.

```
Device(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Device(config)# end
Device# how access-lists
Standard IP access list 6
    10 permit 172.20.128.64, wildcard bits 0.0.0.31
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 6 out
```

This example uses an extended ACL to filter traffic coming from Server B into a port, permitting traffic from any source address (in this case Server B) to only the Accounting destination addresses 172.20.128.64 to 172.20.128.95. The ACL is applied to traffic going into routed Port 1, permitting it to go only to the specified destination addresses. Note that with extended ACLs, you must enter the protocol (IP) before the source and destination information.

```
Device(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Device(config)# end
Device# show access-lists
Extended IP access list 106
    10 permit ip any 172.20.128.64 0.0.0.31
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 106 in
```

Example: Numbered ACLs

In this example, network 10.0.0.0 is a Class A network whose second octet specifies a subnet; that is, its subnet mask is 255.255.0.0. The third and fourth octets of a network 10.0.0.0 address specify a particular host. Using access list 2, the switch accepts one address on subnet 48 and reject all others on that subnet. The last line of the list shows that the switch accepts addresses on all other network 10.0.0.0 subnets. The ACL is applied to packets entering a port.

```
Device(config)# access-list 2 permit 10.48.0.3
Device(config)# access-list 2 deny 10.48.0.0 0.0.255.255
Device(config)# access-list 2 permit 10.0.0.0 0.255.255.255
Device(config)#
Device(config-if)# ip access-group 2 in
```

Examples: Extended ACLs

In this example, the first line permits any incoming TCP connections with destination ports greater than 1023. The second line permits incoming TCP connections to the Simple Mail Transfer Protocol (SMTP) port of host 128.88.1.2. The third line permits incoming ICMP messages for error feedback.

```
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Device(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Device(config)# access-list 102 permit icmp any any
Device(config)#
Device(config-if)# ip access-group 102 in
```

In this example, suppose that you have a network connected to the Internet, and you want any host on the network to be able to form TCP connections to any host on the Internet. However, you do not want IP hosts to be able to form TCP connections to hosts on your network, except to the mail (SMTP) port of a dedicated mail host.

SMTP uses TCP port 25 on one end of the connection and a random port number on the other end. The same port numbers are used throughout the life of the connection. Mail packets coming in from the Internet have a destination port of 25. Because the secure system of the network always accepts mail connections on port 25, the incoming are separately controlled.

```
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
Device(config)#
Device(config-if)# ip access-group 102 in
```

Examples: Named ACLs

Creating named standard and extended ACLs

This example creates a standard ACL named *internet_filter* and an extended ACL named *marketing_group*. The *internet_filter* ACL allows all traffic from the source address 1.2.3.4.

```
Device(config)# ip access-list standard Internet_filter
Device(config-ext-nacl)# permit 1.2.3.4
Device(config-ext-nacl)# exit
```

The *marketing_group* ACL allows any TCP Telnet traffic to the destination address and wildcard 171.69.0.0 0.0.255.255 and denies any other TCP traffic. It permits ICMP traffic, denies UDP traffic from any source to the destination address range 171.69.0.0 through 179.69.255.255 with a destination port less than 1024, denies any other IP traffic, and provides a log of the result.

```
Device(config)# ip access-list extended marketing_group
Device(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Device(config-ext-nacl)# deny tcp any any
Device(config-ext-nacl)# permit icmp any any
Device(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Device(config-ext-nacl)# deny ip any any log
Device(config-ext-nacl)# exit
```

The *Internet_filter* ACL is applied to outgoing traffic and the *marketing_group* ACL is applied to incoming traffic on a Layer 3 port.

```
Device(config)# interface gigabitethernet3/0/1

Device(config-if)# ip address 2.0.5.1 255.255.255.0
Device(config-if)# ip access-group Internet_filter out
Device(config-if)# ip access-group marketing_group in
```

Deleting individual ACEs from named ACLs

This example shows how you can delete individual ACEs from the named access list *border-list*:

```
Device(config)# ip access-list extended border-list
Device(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

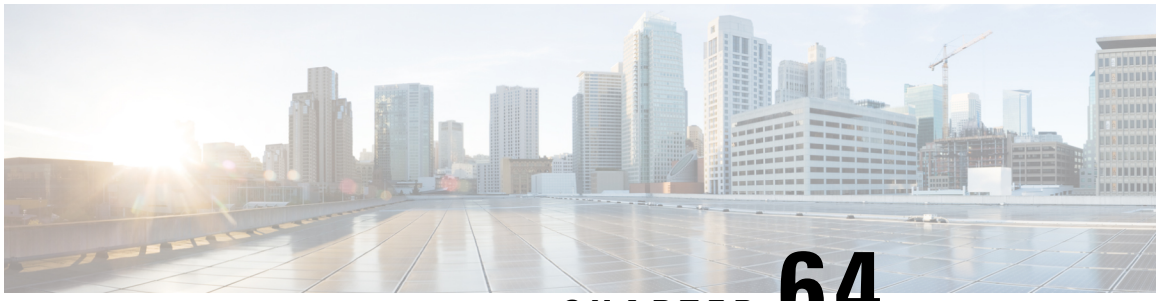
Monitoring IPv4 ACLs

You can monitor IPv4 ACLs by displaying the ACLs that are configured on the switch, and displaying the ACLs that have been applied to interfaces and VLANs.

When you use the **ip access-group** interface configuration command to apply ACLs to a Layer 2 or 3 interface, you can display the access groups on the interface. You can also display the MAC ACLs applied to a Layer 2 interface. You can use the privileged EXEC commands as described in this table to display this information.

Table 15: Commands for Displaying Access Lists and Access Groups

Command	Purpose
show access-lists [*number* | *name*]	Displays the contents of one or all current IP and MAC address a specific access list (numbered or named).
show ip access-lists [*number* | *name*]	Displays the contents of all current IP access lists or a specific I (numbered or named).
show ip interface *interface-id*	Displays detailed configuration and status of an interface. If IP i the interface and ACLs have been applied by using the **ip access-g** configuration command, the access groups are included in the d
show running-config [**interface** *interface-id*]	Displays the contents of the configuration file for the switch or t interface, including all configured MAC and IP access lists and groups are applied to an interface.



CHAPTER 64

DNS-Based Access Control Lists

- Information About DNS-Based Access Control Lists, on page 523
- Restrictions on DNS-Based Access Control Lists, on page 526
- Flex Mode, on page 527
- Local Mode, on page 528
- Viewing DNS-Based Access Control Lists, on page 532
- Configuration Examples for DNS-Based Access Control Lists, on page 532
- Verifying DNS Snoop Agent (DSA), on page 533
- Information About Flex Client IPv6 Support with WebAuth Pre and Post ACL, on page 535
- Enabling Pre-Authentication ACL for LWA and EWA (GUI), on page 536
- Enabling Pre-Authentication ACL for LWA and EWA, on page 536
- Enabling Post-Authentication ACL for LWA and EWA (GUI), on page 538
- Enabling Post-Authentication ACL for LWA and EWA, on page 538
- Enabling DNS ACL for LWA and EWA (GUI), on page 538
- Enabling DNS ACL for LWA and EWA, on page 539
- Verifying Flex Client IPv6 Support with WebAuth Pre and Post ACL, on page 539

Information About DNS-Based Access Control Lists

The DNS-based ACLs are used for wireless client devices. When using these devices, you can set pre-authentication ACLs on the Cisco Catalyst 9800 Series Wireless Controller to determine the data requests that are allowed or blocked.

To enable DNS-based ACLs on the controller , you need to configure the allowed URLs or denied 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 that is returned by the AAA server. 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 AAA server returns the pre-authentication ACL (url-redirect-acl, which is the attribute name given to the AAA server). 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 for 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.

During pre-authentication or post-authentication, DNS ACL is applied to the client in the access point. If the client roams from one AP to another AP, the DNS learned IP addresses on the old AP is valid on the new AP as well.

Note URL filter needs to be attached to a policy profile in case of the local mode. In the flex mode, the URL filter is attached to the flex profile and it is not need to be attached to a policy profile.

Note DNS based URLs work with active DNS query from the client. Hence, for URL filtering, the DNS should be setup correctly.

Note URL filter takes precedence over punt or redirect ACL, and over custom or static pre-auth ACL.s

Defining ACLs

Extended ACLs are like standard ACLs but identifies the traffic more precisely.

The following CLI allows you to define ACLs by name or by an identification number.

```
Device(config)#ip access-list extended ?
<100-199> Extended IP access-list number
<2000-2699> Extended IP access-list number (expanded range)
WORD Access-list name
```

The following is the structure of a CLI ACL statement:

```
<sequence number> [permit/deny] <protocol> <address or any> eq <port number> <subnet>
<wildcard>
```

For example:

```
1 permit tcp any eq www 192.168.1.0 0.0.0.255
```

The sequence number specifies where to insert the Access Control list Entry (ACE) in the ACL order of ACEs. You can define your statements with sequences of 10, 20, 30, 40, and so on.

The controller GUI allows you to write a complete ACL going to the **Configuration** > **Security** > **ACL** page. You can view a list of protocols to pick from, and make changes to an existing ACL.

Applying ACLs

The following are the ways to apply ACLs:

- **Security ACL**: A security ACL defines the type of traffic that should be allowed through the device and that which should be blocked or dropped.

A security ACL is applied:

- **On SVI interfaces**: The ACL will only be evaluated against the traffic that is routed through the interface.

```
Device(config)# interface Vlan<number>
Device(config-if)# ip access-group myACL in/out
```

- **On a physical interface of the controller**: The ACL will be evaluated against all traffic that passes through the interface. Along with applying ACLs on SVI, this is another option for restricting traffic on the controller management plane.

```
Device(config)#interface GigabitEthernet1
Device(config-if)#ip access-group myACL in/out
```

- **In the wireless policy profile or WLAN**: This option includes several places where you can configure an ACL that will be applied to the wireless client traffic, in case of central switching or local switching of traffic. Such ACLs are only supported in the inbound direction.
- **On the AP**: In case of FlexConnect local switching, the ACL is configured and applied from the policy profile on the controller. This ACL has to be downloaded on to the AP through the Flex profile. ACLs must be downloaded to the AP before they can be applied. As an exception, fabric mode APs (in case of Software Defined Access) also use Flex ACLs even though the AP is not operating in Flex mode.

- **Punt ACL or Redirect ACL**: Punt ACL or redirect ACL refers to an ACL that specifies as to which traffic will be sent to the CPU (instead of its normal expected handling by the dataplane) for further processing. For example, the Central Web Authentication (CWA) redirect ACL defines as to which traffic is intercepted and redirected to the web login portal. The ACL does not define any traffic to be dropped or allowed, but follows the regular processing or forwarding rules, and what will be sent to the CPU for interception.

  A redirect ACL has an invisible last statement which is an implicit deny. This implicit deny is applied as a security access list entry (and therefore drops traffic that is not explicitly allowed through or sent to the CPU).

Types of URL Filters

The following are the two types of URL filters:

- **Standard**: Standard URL filters can be applied before client authentication (pre-auth) or after a successful client authentication (post-auth). Pre-auth filters are extremely useful in the case of external web authentication to allow access to the external login page, as well as, some internal websites before authentication takes place. Post-auth, they can work to block specific websites or allow only specific websites while all the rest is blocked by default. This type of URL filtering post-auth is better handled by using Cisco DNS Layer Security (formerly known as Umbrella) for more flexibility. The standard URL filters apply the same action (permit or deny) for the whole list of URLs. It is either all permit or all deny.
- **Enhanced**: Enhanced URL filters allow specification of a different action (deny or permit) for each URL inside the list and have per-URL hit counters.

In both types of URL filters, you can use a wildcard sub-domain such as **`*.cisco.com`**. URLfilters are standalone but always applied along with an IP-based ACL. A maximum of 20 URLs are supported in a given URL filter. Considering one URL can resolve multiple IP addresses, only up to 40 resolved IP addresses can

be tracked for each client. Only DNS records are tracked by URL filters. The controller or APs do not track the resolved IP address of a URL if the DNS answer uses a CNAME alias record.

Restrictions on DNS-Based Access Control Lists

The restriction for DNS-based ACLs is as follows:

- Pre-authentication and Post-authentication filters are supported in local modes. Only Pre-authentication filter is supported in Flex (Fabric) mode.
- ACL override pushed from ISE is not supported.
- FlexConnect Local Switching with External Web authentication using URL filtering is not supported until Cisco IOS XE Gibraltar 16.12.x.
- Fully qualified domain name (FQDN) or DNS based ACLs are not supported on Cisco Wave 1 Access Points.
- The URL filter considers only the first 20 URLs, though you can add more.
- The URL filter employs regular regex patterns and permits wildcard characters only at the beginning or at the end of an URL.
- The URL ACLs are defined and added to the FlexConnect policy profile in which they associate with a WLAN. The URL ACL creation follows a similar mechanism as that of local mode URL ACLs.
- In FlexConnect mode, the URL domain ACL works only if they are connected to a FlexConnect policy profile.
- The ACL can be attached to a WLAN by associating a policy profile with a WLAN or local policies. However, you can override it using "url-redirect-acl".
- For the Cisco AV pair received from ISE, the policy that needs to be applied for a particular client is pushed as part of ADD MOBILE

  message.
- When an AP joins or when an existing URL ACL is modified and applied on FlexConnect profile, the ACL definition along with mapped URL filter list is pushed to the AP.
- The AP stores the URL ACL definition with mapped ACL name and snoops the DNS packets for learning the first IP address for each URL in the ACL. When the AP learns the IP addresses, it updates the controller of the URL and IP bindings. The controller records this information in the client database for future use.
- When a client roams to another AP during the pre-authentication state, the learned IP addresses are pushed to a new AP. Otherwise, these learned IP addresses are purged when a client moves to a post-authentication state or when the TTL for the learned IP address expires.

Flex Mode

Applying URL Filter List to Flex Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *default-flex-profile* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Creates a new flex policy. The default flex profile name is *default-flex-profile*.
Step 3	**acl-policy** *acl policy name* **Example:** `Device(config-wireless-flex-profile)# acl-policy acl_name`	Configures ACL policy.
Step 4	**urlfilter list** *name* **Example:** `Device(config-wireless-flex-profile-acl)# urlfilter list urllist_flex_preauth`	Applies the URL list to the Flex profile.
Step 5	**end** **Example:** `Device(config-wireless-flex-profile-acl)# end`	Returns to privileged EXEC mode.

Configuring ISE for Central Web Authentication (GUI)

Perform the following steps to configure ISE for Central Web Authentication.

Procedure

Step 1 Login to the Cisco Identity Services Engine (ISE).

Step 2 Click **Policy** and then click **Policy Elements**.

Step 3 Click **Results**.

Step 4 Expand **Authorization** and click **Authorization Profiles**.

Step 5 Click **Add** to create a new authorization profile for URL filter.

Step 6 Enter a name for the profile in the **Name** field. For example, CentralWebauth.

Step 7 Choose **ACCESS_ACCEPT** option from the **Access Type** drop-down list.

Step 8 Alternatively, in the **Common Tasks** section, check **Web Redirection**..

Step 9 Choose the **Centralized Web Auth** option from the drop-down list.

Step 10 Specify the ACL and choose the ACL value from the drop-down list.

Step 11 In the **Advanced Attributes Setting** section, choose **Cisco:cisco-av-pair** from the drop-down list.

Note Multiple ACL can be applied on the controller based on priority. In L2 Auth + webauth multi-auth scenario, if the ISE returns ACL during L2 Auth then ISE ACL takes precedence over the default webauth redirect ACL. This leads to traffic running in webauth pending state, if ISE ACL has permit rule. To avoid this scenario, you need to set the precedence for L2 Auth ISE returned ACL. The default webauth redirect ACL priority is 100. To avoid traffic issue, you need to configure the redirect ACL priority above 100 for ACL returned by ISE.

Step 12 Enter the following one by one and click (+) icon after each of them:

- url-redirect-acl=<sample_name>
- url-redirect=<sample_redirect_URL>

  For example,

```
Cisco:cisco-av-pair = priv-lvl=15
Cisco:cisco-av-pair = url-redirect-acl=ACL-REDIRECT2
Cisco:cisco-av-pair = url-redirect=
https://9.10.8.247:port/portal/gateway?
sessionId=SessionIdValue&portal=0ce17ad0-6d90-11e5-978e-005056bf2f0a&daysToExpiry=value&action=cwa
```

Step 13 Verify contents in the **Attributes Details** section and click **Save**.

Local Mode

Defining URL Filter List

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**urlfilter list** *list-name* **Example:** `Device(config)# urlfilter list urllist_local_preauth`	Configures the URL filter list. Here, *list-name* refers to the URL filter list name. The list name must not exceed 32 alphanumeric characters.

	Command or Action	Purpose
Step 3	**action permit** **Example:** `Device(config-urlfilter-params)# action permit`	Configures the action: permit (allowed list) or deny (blocked list).
Step 4	**filter-type post-authentication** **Example:** `Device(config-urlfilter-params)# filter-type post-authentication`	**Note** This step is applicable while configuring post-authentication URL filter only. Configures the URL list as post-authentication filter.
Step 5	**redirect-server-ip4** *IPv4-address* **Example:** `Device(config-urlfilter-params)# redirect-server-ipv4 9.1.0.101`	Configures the IPv4 redirect server for the URL list. Here, *IPv4-address* refers to the IPv4 address.
Step 6	**redirect-server-ip6** *IPv6-address* **Example:** `Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::82`	Configures the IPv6 redirect server for the URL list. Here, *IPv6-address* refers to the IPv6 address.
Step 7	**url** *url* **Example:** `Device(config-urlfilter-params)# url url1.dns.com`	Configures an URL. Here, *url* refers to the name of the URL.
Step 8	**end** **Example:** `Device(config-urlfilter-params)# end`	Returns to privileged EXEC mode.

Applying URL Filter List to Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click on the **Policy Name**.

Step 3 Go to **Access Policies** tab.

Step 4 In the **URL Filters** section, choose the filters from the **Pre Auth** and **Post Auth** drop-down lists.

Step 5 Click **Update & Apply to Device**.

Applying URL Filter List to Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures wireless policy profile. Here, *profile-policy* refers to the name of the WLAN policy profile.

Step 3	**urlfilter list** {**pre-auth-filter** *name* | **post-auth-filter** *name*}
	Example:
	`Device(config-wireless-policy)# urlfilter list pre-auth-filter urllist_local_preauth`
	`Device(config-wireless-policy)# urlfilter list post-auth-filter urllist_local_postauth`
		Applies the URL list to the policy profile.
		Here, *name* refers to the name of the pre-authentication or post-authentication URL filter list configured earlier.
		Note During the client join, the URL filter configured on the policy will be applied.

Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.

Configuring ISE for Central Web Authentication

Creating Authorization Profiles

Procedure

Step 1 Login to the Cisco Identity Services Engine (ISE).
Step 2 Click **Policy**, and click **Policy Elements**.
Step 3 Click **Results**.
Step 4 Expand **Authorization**, and click **Authorization Profiles**.
Step 5 Click **Add** to create a new authorization profile for URL filter.
Step 6 In the Name field, enter a name for the profile. For example, *CentralWebauth*.
Step 7 Choose **ACCESS_ACCEPT** from the Access Type drop-down list.
Step 8 In the Advanced Attributes Setting section, choose **Cisco:cisco-av-pair** from the drop-down list.
Step 9 Enter the following one by one and click (+) icon after each of them:

- url-filter-preauth=<preauth_filter_name>
- url-filter-postauth=<postauth_filter_name>

For example,

```
Cisco:cisco-av-pair = url-filter-preauth=urllist_pre_cwa
Cisco:cisco-av-pair = url-filter-postauth=urllist_post_cwa
```

Step 10 Verify contents in the Attributes Details section and click **Save**.

Mapping Authorization Profiles to Authentication Rule

Procedure

Step 1 In the **Policy** > **Authentication** page, click **Authentication**.

Step 2 Enter a name for your authentication rule.

For example, *MAB*.

Step 3 In the If condition field, select the plus (+) icon.

Step 4 Choose **Compound condition**, and choose **WLC_Web_Authentication**.

Step 5 Click the arrow located next to **and ...** in order to expand the rule further.

Step 6 Click the + icon in the Identity Source field, and choose **Internal endpoints**.

Step 7 Choose **Continue** from the 'If user not found' drop-down list.

This option allows a device to be authenticated even if its MAC address is not known.

Step 8 Click **Save**.

Mapping Authorization Profiles to Authorization Rule

Procedure

Step 1 Click **Policy** > **Authorization**.

Step 2 In the Rule Name field, enter a name.

For example, *CWA Post Auth*.

Step 3 In the Conditions field, select the plus (+) icon.

Step 4 Click the drop-down list to view the Identity Groups area.

Step 5 Choose **User Identity Groups** > **user_group**.

Step 6 Click the plus (+) sign located next to **and ...** in order to expand the rule further.

Step 7 In the Conditions field, select the plus (+) icon.

Step 8 Choose **Compound Conditions**, and choose to create a new condition.

Step 9 From the settings icon, select **Add Attribute/Value** from the options.

Step 10 In the Description field, choose **Network Access** > **UseCase** as the attribute from the drop-down list.

Step 11 Choose the **Equals** operator.

Step 12 From the right-hand field, choose **GuestFlow**.

Step 13 In the Permissions field, select the plus (+) icon to select a result for your rule.

You can choose **Standard** > **PermitAccess** option or create a custom profile to return the attributes that you like.

Viewing DNS-Based Access Control Lists

To view details of a specified wireless URL filter, use the following command:

```
Device# show wireless urlfilter details <urllist_flex_preauth>
```

To view the summary of all wireless URL filters, use the following command:

```
Device# show wireless urlfilter summary
```

To view the URL filter applied to the client in the resultant policy section, use the following command:

```
Device# show wireless client mac-address <MAC_addr> detail
```

Configuration Examples for DNS-Based Access Control Lists

Flex Mode

Example: Defining URL Filter List

This example shows how to define URL list in Flex mode:

```
Device# configure terminal
Device(config)# urlfilter list urllist_flex_pre
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# redirect-server-ipv4 8.8.8.8
Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::81
Device(config-urlfilter-params)# url url1.dns.com
Device(config-urlfilter-params)# end
```

Example: Applying URL Filter List to Flex Profile

This example shows how to apply an URL list to the Flex profile in Flex mode:

```
Device# configure terminal
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy acl_name
Device(config-wireless-flex-profile-acl)# urlfilter list urllist_flex_preauth
Device(config-wireless-flex-profile-acl)# end
```

Local Mode

Example: Defining Preauth URL Filter List

This example shows how to define URL filter list (pre-authentication):

```
Device# configure terminal
Device(config)# urlfilter list urllist_local_preauth
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# redirect-server-ipv4 9.1.0.101
Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::82
Device(config-urlfilter-params)# url url1.dns.com
Device(config-urlfilter-params)# end
```

Example: Defining Postauth URL Filter List

This example shows how to define URL filter list (post-authentication):

```
Device# configure terminal
Device(config)# urlfilter list urllist_local_postauth
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# filter-type post-authentication
Device(config-urlfilter-params)# redirect-server-ipv4 9.1.0.101
Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::82
Device(config-urlfilter-params)# url url1.dns.com
Device(config-urlfilter-params)# end
```

Example: Applying URL Filter List to Policy Profile

This example shows how to apply an URL list to the policy profile in local mode:

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# urlfilter list pre-auth-filter urllist_local_preauth
Device(config-wireless-policy)# urlfilter list post-auth-filter urllist_local_postauth
Device(config-wireless-policy)# end
```

Verifying DNS Snoop Agent (DSA)

To view details of the DNS snooping agent client, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
```

To view details of the DSA enabled interface, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf
```

To view the pattern list in uCode memory, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
hw-pattern-list
```

To view the OpenDNS string for the pattern list, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
hw-pattern-list odns_string
```

To view the FQDN filter for the pattern list, use the following command:

```
Device#
show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list
fqdn-filter <fqdn_filter_ID>
```

Note The valid range of *fqdn_filter_ID* is from 1 to 16.

To view details of the DSA client, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client info
```

To view the pattern list in CPP client, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list
```

To view the OpenDNS string for the pattern list, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list
 odns_string
```

To view the FQDN filter for the pattern list, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list
 fqdn-filter <fqdn_filter_ID>
```

Note The valid range of *fqdn_filter_ID* is from 1 to 16.

To view details of the DSA datapath, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
```

To view details of the DSA IP cache table, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache
```

To view details of the DSA address entry, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache
 address {ipv4 <IPv4_addr> | ipv6 <IPv6_addr>}
```

To view details of all the DSA IP cache address, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache
 all
```

To view details of the DSA IP cache pattern, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache
 pattern <pattern>
```

To view details of the DSA datapath memory, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath memory
```

To view the DSA regular expression table, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
regexp-table
```

To view the DSA statistics, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath stats
```

Information About Flex Client IPv6 Support with WebAuth Pre and Post ACL

IOS IPv6 ACLs is used to send webauth ACL to an AP. A change in the ACL policies of the Flex profile (new ACL, deleted ACL or modified ACL).

ACL definitions are pushed to AP in the following events:

- AP join.
- New ACL mapping in a new Flex profile.
- Configuring IPv6 ACL definition in Flex profile.

Default Local Web Authentication ACLs

The pre-defined default LWA IPv6 ACL is pushed to AP and plumbed to data plane.

Default External Web Authentication ACL

The default EWA ACLs are derived from the redirect portal address configured in the parameter map.

The following list covers the types of default EWA ACLs:

- Security ACL—Pushed and plumbed to AP.
- Intercept ACL—Pushed and plumbed to data plane.

FQDN ACL

- FQDN ACL is encoded along with IPv6 ACL and sent to AP.
- FQDN ACL is always a custom ACL.

The following applies to Flex and Local mode:

- If you are migrating from AireOS, you would explicitly need to execute the following commands:

```
redirect append ap-mac tag ap_mac
redirect append wlan-ssid tag wlan
redirect append client-mac tag client_mac
```

- If the login page has any resource that needs to be fetched from the server, you will need to include those resource URLs in URL filtering.
- If you are trying to access IPv6 URL and you have an IPv4 web server, the controller redirects the client to an internal page as domain redirection is not supported. It is recommended to have a dual-stack web server and configure virtual IPv6 address in the global parameter map.

Enabling Pre-Authentication ACL for LWA and EWA (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**.

Step 4 Choose **Security** > **Layer2** tab. Uncheck the **WPAPolicy**, **AES** and **802.1x** check boxes.

Step 5 Choose **Security** > **Layer3** tab. Choose the Web Auth Parameter Map from the **Web Auth Parameter Map** drop-down list and authentication list from the **Authentication List** drop-down list. Click **Show Advanced Settings** and under the **Preauthenticated ACL** settings, choose the IPv6 ACL from the **IPv6** drop-down list.

Step 6 Choose **Security** > **AAA** tab. Choose the authentication list from the **Authentication List** drop-down list.

Step 7 Click **Apply to Device**.

Enabling Pre-Authentication ACL for LWA and EWA

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-demo 1 ssid-demo`	Enters the WLAN configuration sub-mode. • *wlan-name*—Enter the profile name. The range is from 1 to 32 alphanumeric characters. • *wlan-id*—Enter the WLAN ID. The range is from 1 to 512. • *SSID-name*—Enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID. **Note** If you have already configured WLAN, enter **wlan wlan-name** command.

	Command or Action	Purpose
Step 3	**ipv6 traffic-filter web** *acl_name-preauth* **Example:** `Device(config-wlan)# ipv6 traffic-filter web preauth_v6_acl`	Creates a pre-authentication ACL for web authentication.
Step 4	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables the WPA security.
Step 5	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)#no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 6	**no security wpa akm dot1x** **Example:** `Device(config-wlan)#no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 7	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Configures web authentication.
Step 8	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list wcm_dot1x`	Enables authentication list for WLAN.
Step 9	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map param-custom-webconsent`	Maps the parameter map.
Step 10	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Shutdown the WLAN.

Enabling Post-Authentication ACL for LWA and EWA (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**. The **Profile Name** is the profile name of the policy profile.

Step 4 Enter the **SSID** and the **WLAN ID**.

Step 5 Click **Apply to Device**.

Enabling Post-Authentication ACL for LWA and EWA

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy test1`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**ipv6 acl** *acl_name* **Example:** `Device(config-wireless-policy)# ipv6 acl testacl`	Creates a named WLAN ACL.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Enabling DNS ACL for LWA and EWA (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**. The **Profile Name** is the profile name of the policy profile.

Step 4 Enter the **SSID** and the **WLAN ID**.

Step 5 Click **Apply to Device**.

Enabling DNS ACL for LWA and EWA

Note Post-authentication DNS ACL is not supported.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy test1`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

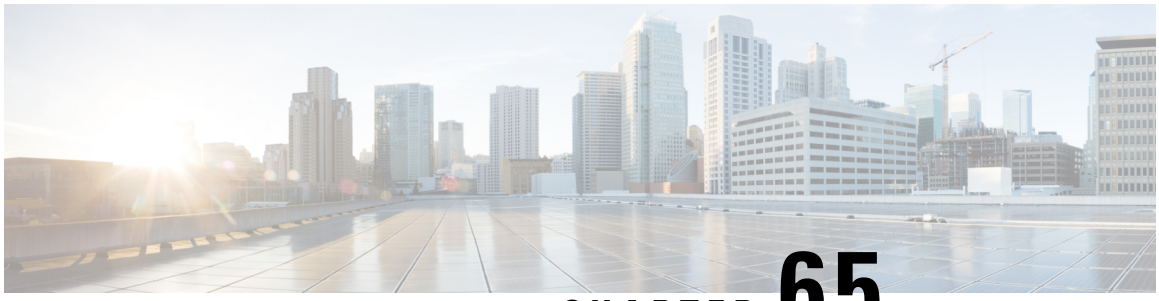
Verifying Flex Client IPv6 Support with WebAuth Pre and Post ACL

To verify the client state after L2 authentication, use the following command:

```
Device# show wireless client summary
Number of Local Clients: 1

MAC Address    AP Name                          WLAN  State             Protocol Method
  Role
-------------------------------------------------------------------------------------------------
1491.82b8.f8c1 AP4001.7A03.544C                 4      Webauth Pending   11n(5)   None
   Local

Number of Excluded Clients: 0
```

To verify the IP state, discovery, and MAC, use the following command:

```
Device# show wireless dev da ip
  IP                                        STATE       DISCOVERY   MAC
  ------------------------------------------------------------------------------------
  15.30.0.4                                 Reachable   ARP         1491.82b8.f8c1
  2001:15:30:0:d1d7:ecf3:7940:af60          Reachable   IPv6 Packet 1491.82b8.f8c1
  fe80::595e:7c29:d7c:3c84                  Reachable   IPv6 Packet 1491.82b8.f8c1
```



CHAPTER 65

Allowed List of Specific URLs

- Allowed List of Specific URLs, on page 541
- Adding URL to Allowed List, on page 541
- Verifying URLs on the Allowed List, on page 543

Allowed List of Specific URLs

This feature helps you to add specific URLs to allowed list on the controller or the AP so that those specific URLs are available for use, even when there is no connectivity to the internet. You can add URLs to allowed list for web authentication of captive portal and walled garden. Authentication is not required to access the allowed list of URLs. When you try to access sites that are not in allowed list, you are redirected to the Login page.

Adding URL to Allowed List

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**urlfilter list** *<urlfilter-name>* **Example:** `Device(config)# urlfilter list url-allowedlist-nbn`	Configures the URL filter profile.
Step 3	**action** [**deny** | **permit**] **Example:** `Device(config-urlfilter-params)# action permit`	Configures the list as allowed list. The **permit** command configures the list as allowed list and the **deny** command configures the list as blocked list.

	Command or Action	Purpose
Step 4	{**redirect-server-ipv4** | **redirect-server-ipv6**} **Example:** `Device(config-urlfilter-params)# redirect-server-ipv4 X.X.X.X`	Configures the IP address of the redirect servers to which the user requests will be redirected in case of denied requests.
Step 5	**url** *url-to-be-allowed* **Example:** `Device(config-urlfilter-params)# url www.cisco.com`	Configures the URL to be allowed.

Note The controller uses two IP addresses and the mechanism only allows for one portal IP to be allowed. To allow pre-authentication access to more HTTP ressources, you need to use URL filters which will dynamically makes holes in the intercept (redirect) and security (preauth) ACLs for the IPs related to the website whose URL you enter in the URL filter. DNS requests will be dynamically snooped for the controller to learn the IP address of those URLs and add it to the ACLs dynamically.

Note **redirect-server-ipv4** and **redirect-server-ipv6** is applicable only in the local mode, specifically in post-authentication. For any further tracking or displaying any warning messages, the denied user request is redirected to the configured server.

But the **redirect-server-ipv4** and **redirect-server-ipv6** configurations do not apply to pre-authentication scenario as you will be redirected to the controller for the redirect login URL for any denied access.

You can associate the allowed URL with the ACL policy in flex profile.

Example

Associating the allowed URL with the ACL policy in flex profile:

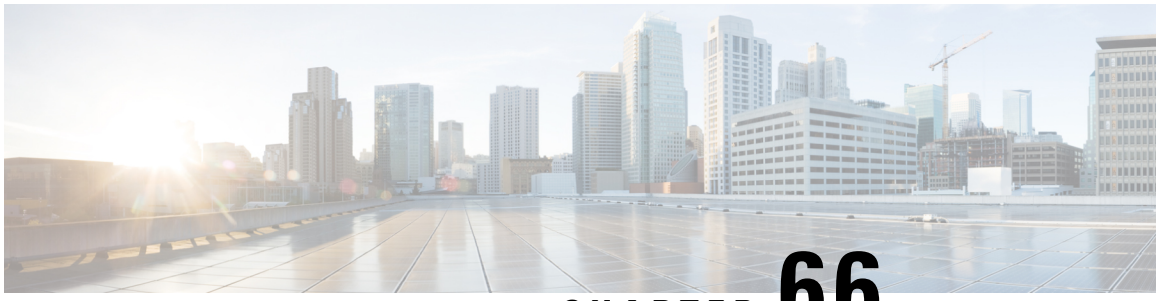
```
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy user_v4_acl
Device(config-wireless-flex-profile-acl)# urlfilter list url_allowedlist_nbn
Device(config-wireless-flex-profile-acl)# exit
Device(config-wireless-flex-profile)# description "default flex profile"

Device(config)# urlfilter enhanced-list urllist_pre_cwa
Device(config-urlfilter-enhanced-params)# url url1.dns.com preference 1 action permit
Device(config-urlfilter-enhanced-params)# url url2.dns.com preference 2 action deny
Device(config-urlfilter-enhanced-params)# url url3.dns.com preference 3 action permit

Device(config)# wlan wlan5 5 wlan5
Device(config-wlan)#ip access-group web user_v4_acl
Device(config-wlan)#no security wpa
Device(config-wlan)#no security wpa
Device(config-wlan)#no security wpa wpa2 ciphers aes
Device(config-wlan)#no security wpa akm dot1x
Device(config-wlan)#security web-auth
Device(config-wlan)#security web-auth authentication-list default
```

```
Device(config-wlan)#security web-auth parameter-map global
Device(config-wlan)#no shutdown
```

Verifying URLs on the Allowed List

To verify the summary and the details of the URLs on the allowed list, use the following **show** commands:

```
Device# show wireless urlfilter summary
Black-list    - DENY
White-list    - PERMIT
Filter-Type   - Specific to Local Mode

URL-List                        ID  Filter-Type  Action   Redirect-ipv4  Redirect-ipv6
-------------------------------------------------------------------------------------------------
url-whitelist                   1    PRE-AUTH     PERMIT   1.1.1.1

Device#

Device# show wireless urlfilter details url-whitelist
List Name..................... : url-whitelist
Filter ID..............  : : 1
Filter Type..............  : PRE-AUTH
Action..................... : PERMIT
Redirect server ipv4...... : 1.1.1.1
Redirect server ipv6...... :
Configured List of URLs
   URL..................... : www.cisco.com
```



CHAPTER 66

Web-Based Authentication

This chapter describes how to configure web-based authentication on the device. It contains these sections:

- Local Web Authentication Overview, on page 545
- How to Configure Local Web Authentication, on page 553
- Configuration Examples for Local Web Authentication, on page 568
- External Web Authentication (EWA), on page 573
- Authentication for Sleeping Clients, on page 578

Local Web Authentication Overview

Web authentication is a Layer 3 security solution designed for providing easy and secure guest access to hosts on WLAN with open authentication or appropriate layer 2 security methods. Web authentication allows users to get authenticated through a web browser on a wireless client, with minimal configuration on the client side. It allows users to associate with an open SSID without having to set up a user profile. The host receives an IP address and DNS information from the DHCP server, however cannot access any of the network resources until they authenticate successfully. When the host connects to the guest network, the WLC redirects the host to an authentication web page where the user needs to enter valid credentials. The credentials are authenticated by the WLC or an external authentication server and if authenticated successfully is given full access to the network. Hosts can also be given limited access to particular network resources before authentication for which the pre-authentication ACL functionality needs to be configured.

The following are the different types of web authentication methods:

- Local Web Authentication (LWA): Configured as Layer 3 security on the controller, the web authentication page and the pre-authentication ACL are locally configured on the controller. The controller intercepts htttp(s) traffic and redirects the client to the internal web page for authentication. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server.

- External Web Authentication (EWA): Configured as Layer 3 security on the controller, the controller intercepts htttp(s) traffic and redirects the client to the login page hosted on the external web server. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server. The pre-authentication ACL is configured statically on the controller.

- Central Web Authentication (CWA): Configured mostly as Layer 2 security on the controller, the redirection URL and the pre-authentication ACL reside on ISE and are pushed during layer 2 authentication to the controller. The controller redirects all web traffic from the client to the ISE login page. ISE validates the credentials entered by the client through HTTPS and authenticates the user.

Use the local web authentication feature, known as web authentication proxy, to authenticate end users on host systems that do not run the IEEE 802.1x supplicant.

When a client initiates an HTTP session, local web authentication intercepts ingress HTTP packets from the host and sends an HTML login page to the users. The users enter their credentials, which the local web authentication feature sends to the authentication, authorization, and accounting (AAA) server for authentication.

If authentication succeeds, local web authentication sends a Login-Successful HTML page to the host and applies the access policies returned by the AAA server.

If authentication fails, local web authentication forwards a Login-Fail HTML page to the user, prompting the user to retry the login. If the user exceeds the maximum number of attempts, local web authentication forwards a Login-Expired HTML page to the host, and the user is excluded with the exclusion reason as Web authentication failure.

Note You should use either global or named parameter-map under WLAN (for method-type, custom, and redirect) for using the same web authentication methods, such as consent, web consent, and webauth. Global parameter-map is applied by default, if none of the parameter-map is configured under WLAN.

Note The traceback that you receive when webauth client tries to do authentication does not have any performance or behavioral impact. It happens rarely when the context for which FFM replied back to EPM for ACL application is already dequeued (possibly due to timer expiry) and the session becomes ‘unauthorized’.

Note When command authorization is enabled as a part of AAA Authorization configuration through TACACS and the corresponding method list is not configured as a part of the HTTP configuration, WebUI pages will not load any data. However, some wireless feature pages may work as they are privilege based and not command based.

Based on where the web pages are hosted, the local web authentication can be categorized as follows:

- *Internal*—The internal default HTML pages (Login, Success, Fail, and Expire) in the controller are used during the local web authentication.
- *Customized*—The customized web pages (Login, Success, Fail, and Expire) are downloaded onto the controller and used during the local web authentication.
- *External*—The customized web pages are hosted on the external web server instead of using the in-built or custom web pages.

Based on the various web authentication pages, the types of web authentication are as follows:

- *Webauth*—This is a basic web authentication. Herein, the controller presents a policy page with the user name and password. You need to enter the correct credentials to access the network.
- *Consent or web-passthrough*—Herein, the controller presents a policy page with the Accept or Deny buttons. You need to click the Accept button to access the network.

- *Webconsent*—This is a combination of webauth and consent web authentication types. Herein, the controller presents a policy page with Accept or Deny buttons along with user name or password. You need to enter the correct credentials and click the Accept button to access the network.

Note

- You can view the webauth parameter-map information using the **show running-config** command output.
- The wireless Web-Authentication feature does not support the bypass type.
- Change in web authentication parameter map redirect login URL does not occur until a AP rejoin happens. You must enable and disable the WLAN to apply the new URL redirection.

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:

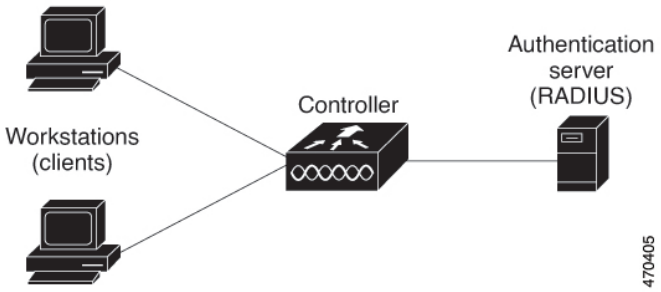
```
<body onload="loadAction();">
```

Device Roles

With local web authentication, the devices in the network have these specific roles:

- *Client*—The device (workstation) that requests access to the network and the controller and responds to requests from the controller. The workstation must be running an HTML browser with Java Script enabled.
- *Authentication server*—Authenticates the client. The authentication server validates the identity of the client and notifies the controller that the client is authorized to access the network and the controller services or that the client is denied.
- *Controller*—Controls the physical access to the network based on the authentication status of the client. The controller acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client.

Figure 9: Local Web Authentication Device Roles



Authentication Process

When the page is hosted on the controller, the controller uses its virtual IP (a non-routable IP like 192.0.2.1 typically) to serve the request. If the page is hosted externally, the web redirection sends the client first to the virtual IP, which then sends the user again to the external login page while it adds arguments to the URL, such as the location of the virtual IP. Even when the page is hosted externally, the user submits its credentials to the virtual IP.

When you enable local web authentication, these events occur:

- The user initiates an HTTP session.
- The HTTP traffic is intercepted, and authorization is initiated. The controller sends the login page to the user. The user enters a username and password, and the controller sends the entries to the authentication server.
- If the authentication succeeds, the controller downloads and activates the user's access policy from the authentication server. The login success page is sent to the user.
- If the authentication fails, the controller sends the login fail page. The user retries the login. If the maximum number of attempts fails, the controller sends the login expired page, and the host is placed in a watch list. After the watch list times out, the user can retry the authentication process.
- If authentication server is not available, after the web authentication retries, the client moves to the excluded state and the client receives an Authentication Server is Unavailable page.
- The controller reauthenticates a client when the host does not respond to an ARP probe on a Layer 2 interface, or when the host does not send any traffic within the idle timeout on a Layer 3 interface.
- Web authentication sessions can not apply new VLAN as part of the authorization policy, as the client already has been assigned an IP address and you will not be able to change the IP address in the client, in case the VLAN changes.
- If the terminate action is default, the session is dismantled, and the applied policy is removed.

Note Do not use semicolons (;) while configuring username for GUI access.

Local Web Authentication Banner

With Web Authentication, you can create a default and customized web-browser banners that appears when you log in to the controller.

The banner appears on both the login page and the authentication-result pop-up pages. The default banner messages are as follows:

- *Authentication Successful*
- *Authentication Failed*
- *Authentication Expired*

The Local Web Authentication Banner can be configured as follows:

- Use the following global configuration command:

```
Device(config)# parameter map type webauth global
Device(config-params-parameter-map)# banner ?
file <file-name>
text <Banner text>
title <Banner title>
```

The default banner *Cisco Systems* and *Switch host-name Authentication* appear on the Login Page. *Cisco Systems* appears on the authentication result pop-up page.

Figure 10: Authentication Successful Banner

The banner can be customized as follows:

- Add a message, such as switch, router, or company name to the banner:
  - New-style mode—Use the following global configuration command:

    parameter-map type webauth global

    banner text <text>

- Add a logo or text file to the banner:
  - New-style mode—Use the following global configuration command:

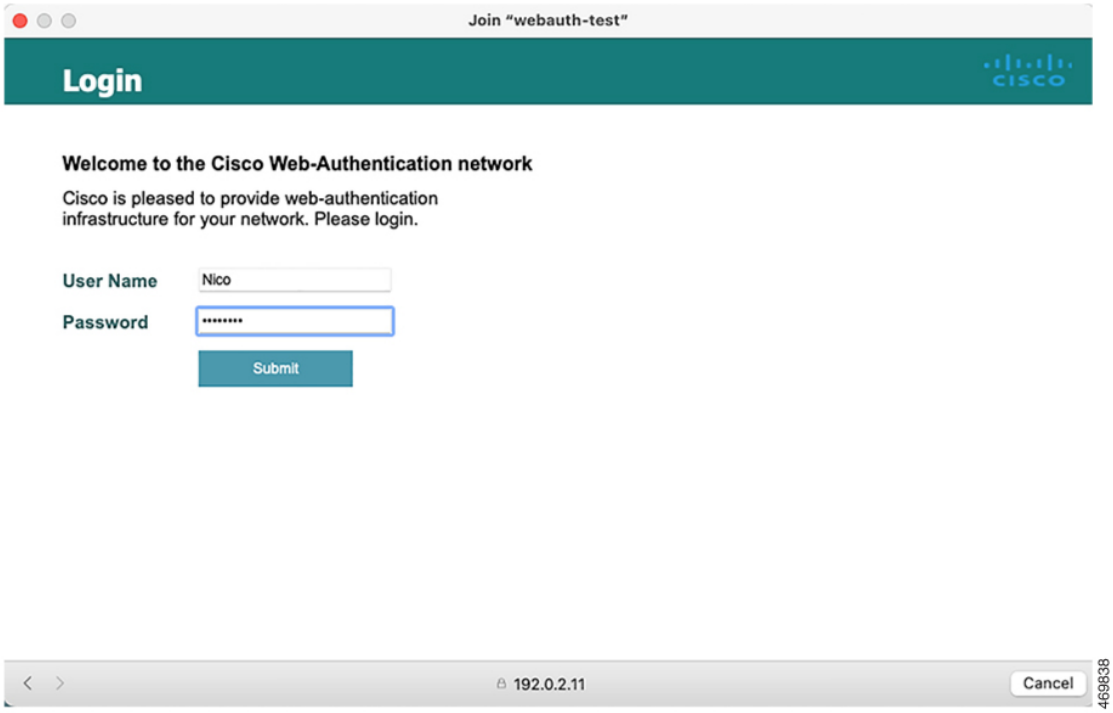
    parameter-map type webauth global

    banner file <filepath>

Figure 11: Customized Web Banner

If you do not enable a banner, only the username and password dialog boxes appear in the web authentication login screen, and no banner appears when you log into the switch.

Figure 12: Login Screen With No Banner



Customized Local Web Authentication

During the local web authentication process, the switch's internal HTTP server hosts four HTML pages to deliver to an authenticating client. The server uses these pages to notify you of these four authentication process states:

- Login: Your credentials are requested
- Success: The login was successful
- Fail: The login failed
- Expire: The login session has expired because of excessive login failures

Note Virtual IP address is mandatory to configure custom web authentication.

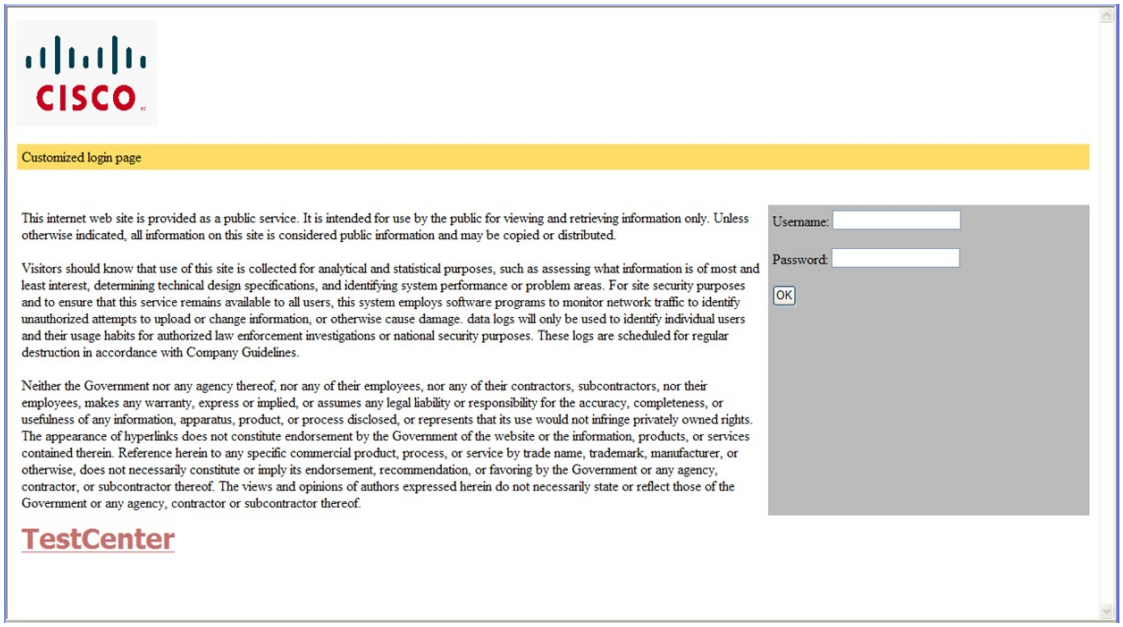
Guidelines

- You can substitute your own HTML pages for the default internal HTML pages.
- You can use a logo or specify text in the *login*, *success*, *failure*, and *expire* web pages.
- On the banner page, you can specify text in the login page.
- The pages are in HTML.

- You must include an HTML redirect command in the success page to access a specific URL.
- The URL string must be a valid URL (for example, http://www.cisco.com). An incomplete URL might cause *page not found* or similar errors on a web browser.
- If you configure web pages for HTTP authentication, they must include the appropriate HTML commands (for example, to set the page time out, to set a hidden password, or to confirm that the same page is not submitted twice). The custom page samples in the webauth bundle are provided with the image and the details of what you can and cannot change.
- The CLI command to redirect users to a specific URL is not available when the configured login form is enabled. The administrator should ensure that the redirection is configured in the web page.
- If the CLI command redirecting users to specific URL after authentication occurs is entered and then the command configuring web pages is entered, the CLI command redirecting users to a specific URL does not take effect.
- Configured web pages can be copied to the switch boot flash or flash.
- The login page can be on one flash, and the success and failure pages can be another flash (for example, the flash on the active switch or a member switch).
- You must configure all four pages.
- All of the logo files (image, flash, audio, video, and so on) that are stored in the system directory (for example, flash, disk0, or disk) and that are displayed on the login page must use *web_auth_<filename>* as the file name.
- The configured authentication proxy feature supports both HTTP and SSL.

You can substitute your HTML pages for the default internal HTML pages. You can also specify a URL to which users are redirected after authentication occurs, which replaces the internal Success page.

Figure 13: Customizable Authentication Page



Redirection URL for Successful Login Guidelines

When configuring a redirection URL for successful login, consider these guidelines:

- If the custom authentication proxy web pages feature is enabled, the redirection URL feature is disabled and is not available in the CLI. You can perform redirection in the custom-login success page.
- If the redirection URL feature is enabled, a configured auth-proxy-banner is not used
- To remove the specification of a redirection URL, use the **no** form of the command.
- If the redirection URL is required after the web-based authentication client is successfully authenticated, then the URL string must start with a valid URL (for example, http://) followed by the URL information. If only the URL is given without http://, then the redirection URL on successful authentication might cause page not found or similar errors on a web browser.

How to Configure Local Web Authentication

Configuring Default Local Web Authentication

The following table shows the default configurations required for local web authentication.

Table 16: Default Local Web Authentication Configuration

Feature	Default Setting
AAA	Disabled
RADIUS server • IP address • UDP authentication port • Key	• None specified
Default value of inactivity timeout	3600 seconds
Inactivity timeout	Disabled

Configuring AAA Authentication (GUI)

Note The WebUI does not support the ipv6 radius source-interface under AAA radius server group configuration.

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA**.

Step 2 In the **Authentication** section, click **Add**.

Step 3 In the **Quick Setup: AAA Authentication** window that is displayed, enter a name for your method list.

Step 4 Choose the type of authentication you want to perform before allowing access to the network, in the **Type** drop-down list.

Step 5 Choose if you want to assign a group of servers as your access server, or if you want to use a local server to authenticate access, from the **Group** Type drop-down list.

Step 6 To configure a local server to act as a fallback method when servers in the group are unavailable, check the **Fallback** to local check box.

Step 7 Choose the server groups you want to use to authenticate access to your network, from the **Available Server Groups** list and click > icon to move them to the **Assigned Server Groups** list.

Step 8 Click **Save & Apply to Device**.

Configuring AAA Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA functionality.
Step 2	**aaa authentication login** {**default** | *named_authentication_list*} **group** *AAA_group_name* **Example:** `Device(config)# aaa authentication login default group group1`	Defines the list of authentication methods at login. **named_authentication_list** refers to any name that is not greater than 31 characters. **AAA_group_name** refers to the server group name. You need to define the server-group **server_name** at the beginning itself.
Step 3	**aaa authorization network** {**default** | **named**} **group** *AAA_group_name* **Example:** `Device(config)# aaa authorization network default group group1`	Creates an authorization method list for web-based authorization.
Step 4	**tacacs server** *server-name* **Example:** `Device(config)# tacacs server yourserver`	Specifies an AAA server.

	Command or Action	Purpose
Step 5	**address** {**ipv4** | **ipv6**}*ip_address* **Example:** `Device(config-server-tacacs)# address ipv4 10.0.1.12`	Configures the IP address for the TACACS server.
Step 6	**tacacs-server host** {*hostname* | *ip_address*} **Example:** `Device(config)# tacacs-server host 10.1.1.1`	Specifies a AAA server.

Configuring the HTTP/HTTPS Server (GUI)

Procedure

Step 1 Choose **Administration** > **Management** > **HTTP/HTTPS/Netconf**.

Step 2 In the **HTTP/HTTPS Access Configuration** section, enable HTTP Access and enter the port that will listen for HTTP requests. The default port is 80. Valid values are 80, and ports between 1025 and 65535.

Step 3 Enable **HTTPS Access** on the device and enter the designated port to listen for HTTPS requests. The default port is 1025. Valid values are 443, and ports between 1025 and 65535. On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over the Internet. HTTP with SSL encryption provides a secure connection to allow such functions as configuring a switch from a Web browser.

Step 4 Choose the **Personal Identity Verification** as enabled or disabled.

Step 5 In the **HTTP Trust Point Configuration** section, enable **Enable Trust Point** to use Certificate Authority servers as trustpoints.

Step 6 From the **Trust Points** drop-down list, choose a trust point.

Step 7 In the **Timeout Policy Configuration** section, enter the HTTP timeout policy in seconds. Valid values can range from 1 to 600 seconds.

Step 8 Enter the number of minutes of inactivity allowed before the session times out. Valid values can range from 180 to 1200 seconds.

Step 9 Enter the server life time in seconds. Valid values can range from 1 to 86400 seconds.

Step 10 Enter the maximum number of requests the device can accept. Valid values range from 1 to 86400 requests.

Step 11 Save the configuration.

Configuring the HTTP Server (CLI)

To use local web authentication, you must enable the HTTP server within the device. You can enable the server for either HTTP or HTTPS.

Note The Apple psuedo-browser will not open if you configure only the **ip http secure-server** command. You should also configure the **ip http server** command.

Follow the procedure given below to enable the server for either HTTP or HTTPS:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip http server** **Example:** `Device(config)# ip http server`	Enables the HTTP server. The local web authentication feature uses the HTTP server to communicate with the hosts for user authentication.
Step 3	**ip http secure-server** **Example:** `Device(config)# ip http secure-server`	Enables HTTPS. You can configure custom authentication proxy web pages or specify a redirection URL for successful login. **Note** To ensure secure authentication when you enter the **ip http secure-server** command, the login page is always in HTTPS (secure HTTP) even if the user sends an HTTP request.
Step 4	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Creating a Parameter Map (GUI)

Procedure

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

Step 2 Click **Add**.

Step 3 Click **Policy Map**.

Step 4 Enter **Parameter Name**, **Maximum HTTP connections**, **Init-State Timeout(secs)** and choose **webauth** in the **Type** drop-down list.

Step 5 Click **Apply to Device**.

Creating Parameter Maps

Configuring Local Web Authentication (GUI)

Procedure

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

Step 2 On the **Web Auth** page, click **Add**.

Step 3 In the **Create Web Auth Parameter** window that is displayed, enter a name for the parameter map.

Step 4 In the **Maximum HTTP Connections** field, enter the maximum number of HTTP connections that you want to allow.

Step 5 In the **Init-State Timeout** field, enter the time after which the init state timer should expire due to user's failure to enter valid credentials in the login page.

Step 6 Choose the type of Web Auth parameter.

Step 7 Click **Apply to Device**.

Step 8 On the **Web Auth** page, click the name of the parameter map.

Step 9 In the **Edit WebAuth Parameter** window that is displayed, choose the required **Banner Type**.

- If you choose **Banner Text**, enter the required banner text to be displayed.
- If you choose **File Name**, specify the path of the file from which the banner text has to be picked up.

Step 10 Enter the virtual IP addresses as required.

Step 11 Set appropriate status of **WebAuth Intercept HTTPS**, **Captive Bypass Portal**.

Step 12 Set appropriate status for **Disable Success Window**, **Disable Logout Window**, and **Login Auth Bypass for FQDN**.

Step 13 Check the **Sleeping Client Status** check box to enable authentication of sleeping clients and then specify the **Sleeping Client Timeout** in minutes. Valid range is between 10 minutes and 43200 minutes.

Step 14 Click the **Advanced** tab.

Step 15 To configure external web authentication, perform these tasks:

a) In the **Redirect for log-in** field, enter the name of the external server to send login request.
b) In the **Redirect On-Success** field, enter the name of the external server to redirect after a successful login.
c) In the **Redirect On-Failure** field, enter the name of the external server to redirect after a login failure.
d) (Optional) Under **Redirect to External Server** in the **Redirect Append for AP MAC Address** field, enter the AP MAC address.
e) (Optional) In the **Redirect Append for Client MAC Address** field, enter the client MAC address.
f) (Optional) In the **Redirect Append for WLAN SSID** field, enter the WLAN SSID.
g) In the **Portal IPV4 Address** field, enter the IPv4 address of the portal to send redirects.
h) In the **Portal IPV6 Address** field, enter the IPv6 address of the portal to send redirects, if IPv6 address is used.

Step 16 To configure customized local web authentication, perform these tasks:

a) Under **Customized Page**, specify the following pages:

- **Login Failed Page**
- **Login Page**
- **Logout Page**
- **Login Successful Page**

Step 17 Click **Update & Apply**.

Configuring the Internal Local Web Authentication (CLI)

Follow the procedure given below to configure the internal local web authentication:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** {*parameter-map-name* | **global**} **Example:** `Device(config)# parameter-map type webauth sample`	Creates the parameter map. The **parameter-map-name** must not exceed 99 characters.
Step 3	**end** **Example:** `Device(config-params-parameter-map)# end`	Returns to privileged EXEC mode.

Configuring the Customized Local Web Authentication (CLI)

Follow the procedure given below to configure the customized local web authentication:

Note Virtual IP address is mandatory for custom web authentication.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** *parameter-map-name* **Example:** `Device(config)# parameter-map type webauth sample`	Configures the webauth type parameter. **Note** You need to configure a virtual IP in the global parameter map to use the customized web authentication bundle.
Step 3	**type** {**authbypass** | **consent** | **webauth** | **webconsent**} **Example:** `Device(config-params-parameter-map)# type webauth`	Configures webauth sub-types, such as passthru, consent, webauth, or webconsent.
Step 4	**custom-page login device** *html-filename* **Example:** `Device(config-params-parameter-map)# custom-page login device bootflash:login.html`	Configures the customized login page.
Step 5	**custom-page login expired device** *html-filename* **Example:** `Device(config-params-parameter-map)# custom-page login expired device bootflash:loginexpired.html`	Configures the customized login expiry page.
Step 6	**custom-page success device** *html-filename* **Example:** `Device(config-params-parameter-map)# custom-page success device bootflash:loginsuccess.html`	Configures the customized login success page.
Step 7	**custom-page failure device** *html-filename* **Example:** `Device(config-params-parameter-map)#`	Configures the customized login failure page.

	Command or Action	Purpose
	`custom-page failure device bootflash:loginfail.html`	
Step 8	**end** **Example:** `Device(config-params-parameter-map)# end`	Returns to privileged EXEC mode.

Configuring the External Local Web Authentication (CLI)

Follow the procedure given below to configure the external local web authentication:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** *parameter-map-name* **Example:** `Device(config)# parameter-map type webauth sample`	Configures the webauth type parameter.
Step 3	**type** {**authbypass** | **consent** | **webauth** | **webconsent**} **Example:** `Device(config-params-parameter-map)# type webauth`	Configures the webauth sub-types, such as authbypass, consent, passthru, webauth, or webconsent.
Step 4	**redirect** [**for-login** | **on-failure** | **on-success**] *URL* **Example:** `Device(config-params-parameter-map)# redirect for-login http://www.cisco.com/login.html`	Configures the redirect URL for the login, failure, and success pages. **Note** In the redirect url, you need to press *Ctrl+v* and type *?* to configure the *?* character. The *?* character is commonly used in URL when ISE is configured as an external portal.
Step 5	**redirect portal** {**ipv4** | **ipv6**} *ip-address*	Configures the external portal IPv4 address.

	Command or Action	Purpose
	Example: `Device(config-params-parameter-map)# redirect portal ipv4 23.0.0.1`	**Note** The IP address should be one of the associated IP addresses of the domain and not a random IP address when using FQDN. It is recommended to use the FQDN URL here, if a given domain resolves to more than a single IP address.
Step 6	**end** **Example:** `Device(config-params-parameter-map)# end`	Returns to privileged EXEC mode.

Configuring the Web Authentication WLANs

Follow the procedure given below to configure WLAN using web auth security and map the authentication list and parameter map:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id ssid-name* **Example:** `Device(config)# wlan mywlan 34 mywlan-ssid`	Specifies the WLAN name and ID. *profile-name* is the WLAN name which can contain 32 alphanumeric characters. *wlan-id* is the wireless LAN identifier. The valid range is from 1 to 512. *ssid-name* is the SSID which can contain 32 alphanumeric characters.
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables the WPA security.
Step 4	**security web-auth** **Example:**	Enables web authentication for WLAN.

	Command or Action	Purpose
	`Device(config-wlan)# security web-auth`	

Step 5	**security web-auth** {**authentication-list** *authentication-list-name* | **parameter-map** *parameter-map-name*}
	Example:
	`Device(config-wlan)# security web-auth authentication-list webauthlistlocal`
	`Device(config-wlan)# security web-auth parameter-map sample`
		Enables web authentication for WLAN.
		Here,
		• **authentication-list** *authentication-list-name*: Sets the authentication list for IEEE 802.1x.
		• **parameter-map** *parameter-map-name*: Configures the parameter map.
		Note When **security web-auth** is enabled, you get to map the default **authentication-list** and global **parameter-map**. This is applicable for authentication-list and parameter-map that are not explicitly mentioned.

Step 6	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Configuring Pre-Auth Web Authentication ACL (GUI)

Before you begin

Ensure that you have configured an access control list (ACL) and a WLAN.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.
Step 2 Click the name of the WLAN.
Step 3 In the **Edit WLAN** window, click the **Security** tab and then click the **Layer3** tab.
Step 4 Click **Show Advanced Settings**.
Step 5 In the **Preauthenticaion ACL** section, choose the appropriate ACL to be mapped to the WLAN.
Step 6 Click **Update & Apply to Device**.

Configuring Pre-Auth Web Authentication ACL (CLI)

Follow the procedure given below to configure pre-auth web authentication ACL:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**access-list** *access-list-number* {**deny** | **permit**} *hostname source-wildcard-bits* **Example:** `Device(config)# access-list 2 deny your_host 10.1.1.1 log`	Creates an ACL list. The *access-list-number* is a decimal number from 1 to 99, 100 to 199, 300 to 399, 600 to 699, 1300 to 1999, 2000 to 2699, or 2700 to 2799. Enter **deny** or **permit** to specify whether to deny or permit if the conditions are matched. The *source* is the source address of the network or host from which the packet is being sent specified as: • The 32-bit quantity in dotted-decimal format. • The keyword **any** as an abbreviation for *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard. • The keyword **host** as an abbreviation for *source* and *source-wildcard* of source 0.0.0.0. (Optional) The *source-wildcard* applies wildcard bits to the source.
Step 3	**wlan** *profile-name wlan-id ssid-name* **Example:** `Device(config)# wlan mywlan 34 mywlan-ssid`	Creates the WLAN. *profile-name* is the WLAN name which can contain 32 alphanumeric characters. *wlan-id* is the wireless LAN identifier. The valid range is from 1 to 512. *ssid-name* is the SSID which can contain 32 alphanumeric characters.
Step 4	**ip access-group web** *access-list-name* **Example:** `Device(config-wlan)# ip access-group web name`	Maps the ACL to the web auth WLAN. *access-list-name* is the IPv4 ACL name or ID.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Configuring the Maximum Web Authentication Request Retries

Follow these steps to configure the maximum web authentication request retries:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wireless security web-auth retries** *number* **Example:** `Device(config)# wireless security web-auth retries 2`	*number* is the maximum number of web auth request retries. The valid range is 0 to 20.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring a Local Banner in Web Authentication Page (GUI)

Procedure

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

Step 2 In the **Webauth Parameter Map** tab, click the parameter map name. The **Edit WebAuth Parameter** window is displayed.

Step 3 In the **General** tab and choose the required Banner Type:

- If you choose **Banner Text**, enter the required banner text to be displayed.
- If you choose **File Name**, specify the path of the file from which the banner text has to be picked up.

Step 4 Click **Update & Apply**.

Configuring a Local Banner in Web Authentication Page (CLI)

Follow the procedure given below to configure a local banner in web authentication pages.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** *param-map* **Example:** `Device(config)# parameter-map type webauth param-map`	Configures the web authentication parameters. Enters the parameter map configuration mode.
Step 3	**banner** [*file* | *banner-text* | *title*] **Example:** `Device(config-params-parameter-map)# banner http C My Switch C`	Enables the local banner. Create a custom banner by entering *C banner-text C* (where *C* is a delimiting character), or *file* that indicates a file (for example, a logo or text file) that appears in the banner, or *title* that indicates the title of the banner.
Step 4	**end** **Example:** `Device(config-params-parameter-map)# end`	Returns to privileged EXEC mode.

Configuring Type WebAuth, Consent, or Both

Procedure

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

	Command or Action	Purpose
Step 2	**parameter-map type webauth** *parameter-map name* **Example:** `Device (config) # parameter-map type webauth webparalocal`	Configures the webauth type parameter.
Step 3	**type consent** **Example:** `Device (config-params-parameter-map) # type consent`	Configures webauth type as consent. You can configure the type as webauth, consent, or both (webconsent).
Step 4	**end** **Example:** `Device (config-params-parameter-map) # end`	Returns to privileged EXEC mode.
Step 5	**show running-config | section parameter-map type webauth** *parameter-map* **Example:** `Device (config) # show running-config | section parameter-map type webauth test`	Displays the configuration details.

Configuring Preauthentication ACL

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name* **Example:** `Device (config)# wlan ramban`	For *wlan-name*, enter the profile name.
Step 3	**shutdown** **Example:** `Device (config-wlan)# shutdown`	Disables the WLAN.
Step 4	**ip access-group web** *preauthrule* **Example:** `Device (config-wlan)# ip access-group web preauthrule`	Configures ACL that has to be applied before authentication.

	Command or Action	Purpose
Step 5	**no shutdown** **Example:** `Device (config)# no shutdown`	Enables the WLAN.
Step 6	**end** **Example:** `Device (config-wlan)# end`	Returns to privileged EXEC mode.
Step 7	**show wlan name** *wlan-name* **Example:** `Device# show wlan name ramban`	Displays the configuration details.

Configuring TrustPoint for Local Web Authentication

Before you begin

Ensure that a certificate is installed on your controller . Using trustpoint controller presents the domain specific certificate that client browser trusts when it gets redirected to ***.com** portal.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth global** **Example:** `Device (config)# parameter-map type webauth global`	Creates the parameter map.
Step 3	**trustpoint** *trustpoint-name* **Example:** `Device (config-params-parameter-map)# trustpoint trustpoint-name`	Configures trustpoint for local web authentication.
Step 4	**end** **Example:** `Device (config-params-parameter-map)# end`	Returns to privileged EXEC mode.

Configuration Examples for Local Web Authentication

Example: Obtaining Web Authentication Certificate

This example shows how to obtain web authentication certificate.

```
Device# configure terminal
Device(config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco
Device(config)# end
Device# show crypto pki trustpoints cert
 Trustpoint cert:
    Subject Name:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
          Serial Number (hex): 00
    Certificate configured.
Device# show  crypto pki certificates cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    Name: ldapserver
    e=rkannajr@cisco.com
    cn=ldapserver
    ou=WNBU
    o=Cisco
    st=California
    c=US
  Validity Date:
    start date: 07:35:23 UTC Jan 31 2012
    end   date: 07:35:23 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12
  Storage: nvram:rkannajrcisc#4.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 00
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
```

```
    c=US
  Subject:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Validity Date:
    start date: 07:27:56 UTC Jan 31 2012
    end   date: 07:27:56 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12 ldap
  Storage: nvram:rkannajrcisc#0CA.cer
```

Example: Displaying a Web Authentication Certificate

This example shows how to display a web authentication certificate.

```
Device# show crypto ca certificate verb
     Certificate
     Status: Available
     Version: 3
     Certificate Serial Number (hex): 2A9636AC00000000858B
     Certificate Usage: General Purpose
     Issuer:
    cn=Cisco Manufacturing CA
    o=Cisco Systems
    Subject:
    Name: WS-C3780-6DS-S-2037064C0E80
    Serial Number: PID:WS-C3780-6DS-S SN:FOC1534X12Q
    cn=WS-C3780-6DS-S-2037064C0E80
    serialNumber=PID:WS-C3780-6DS-S SN:FOC1534X12Q
    CRL Distribution Points:
    http://www.cisco.com/security/pki/crl/cmca.crl
    Validity Date:
    start date: 15:43:22 UTC Aug 21 2011
    end   date: 15:53:22 UTC Aug 21 2021
    Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
    Signature Algorithm: SHA1 with RSA Encryption
    Fingerprint MD5: A310B856 A41565F1 1D9410B5 7284CB21
    Fingerprint SHA1: 04F180F6 CA1A67AF 9D7F561A 2BB397A1 0F5EB3C9
    X509v3 extensions:
    X509v3 Key Usage: F0000000
      Digital Signature
      Non Repudiation
      Key Encipherment
      Data Encipherment
    X509v3 Subject Key ID: B9EEB123 5A3764B4 5E9C54A7 46E6EECA 02D283F7
    X509v3 Authority Key ID: D0C52226 AB4F4660 ECAE0591 C7DC5AD1 B047F76C
    Authority Info Access:
    Associated Trustpoints: CISCO_IDEVID_SUDI
    Key Label: CISCO_IDEVID_SUDI
```

Example: Choosing the Default Web Authentication Login Page

This example shows how to choose a default web authentication login page.

```
Device# configure terminal
Device(config)# parameter-map type webauth test
This operation will permanently convert all relevant authentication commands to their CPL
control-policy equivalents. As this conversion is irreversible and will
disable the conversion CLI 'authentication display [legacy|new-style]', you are strongly
advised to back up your current configuration before proceeding.
Do you wish to continue? [yes]: yes
Device(config)# wlan wlan50
Device(config-wlan)# shutdown
Device(config-wlan)# security web-auth authentication-list test
Device(config-wlan)# security web-auth parameter-map test
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show running-config | section wlan50
wlan wlan50 50 wlan50
 security wpa akm cckm
 security wpa wpa1
 security wpa wpa1 ciphers aes
 security wpa wpa1 ciphers tkip
 security web-auth authentication-list test
 security web-auth parameter-map test
 session-timeout 1800
 no shutdown

Device# show running-config | section parameter-map type webauth test
parameter-map type webauth test
 type webauth
```

Example: Choosing a Customized Web Authentication Login Page from an IPv4 External Web Server

This example shows how to choose a customized web authentication login page from an IPv4 external web server.

```
Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# virtual-ip ipv4 192.0.2.1.
Device(config-params-parameter-map)# parameter-map type webauth test
Device(config-params-parameter-map)# type webauth
Device(config-params-parameter-map)# redirect for-login http://9.1.0.100/login.html
Device(config-params-parameter-map)# redirect portal ipv4 9.1.0.100
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv4 192.0.2.1.
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

Example: Choosing a Customized Web Authentication Login Page from an IPv6 External Web Server

This example shows how to choose a customized web authentication login page from an IPv6 external web server.

```
Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# virtual-ip ipv6 2001:DB8::/48
Device(config-params-parameter-map)# parameter-map type webauth test
Device(config-params-parameter-map)# type webauth
Device(config-params-parameter-map)# redirect for-login http://9:1:1::100/login.html
Device(config-params-parameter-map)# redirect portal ipv6 9:1:1::100
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv6 2001:DB8::/48
parameter-map type webauth test
type webauth
redirect for-login http://9:1:1::100/login.html
redirect portal ipv6 9:1:1::100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

Example: Assigning Login, Login Failure, and Logout Pages per WLAN

This example shows how to assign login, login failure and logout pages per WLAN.

```
Device# configure terminal
Device(config)# parameter-map type webauth test
Device(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
Device(config-params-parameter-map)# custom-page login expired device flash:loginexpire.html
Device(config-params-parameter-map)# custom-page failure device flash:loginfail.html
Device(config-params-parameter-map)# custom-page success device flash:loginsucess.html
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 9.1.0.100
 custom-page login device flash:loginsantosh.html
 custom-page success device flash:loginsucess.html
 custom-page failure device flash:loginfail.html
 custom-page login expired device flash:loginexpire.html
```

Example: Configuring Preauthentication ACL

This example shows how to configure preauthentication ACL.

```
Device# configure terminal
Device(config)# wlan fff
Device(config-wlan)# shutdown
Device(config-wlan)# ip access-group web preauthrule
Device(config-wlan)# no shutdown
```

```
Device(config-wlan)# end
Device# show wlan name fff
```

Example: Configuring Webpassthrough

This example shows how to configure webpassthrough.

```
Device# configure terminal
Device(config)# parameter-map type webauth webparalocal
Device(config-params-parameter-map)# type consent
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 9.1.0.100
```

Verifying Web Authentication Type

To verify the web authentication type, run the following command:

```
Device# show parameter-map type webauth all
Type Name
---------------------------------
Global global
Named webauth
Named ext
Named redirect
Named abc
Named glbal
Named ewa-2
```

```
Device# show parameter-map type webauth global
Parameter Map Name : global
Banner:
Text : CisCo
Type : webauth
Auth-proxy Init State time : 120 sec
Webauth max-http connection : 100
Webauth logout-window : Enabled
Webauth success-window : Enabled
Consent Email : Disabled
Sleeping-Client : Enabled
Sleeping-Client timeout : 60 min
Virtual-ipv4 : 192.0.2.1.
Virtual-ipv4 hostname :
Webauth intercept https : Disabled
Webauth Captive Bypass : Disabled
Webauth bypass intercept ACL :
Trustpoint name :
HTTP Port : 80
Watch-list:
Enabled : no
Webauth login-auth-bypass:
```

```
Device# show parameter-map type webauth name global
Parameter Map Name : global
Type : webauth
Auth-proxy Init State time : 120 sec
Webauth max-http connection : 100
Webauth logout-window : Enabled
```

```
Webauth success-window : Enabled
Consent Email : Disabled
Sleeping-Client : Disabled
Webauth login-auth-bypass:
```

External Web Authentication (EWA)

Configuring EWA with Single WebAuth Server Address and Default Ports (80/443) (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa authentication login** **Example:** `Device(config)# aaa authentication login WEBAUTH local`	Defines the authentication method at login.
Step 3	**parameter-map type webauth** *parameter-map-name* **Example:** `Device(config)# parameter-map type webauth ISE-Ext-Webauth_IP`	Creates the parameter map. The *parameter-map-name* must not exceed 99 characters.
Step 4	**type webauth** **Example:** `Device(config-params-parameter-map)# type webauth`	Configures the webauth type parameter.
Step 5	**redirect for-login** *URL-String* **Example:** `Device(config-params-parameter-map)# redirect for-login https://192.168.0.98:443/portal/PortalSetup.action?portal=a64b62-108-11e7-8591-0050569b152`	Configures the URL string for redirect during login.
Step 6	**redirect portal ipv4** *ip-address* **Example:** `Device(config-params-parameter-map)# redirect portal ipv4 192.168.0.98`	Configures the external portal IPv4 address.
Step 7	**exit** **Example:**	Returns to global configuration mode.

	Command or Action	Purpose
	`Device(config-params-parameter-map)# exit`	
Step 8	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)#  wlan EWLC3-GUEST 3 EWLC3-GUEST`	Configures a WLAN.
Step 9	**no security ft adaptive** **Example:** `Device(config-wlan)# no security ft adaptive`	Disables adaptive 11r.
Step 10	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 11	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 12	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 13	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 14	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables web authentication for WLAN.
Step 15	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list WEBAUTH`	Enables authentication list for dot1x security.
Step 16	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map ISE-Ext-Webauth_IP`	Configures the parameter map. **Note** If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.

	Command or Action	Purpose
Step 17	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Configuring EWA with Multiple Web Servers and/or Ports Different than Default (80/443)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended** *name* **Example:** `Device(config)# ip access-list extended preauth_ISE_Ext_WA`	Defines an extended IPv4 access list using a name, and enters access-list configuration mode.
Step 3	*access-list-number* **permit tcp any host** *external_web_server_ip_address1* **eq** *port-number* **Example:** `Device(config)# 10 permit tcp any host 192.168.0.98 eq 8443`	Permits access from any host to the external web server port number 8443.
Step 4	*access-list-number* **permit tcp any host** *external_web_server_ip_address2* **eq** *port-number* **Example:** `Device(config)# 10 permit tcp any host 192.168.0.99 eq 8443`	Permits access from any host to the external web server port number 8443.
Step 5	*access-list-number* **permit udp any any eq domain** **Example:** `Device(config)# 20 permit udp any any eq domain`	Permits DNS UDP traffic.
Step 6	*access-list-number* **permit udp any any eq bootpc** **Example:** `Device(config)# 30 permit udp any any eq bootpc`	Permits DHCP traffic.

	Command or Action	Purpose
Step 7	*access-list-number* **permit udp any any eq bootps** **Example:** `Device(config)# 40 permit udp any any eq bootps`	Permits DHCP traffic.
Step 8	*access-list-number* **permit tcp host** *external_web_server_ip_address1* **eq** *port_number* **any** **Example:** `Device(config)# 50 permit tcp host 192.168.0.98 eq 8443 any`	Permits the access from the external web server port 8443 to any host.
Step 9	*access-list-number* **permit tcp host** *external_web_server_ip_address2* **eq** *port_number* **any** **Example:** `Device(config)# 50 permit tcp host 192.168.0.99 eq 8443 any`	Permits the access from the external web server port 8443 to any host.
Step 10	*access-list-number* **permit tcp any any eq domain** **Example:** `Device(config)# 60 permit tcp any any eq domain`	Permits the DNS TCP traffic.
Step 11	*access-list-number* **deny ip any any** **Example:** `Device(config)# 70 deny ip any any`	Denies all the other traffic.
Step 12	**wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# wlan EWLC3-GUEST 3 EWLC3-GUEST`	Creates the WLAN.
Step 13	**ip access-group web** *name* **Example:** `Device(config-wlan)# ip access-group web preauth_ISE_Ext_WA`	Configures the IPv4 WLAN web ACL. The variable *name* specifies the user-defined IPv4 ACL name.
Step 14	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Configuring Wired Guest EWA with Multiple Web Servers and/or Ports Different than Default (80/443)

Before you begin

You cannot assign a manual ACL to a wired guest LAN configuration. The workaround is to use the bypass ACL in the global parameter map.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended** *name* **Example:** `Device(config)# ip access-list extended BYPASS_ACL`	Defines an extended IPv4 access list using a name, and enters access-list configuration mode.
Step 3	*access-list-number* **deny ip any host** *hostname* **Example:** `Device(config)# 10 deny ip any host 192.168.0.45`	Allows the traffic to switch centrally.
Step 4	*access-list-number* **deny ip any host** *hostname* **Example:** `Device(config)# 20 deny ip any host 4.0.0.1`	Allows the traffic to switch centrally.
Step 5	**parameter-map type webauth global** **Example:** `Device(config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 6	**webauth-bypass-intercept** *name* **Example:** `Device(config-params-parameter-map)# webauth-bypass-intercept BYPASS_ACL`	Creates a WebAuth bypass intercept using the ACL name. **Note** You cannot apply a manual ACL to the wired guest profile and configure an external web authentication with multiple IP addresses or different ports. The workaround is to use the bypass ACL for wired guest profile.
Step 7	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-params-parameter-map)# end`	

Authentication for Sleeping Clients

Information About Authenticating 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 sleeping clients should be remembered for before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes, with the default being 720 minutes. You can also configure this duration on WebAuth parameter map that is mapped to a WLAN. Note that the sleeping client timer comes into effect due to instances such as idle timeout, session timeout, disabling of the WLAN, and the AP being nonoperational.

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.

Mobility Scenarios

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.

A sleeping client does not require reauthentication in the following scenarios:

- Suppose there are two controller s 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 controller s 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.

Restrictions on Authenticating Sleeping Clients

- The sleep client feature works only for WLAN configured with WebAuth security.
- You can configure the sleeping clients only on a per WebAuth parameter-map basis.

- The authentication of sleeping clients feature is supported only on WLANs that have Layer 3 security enabled.
- With Layer 3 security, the Authentication, Passthrough, and On MAC Filter failure web policies are supported. The Conditional Web Redirect and Splash Page Web Redirect web policies are not supported.
- The central web authentication of sleeping clients is not supported.
- The authentication of sleeping clients feature is not supported on guest LANs and remote LANs.
- A guest access sleeping client that has a local user policy is not supported. In this case, the WLAN-specific timer is applied.

Configuring Authentication for Sleeping Clients (GUI)

Procedure

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

Step 2 In the **Webauth Parameter Map** tab, click the parameter map name. The **Edit WebAuth Parameter** window is displayed.

Step 3 Select **Sleeping Client Status** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Authentication for Sleeping Clients (CLI)

Procedure

	Command or Action	Purpose
Step 1	**[no] parameter-map type webauth** {*parameter-map-name* | **global**} **Example:** `Device(config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 2	**sleeping-client** [**timeout** *time*] **Example:** `Device(config-params-parameter-map)# sleeping-client timeout 100`	Configures the sleeping client timeout to 100 minutes. Valid range is between 10 minutes and 43200 minutes. **Note** If you do not use the timeout keyword, the sleeping client is configured with the default timeout value of 720 minutes.
Step 3	**end**	Exits parameter-map webauth configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 4	(Optional) **show wireless client sleeping-client** **Example:** `Device# show wireless client sleeping-client`	Shows the MAC address of the clients and the time remaining in their respective sessions.
Step 5	(Optional) **clear wireless client sleeping-client** [**mac-address** *mac-addr*] **Example:** `Device# clear wireless client sleeping-client mac-address 00e1.e1e1.0001`	• **clear wireless client sleeping-client**—Deletes all sleeping client entries from the sleeping client cache. • **clear wireless client sleeping-client mac-address** *mac-addr*—Deletes the specific MAC entry from the sleeping client cache.

CHAPTER 67

Central Web Authentication

- Information About Central Web Authentication, on page 581
- How to Configure ISE, on page 582
- How to Configure Central Web Authentication on the Controller, on page 584
- Authentication for Sleeping Clients, on page 591

Information About Central Web Authentication

Central web authentication offers the possibility to have a central device that acts as a web portal (in this example, the ISE). The major difference compared to the usual local web authentication is that it is shifted to Layer 2 along with MAC filtering or dot1x authentication. The concept also differs in that the radius server (ISE in this example) returns special attributes that indicate to the switch that a web redirection must occur. This solution eliminates any delay to start the web authentication.

The following are the different types of web authentication methods:

- Local Web Authentication (LWA): Configured as Layer 3 security on the controller, the web authentication page and the pre-authentication ACL are locally configured on the controller. The controller intercepts htttp(s) traffic and redirects the client to the internal web page for authentication. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server.
- External Web Authentication (EWA): Configured as Layer 3 security on the controller, the controller intercepts htttp(s) traffic and redirects the client to the login page hosted on the external web server. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server. The pre-authentication ACL is configured statically on the controller.
- Central Web Authentication (CWA): Configured mostly as Layer 2 security on the controller, the redirection URL and the pre-authentication ACL reside on ISE and are pushed during layer 2 authentication to the controller. The controller redirects all web traffic from the client to the ISE login page. ISE validates the credentials entered by the client through HTTPS and authenticates the user.

Globally, if the MAC address of the client station is not known by the radius server (but other criteria can also be used), the server returns the redirection attributes, and the controller authorizes the station (using the MAC filtering) but places an access list to redirect the web traffic to the portal.

Once the user logs into the guest portal, it is possible to re-authenticate the client so that a new Layer 2 MAC filtering occurs using the Change of Authorization (CoA). This way, the ISE remembers that it was a webauth user and pushes the necessary authorization attributes to the controller for accessing the network.

Note In Central Web Authentication (CWA) with dual VLAN posture scenario, Cisco AireOS and IOS-XE controller performs 2 and 3 EAPOL handshakes respectively. If a client is stuck in a quarantine VLAN because of any break in EAPOL handshake due to client or network issue, you need to analyze the client or network issue.

However, you can manually disconnect or reconnect the client to come out of the quarantine loop (or) click the Scan Again on AnyConnect (Or) enable posture lease (Or) use the ISE posture sync feature.

Prerequisites for Central Web Authentication

- Cisco Identity Services Engine (ISE)

How to Configure ISE

To configure ISE, proceed as follows:

1. Create an authorization profile.
2. Create an authentication rule.
3. Create an authorization rule.

Creating an Authorization Profile

Procedure

Step 1 Click **Policy**, and click **Policy Elements**.

Step 2 Click **Results**.

Step 3 Expand **Authorization**, and click **Authorization Profiles**.

Step 4 Click **Add** to create a new authorization profile for central webauth.

Step 5 In the **Name** field, enter a name for the profile. For example, CentralWebauth.

Step 6 Choose **ACCESS_ACCEPT** from the Access Type drop-down list.

Step 7 Check the **Web Redirection (CWA, MDM, NSP, CPP)** check box, and choose **Centralized Web Auth** from the drop-down list.

Step 8 In the **ACL** field, enter the name of the ACL that defines the traffic to be redirected. For example, redirect.

Step 9 In the **Value** field, choose the default or customized values.

The Value attribute defines whether the ISE sees the default or a custom web portal that the ISE admin created.

Step 10 Click **Save**.

Creating an Authentication Rule

Follow the procedure given below to use the authentication profile and create the authentication rule:

Procedure

Step 1 In the **Policy** > **Authentication** page, click **Authentication**.

Step 2 Enter a name for your authentication rule. For example, MAB.

Step 3 In the If condition field, select the plus (+) icon.

Step 4 Choose **Compound condition**, and choose **Wireless_MAB**.

Step 5 Click the arrow located next to **and ...** in order to expand the rule further.

Step 6 Click the + icon in the Identity Source field, and choose **Internal endpoints**.

Step 7 Choose **Continue** from the 'If user not found' drop-down list.

This option allows a device to be authenticated even if its MAC address is not known.

Step 8 Click **Save**.

Creating an Authorization Rule

You can configure many rules in the authorization policy. The *MAC not known* rule is configured in this section:

Procedure

Step 1 Click **Policy** > **Authorization**.

Step 2 In the Rule Name field, enter a name. For example: *Mac not known*.

Step 3 In the Conditions field, click the plus (+) icon.

Step 4 Choose **Compound Conditions**, and choose **Wireless_MAB**.

Step 5 From the settings icon, select **Add Attribute/Value** from the options.

Step 6 In the Description field, choose **Network Access** > **AuthenticationStatus** as the attribute from the drop-down list.

Step 7 Choose the **Equals** operator.

Step 8 From the right-hand field, choose **UnknownUser**.

Step 9 In the Permissions field, choose the authorization profile name that you had created earlier.

The ISE continues even though the user (or MAC) is not known.

Unknown users are now presented with the Login page. However, once they enter their credentials, they are presented again with an authentication request on the ISE; therefore, another rule must be configured with a condition that is met if the user is a guest user. For example, if UseridentityGroup Equals Guest is used then it is assumed that all guests belong to this group.

Step 10 In the Conditions field, click the plus (+) icon.

Step 11 Choose **Compound Conditions**, and choose to create a new condition.

The new rule must come before the *MAC not known* rule.

Step 12 From the settings icon, select **Add Attribute/Value** from the options.

Step 13 In the Description field, choose **Network Access** > **UseCase** as the attribute from the drop-down list.

Step 14 Choose the **Equals** operator.

Step 15 From the right-hand field, choose **GuestFlow**.

Step 16 In the Permissions field, click the plus (+) icon to select a result for your rule.

You can choose **Standard** > **PermitAccess** option or create a custom profile to return the attributes that you like.

When the user is authorized on the login page, the ISE triggers a COA that results in the restart of Layer 2 authentication. When the user is identified as a guest user, the user is authorized.

How to Configure Central Web Authentication on the Controller

To configure central web authentication on the controller, proceed as follows:

1. Configure WLAN.
2. Configure policy profile.
3. Configure redirect ACL.
4. Configure AAA for central web authentication.
5. Configure redirect ACL in Flex profile.

Configuring WLAN (GUI)

Before you begin

You need to enable MAC filtering for Layer 2 authentication to download the redirect URL and ACL.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 In the **WLANs** window, click the name of the **WLAN** or click **Add** to create a new one.

Step 3 In the **Add/Edit WLAN** window that is displayed, click the **General** tab to configure the following parameters.

- In the **Profile Name** field, enter or edit the name of the profile.
- In the **SSID** field, enter or edit the SSID name.

  The SSID name can be alphanumeric, and up to 32 characters in length.
- In the **WLAN ID** field, enter or edit the ID number.The valid range is between 1 and 512.
- From the **Radio Policy** drop-down list, choose the **802.11** radio band.

- Using the **Broadcast SSID** toggle button, change the status to either **Enabled** or **Disabled** .
- Using the **Status** toggle button, change the status to either **Enabled** or **Disabled** .

Step 4 Click the **Security** tab, and then **Layer 2** tab to configre the following parameters:

- From the **Layer 2 Security Mode** drop-down list, choose **None**. .This setting disables Layer 2 security.
- Enter the **Reassociation Timeout** value, in seconds. This is the time after which a fast transition reassociation times out.
- Check the **Over the DS** check box to enable Fast Transition over a distributed system.
- Choose OWE, Opportunistic Wireless Encryption (OWE) provides data confidentiality with encryption over the air between an AP radio and a wireless client. OWE Transition Mode is meant to provide a sort of backwards compatibility.
- Choose Fast Transition, 802.11r which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with a new AP is done even before the corresponding client roams to the target access point. This concept is called Fast Transition.
- Check the check box to enable MAC filtering in the WLAN.

Step 5 Click **Save & Apply to Device**.

Configuring WLAN (CLI)

Note You need to enable MAC filtering for Layer 2 authentication to download the redirect URL and ACL.

After completing the WLAN configuration, if the changes are not pushed to all the APs, the following syslog message appears:

2021/01/06 16:20:00.597927186 {wncd_x_R0-4}{1}: [wlanmgr-db] [20583]: UUID: 0, ra: 0, TID: 0 (note): Unable to push WLAN config changes to all APs, cleanup required for WlanId: 2, profile: wlan1 state: Delete pending

If the above mentioned syslog message appears for more than six minutes, reload the controller.

If the controller does not reload and still the syslog message appears, then collect the archive logs, wncd core file, and raise a case by clicking the following link: Support Case Manager.

Procedure

	Command or Action	Purpose
Step 1	**wlan `wlan-name wlan-id SSID-name`** **Example:** `Device(config)# wlan wlanProfileName 1 ngwcSSID`	Enters the WLAN configuration sub-mode. **wlan-name** is the name of the configured WLAN. **wlan-id** is the wireless LAN identifier. The range is 1 to 512.

	Command or Action	Purpose
		SSID-name is the SSID name which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan wlan-name** command.
Step 2	**mac-filtering** [*name*] **Example:** `Device(config-wlan)# mac-filtering name`	Enables MAC filtering on a WLAN. **Note** While configuring mac-filtering the default authentication list is considered, if the authentication list is not configured earlier.
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disable WPA security.
Step 4	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 5	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Example

```
Device# config terminal
Device(config)# wlan wlanProfileName 1 ngwcSSID
Device(config-wlan)# mac-filtering default
Device(config-wlan)# no security wpa
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

Configuring Policy Profile (CLI)

Note You need a AAA override to apply policies coming from the AAA or ISE servers. When a redirect URL and redirect ACL is received from the ISE server, NAC is used to trigger the Central Web Authentication (CWA).

Both NAC and AAA override must be available in the policy profile to which the client is being associated.

The default policy profile is associated to an AP, if the AP is not associated to any other policy profiles.

Procedure

	Command or Action	Purpose
Step 1	**wireless profile policy default-policy-profile** **Example:** `Device(config)# wireless profile policy default-policy-profile`	Sets the policy profile.
Step 2	**vlan `vlan-id`** **Example:** `Device(config-wireless-policy)# vlan 41`	Maps the VLAN to a policy profile. If vlan-id is not specified, the default native vlan 1 is applied. The valid range for vlan-id is 1 to 4096. Management VLAN is applied if no VLAN is configured on the policy profile.
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Configures AAA override to apply policies coming from the AAA or ISE servers.
Step 4	**nac** **Example:** `Device(config-wireless-policy)# nac`	Configures Network Access Control in the policy profile. NAC is used to trigger the Central Web Authentication (CWA).
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the WLAN.
Step 6	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.

Example

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# vlan 41
Device(config-wireless-policy)# aaa-override
Device(config-wireless-policy)# nac
Device(config-wireless-policy)# no shutdown
Device(config-wireless-policy)# end
```

Configuring a Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, click **Add**.

Step 3 In the **Add Policy Profile** window, in General Tab, enter a name and description for the policy profile.

Step 4 To enable the policy profile, set **Status** as Enabled.

Step 5 Use the slider to enable or disable **Passive Client** and **Encrypted Traffic Analytics**.

Step 6 (Optional) In the **CTS Policy** section, choose the appropriate status for the following:

- Inline Tagging—a transport mechanism using which a controller embedded wireless controller or access point understands the source SGT.
- SGACL Enforcement

Step 7 Specify a default **SGT**. The valid range is from 2 to 65519.

Step 8 In the WLAN Switching Policy section, choose the following, as required:

- Central Switching
- Central Authentication
- Central DHCP
- Central Association Enable
- Flex NAT/PAT

Step 9 Click **Save & Apply to Device**.

Creating Redirect ACL

The redirect ACL is a punt ACL that needs to be predefined on the controller (or the AP in case of FlexConnect local switching): the AAA server returns the name of the ACL and not its definition. The redirect ACL defines traffic (matching “deny”statements, as it denies redirection for it) that will be allowed through on the data plane and traffic (matching “permit” statements) that will be sent to the control plane towards the CPU for further processing (that is, the web interception and redirection in this case). The ACL has implicit (that is, the invisible) statements allowing DHCP and DNS traffic towards all IPs, just like it is the case with LWA. It also ends with a statement that a security ACL implicit deny.

Procedure

	Command or Action	Purpose
Step 1	**ip access-list extended redirect** **Example:**	The HTTP and HTTPS browsing does not work without authentication (per the other ACL) as

	Command or Action	Purpose
	`Device(config)# ip access-list extended redirect`	ISE is configured to use a redirect ACL (named **`redirect`**).
Step 2	**deny ip any host `ISE-IP-add`** **Example:** `Device(config)# deny ip any host 123.123.134.112`	Allows traffic to ISE and all other traffic is blocked.
Step 3	**deny ip host `ISE-IP-add` any** **Example:** `Device(config)# deny ip host 123.123.134.112 any`	Allows traffic to ISE and all other traffic is blocked. **Note** This ACL is applicable for both local and flex mode.

Step 4	**permit TCP any any eq `web address/port-number`**
	Example:
	In case of HTTP:
	`Device(config)# permit TCP any any eq www`
	`Device(config)# permit TCP any any eq 80`
	Example:
	In case of HTTPS:
	`Device(config)# permit TCP any any eq 443`
		Redirects all HTTP or HTTPS access to the ISE login page. port-number 80 is used for HTTP and port-number 443 is used for HTTPS.
		For the ACE to allow traffic to ISE, ISE should be configured above the HTTP/HTTPS ACE.

Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring AAA for Central Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Configures the Change of Authorization (CoA) on the controller.
Step 2	**client `ISE-IP-add` server-key `radius-shared-secret`** **Example:**	Specifies a RADIUS client and the RADIUS key to be shared between a device and a RADIUS client.

	Command or Action	Purpose
	`Device(config-locsvr-da-radius)# client 123.123.134.112 server-key 0 SECRET`	**ISE-IP-add** is the IP address of the RADIUS client. **server-key** is the radius client server-key. **radius-shared-secret** covers the following: • **0**—Specifies unencrypted key. • **6**—Specifies encrypted key. • **7**—Specifies HIDDEN key. • **Word**—Unencrypted (cleartext) server key. The RADIUS shared secret should not exceed 240 characters while configuring WSMA data in GUI. **Note** All these steps work only if the AAA configuration is in place. See the *Configuring AAA Authentication* for details.

Example

```
Device# config terminal
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 123.123.134.112 server-key 0 SECRET
Device(config-locsvr-da-radius)# end
```

Configuring Redirect ACL in Flex Profile (GUI)

The redirect ACL definition must be sent to the access point in the FlexConnect profile. For this, the redirect ACL associated with an AP must be configured in the FlexConnect profile where the client is hosted. If an access point is not configured with any of the FlexConnect profiles, the default FlexConnect profile is associated with it.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 On the **Flex Profile** page, click the name of the FlexConnect profile or click **Add** to create a new FlexConnect profile.

Step 3 In the **Add/Edit Flex Profile** window that is displayed, click the **Policy ACL** tab.

Step 4 Click **Add** to map an ACL to the FlexConnect profile.

Step 5 Choose the ACL name, enable central web authentication, and specify the preauthentication URL filter.

Step 6 Click **Save**.

Step 7 Click **Update & Apply to Device**.

Configuring Redirect ACL in Flex Profile (CLI)

The redirect ACL definition must be sent to the access point in the Flex profile. For this, the redirect ACL associated to an AP must be configured in the Flex profile where the client is being hosted. If an access point is not configured with any of the Flex profiles, the default Flex profile is associated with it.

Procedure

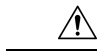
	Command or Action	Purpose
Step 1	**wireless profile flex default-flex-profile** **Example:** `Device(config)# wireless profile flex default-flex-profile`	Creates a new flex policy. The default flex profile name is **`default-flex-profile`**.
Step 2	**acl-policy** *acl policy name* **Example:** `Device(config-wireless-flex-profile)# acl-policy acl1`	Configures ACL policy.
Step 3	**central-webauth** **Example:** `Device(config-wireless-flex-profile-acl)# central-webauth`	Configures central web authentication.
Step 4	**end** **Example:** `Device(config-wireless-flex-profile-acl)# end`	Returns to privileged EXEC mode.

Authentication for Sleeping Clients

Information About Authenticating 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 sleeping clients should be remembered for before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes, with the default being 720 minutes. You can also configure this duration on WebAuth parameter map that is mapped to a WLAN. Note that the sleeping client timer comes into effect due to instances such as idle timeout, session timeout, disabling of the WLAN, and the AP being nonoperational.

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.

Mobility Scenarios

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.

A sleeping client does not require reauthentication in the following scenarios:

- Suppose there are two controller s 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 controller s 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.

Restrictions on Authenticating Sleeping Clients

- The sleep client feature works only for WLAN configured with WebAuth security.
- You can configure the sleeping clients only on a per WebAuth parameter-map basis.
- The authentication of sleeping clients feature is supported only on WLANs that have Layer 3 security enabled.
- With Layer 3 security, the Authentication, Passthrough, and On MAC Filter failure web policies are supported. The Conditional Web Redirect and Splash Page Web Redirect web policies are not supported.
- The central web authentication of sleeping clients is not supported.
- The authentication of sleeping clients feature is not supported on guest LANs and remote LANs.
- A guest access sleeping client that has a local user policy is not supported. In this case, the WLAN-specific timer is applied.

Configuring Authentication for Sleeping Clients (GUI)

Procedure

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

Step 2 In the **Webauth Parameter Map** tab, click the parameter map name. The **Edit WebAuth Parameter** window is displayed.

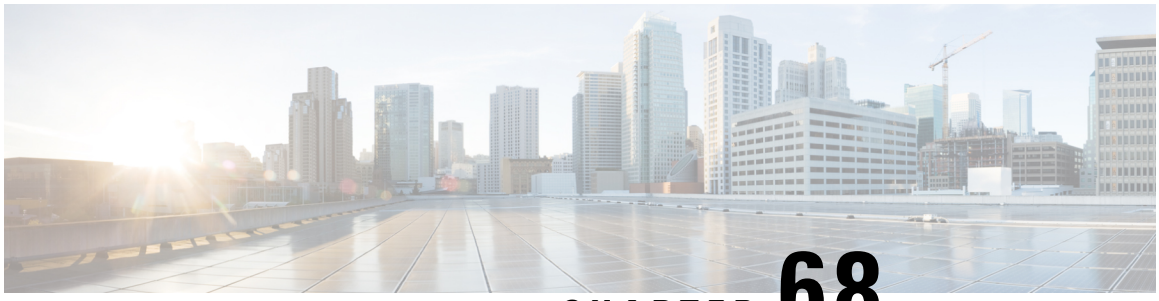
Step 3 Select **Sleeping Client Status** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Authentication for Sleeping Clients (CLI)

Procedure

	Command or Action	Purpose
Step 1	**[no] parameter-map type webauth** {*parameter-map-name* | **global**} **Example:** `Device(config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 2	**sleeping-client** [**timeout** *time*] **Example:** `Device(config-params-parameter-map)# sleeping-client timeout 100`	Configures the sleeping client timeout to 100 minutes. Valid range is between 10 minutes and 43200 minutes. **Note** If you do not use the timeout keyword, the sleeping client is configured with the default timeout value of 720 minutes.
Step 3	**end**	Exits parameter-map webauth configuration mode and returns to privileged EXEC mode.
Step 4	(Optional) **show wireless client sleeping-client** **Example:** `Device# show wireless client sleeping-client`	Shows the MAC address of the clients and the time remaining in their respective sessions.
Step 5	(Optional) **clear wireless client sleeping-client** [**mac-address** *mac-addr*] **Example:** `Device# clear wireless client sleeping-client mac-address 00e1.e1e1.0001`	• **clear wireless client sleeping-client**—Deletes all sleeping client entries from the sleeping client cache. • **clear wireless client sleeping-client mac-address** *mac-addr*—Deletes the specific MAC entry from the sleeping client cache.



CHAPTER 68

ISE Simplification and Enhancements

- Utilities for Configuring Security, on page 595
- Configuring Captive Portal Bypassing for Local and Central Web Authentication, on page 597
- Sending DHCP Options 55 and 77 to ISE, on page 600
- Captive Portal, on page 603

Utilities for Configuring Security

This chapter describes how to configure all the RADIUS server side configuration using the following command:

wireless-default radius server *ip* **key** *secret*

This simplified configuration option provides the following:

- Configures AAA authorization for network services, authentication for web auth and Dot1x.
- Enables local authentication with default authorization.
- Configures the default redirect ACL for CWA.
- Creates global parameter map with virtual IP and enables captive bypass portal.
- Configures all the AAA configuration for a default case while configuring the RADIUS server.
- The method-list configuration is assumed by default on the WLAN.
- Enables the radius accounting by default.
- Disables the radius aggressive failovers by default.
- Sets the radius request timeouts to 5 seconds by default.
- Enables captive bypass portal.

This command configures the following in the background:

```
aaa new-model
aaa authentication webauth default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting identity default start-stop group radius
!
aaa server radius dynamic-author
```

```
 client <IP> server-key cisco123
!
radius server RAD_SRV_DEF_<IP>
 description Configured by wireless-default
 address ipv4 <IP> auth-port 1812 acct-port 1813
 key <key>
!
aaa local authentication default authorization default
aaa session-id common
!
ip access-list extended CISCO-CWA-URL-REDIRECT-ACL-DEFAULT
remark " CWA ACL to be referenced from ISE "
deny udp any any eq domain
deny tcp any any eq domain
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny ip any host <IP>
permit tcp any any eq www
!
parameter-map type webauth global
  captive-bypass-portal
  virtual-ip ipv4 192.0.2.1
  virtual-ip ipv6 1001::1
!
wireless profile policy default-policy-profile
   aaa-override
   local-http-profiling
   local-dhcp-profiling
   accounting
```

Thus, you need not go through the entire Configuration Guide to configure wireless controller for a simple configuration requirement.

Configuring Multiple Radius Servers

Use the following procedure to configure a RADIUS server.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless-default radius server** *ip* **key** *secret* **Example:** `Device(config)# wireless-default radius server 9.2.58.90 key cisco123`	Configures a radius server. **Note** You can configure up to ten RADIUS servers.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying AAA and Radius Server Configurations

To view details of AAA server, use the following command:

```
Device# show run aaa
!
aaa new-model
aaa authentication webauth default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting Identity default start-stop group radius
!
aaa server radius dynamic-author
 client 9.2.58.90 server-key cisco123
!
radius server RAD_SRV_DEF_9.2.58.90
 description Configured by wireless-default
 address ipv4 9.2.58.90 auth-port 1812 acct-port 1813
 key cisco123
!
aaa local authentication default authorization default
aaa session-id common
!
!
ip access-list extended CISCO-CWA-URL-REDIRECT-ACL-DEFAULT
remark " CWA ACL to be referenced from ISE "
deny udp any any eq domain
deny tcp any any eq domain
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny ip any host 9.2.58.90
permit tcp any any eq www
!
parameter-map type webauth global
  captive-bypass-portal
  virtual-ip ipv4 192.0.2.1
  virtual-ip ipv6 1001::1
!
wireless profile policy default-policy-profile
   aaa-override
   local-http-profiling
   local-dhcp-profiling
   accounting
```

Note The **show run aaa** output may change when new commands are added to this utility.

Configuring Captive Portal Bypassing for Local and Central Web Authentication

Information About Captive Bypassing

WISPr is a draft protocol that enables users to roam between different wireless service providers. Some devices (For example, Apple iOS devices) have a mechanism using which they can determine if the device is connected

to Internet, based on an HTTP WISPr request made to a designated URL. This mechanism is used for the device to automatically open a web browser when a direct connection to the internet is not possible. This enables the user to provide his credentials to access the internet. The actual authentication is done in the background every time the device connects to a new SSID.

The client device (Apple iOS device) sends a WISPr request to the controller , which checks for the user agent details and then triggers an HTTP request with a web authentication interception in the controller . After verification of the iOS version and the browser details provided by the user agent, the controller allows the client to bypass the captive portal settings and provides access to the Internet.

This HTTP request triggers a web authentication interception in the controller as any other page requests are performed by a wireless client. This interception leads to a web authentication process, which will be completed normally. If the web authentication is being used with any of the controller splash page features (URL provided by a configured RADIUS server), the splash page may never be displayed because the WISPr requests are made at very short intervals, and as soon as one of the queries is able to reach the designated server, any web redirection or splash page display process that is performed in the background is cancelled, and the device processes the page request, thus breaking the splash page functionality.

For example, Apple introduced an iOS feature to facilitate network access when captive portals are present. This feature detects the presence of a captive portal by sending a web request on connecting to a wireless network. This request is directed to http://www.apple.com/library/test/success.html for Apple iOS version 6 and older, and to several possible target URLs for Apple iOS version 7 and later. If a response is received, then the Internet access is assumed to be available and no further interaction is required. If no response is received, then the Internet access is assumed to be blocked by the captive portal and Apple's Captive Network Assistant (CNA) auto-launches the pseudo-browser to request portal login in a controlled window. The CNA may break when redirecting to an ISE captive portal. The controller prevents this pseudo-browser from popping up.

You can now configure the controller to bypass WISPr detection process, so the web authentication interception is only done when a user requests a web page leading to splash page load in user context, without the WISPr detection being performed in the background.

Configuring Captive Bypassing for WLAN in LWA and CWA (GUI)

Procedure

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

Step 2 In the **Webauth Parameter Map** tab, click the parameter map name. The **Edit WebAuth Parameter** window is displayed.

Step 3 Select **Captive Bypass Portal** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Captive Bypassing for WLAN in LWA and CWA (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** *parameter-map-name* **Example:** `Device(config)# parameter-map type webauth WLAN1_MAP`	Creates the parameter map. The *parameter-map-name* must not exceed 99 characters.
Step 3	**captive-bypass-portal** **Example:** `Device(config)# captive-bypass-portal`	Configures captive bypassing.
Step 4	**wlan** *profile-name wlan-id ssid-name* **Example:** `Device(config)# wlan WLAN1_NAME 4 WLAN1_NAME`	Specifies the WLAN name and ID. • *profile-name* is the WLAN name which can contain 32 alphanumeric characters. • *wlan-id* is the wireless LAN identifier. The valid range is from 1 to 512. • *ssid-name* is the SSID which can contain 32 alphanumeric characters.
Step 5	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables the web authentication for the WLAN.
Step 6	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	Maps the parameter map. **Note** If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 7	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Sending DHCP Options 55 and 77 to ISE

Information about DHCP Option 55 and 77

The DHCP sensors use the following DHCP options on the ISE for native and remote profiling:

- **Option 12**: Hostname
- **Option 6**: Class Identifier

Along with this, the following options needs to be sent to the ISE for profiling:

- **Option 55**: Parameter Request List
- **Option 77**: User Class

Configuration to Send DHCP Options 55 and 77 to ISE (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the**Policy Profile** page, click **Add** to view the **Add Policy Profile** window.

Step 3 Click **Access Policies** tab, choose the **RADIUS Profiling** and **DHCP TLV Caching** check boxes to configure radius profiling and DHCP TLV Caching on a WLAN.

Step 4 Click **Save & Apply to Device**.

Configuration to Send DHCP Options 55 and 77 to ISE (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**dhcp-tlv-caching** **Example:**	Configures DHCP TLV caching on a WLAN.

	Command or Action	Purpose
	`Device(config-wireless-policy)# dhcp-tlv-caching`	
Step 4	**radius-profiling** **Example:** `Device(config-wireless-policy)# radius-profiling`	Configures client radius profiling on a WLAN.
Step 5	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring EAP Request Timeout (GUI)

Follow the steps given below to configure the EAP Request Timeout through the GUI:

Procedure

Step 1 Choose **Configuration** > **Security** > **Advanced EAP**.

Step 2 In the **EAP-Identity-Request Timeout** field, specify the amount of time (in seconds) in which the device attempts to send an EAP identity request to wireless clients using local EAP.

Step 3 In the **EAP-Identity-Request Max Retries** field, specify the maximum number of times that the device attempts to retransmit the EAP identity request to wireless clients using local EAP.

Step 4 Set **EAP Max-Login Ignore Identity Response** to **Enabled** state to limit the number of clients that can be connected to the device with the same username. You can log in up to eight times from different clients (PDA, laptop, IP phone, and so on) on the same device. The default state is **Disabled**.

Step 5 In the **EAP-Request Timeout** field, specify the amount of time (in seconds) in which the device attempts to send an EAP request to wireless clients using local EAP.

Step 6 In the **EAP-Request Max Retries** field, specify the maximum number of times that the device attempts to retransmit the EAP request to wireless clients using local EAP.

Step 7 In the **EAPOL-Key Timeout** field, specify the amount of time (in seconds) in which the device attempts to send an EAP key over the LAN to wireless clients using local EAP.

Step 8 In the **EAPOL-Key Max Retries** field, specify the maximum number of times that the device attempts to send an EAP key over the LAN to wireless clients using local EAP.

Step 9 In the **EAP-Broadcast Key Interval** field, specify the time interval between rotations of the broadcast encryption key used for clients and click **Apply**.

Note After configuring the EAP-Broadcast key interval to a new time period, you must shut down or restart the WLAN for the changes to take effect. Once the WLAN is shut down or restarted, the M5 and M6 packets are exchanged when the configured timer value expires.

Configuring EAP Request Timeout

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps client-exclusion dot1x-timeout** **Example:** `Device(config)# wireless wps client-exclusion dot1x-timeout`	Enables exclusion on timeout and no response. By default, this feature is enabled. To disable, append a **no** at the beginning of the command.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring EAP Request Timeout in Wireless Security (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless security dot1x request** {**retries** *0 - 20* | **timeout** *1 - 120*} **Example:** `Device(config)# wireless security dot1x request timeout 60`	Configures the EAP request retransmission timeout value in seconds.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Captive Portal

Captive Portal Configuration

This feature enables you to configure multiple web authentication URLs (including external captive URLs) for the same SSID based on an AP. The default setting is to use the Global URL for authentication. The override option is available at WLAN and AP level.

The order of precedence is:

- AP
- WLAN
- Global configuration

Restrictions for Captive Portal Configuration

- This configuration is supported in a standalone controller only.
- Export-Anchor configuration is not supported.

Configuring Captive Portal (GUI)

Procedure

Step 1	Choose **Configuration** > **Tags & Profiles** > **WLANs**.
Step 2	Click **Add**.
Step 3	In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.
Step 4	In the **Security** > **Layer2** tab, uncheck the **WPA Policy**, **AES** and **802.1x** check boxes.
Step 5	In the **Security** > **Layer3** tab, choose the parameter map from the **Web Auth Parameter Map** drop-down list and authentication list from the **Authentication List** drop-down list.
Step 6	In the **Security** >**AAA** tab, choose the Authentication list from the **Authentication List** drop-down list.
Step 7	Click **Apply to Device**.
Step 8	Choose **Configuration** > **Security** > **Web Auth**.
Step 9	Choose a **Web Auth Parameter Map**.
Step 10	In the **General** tab, enter the **Maximum HTTP connections**, **Init-State Timeout(secs)** and choose **webauth** from the **Type** drop-down list.
Step 11	In the **Advanced** tab, under the **Redirect to external server** settings, enter the **Redirect for log-in** server.
Step 12	Click **Update & Apply**.

Configuring Captive Portal

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** {*profile-name* | **shutdown**} *network-name* **Example:** `Device(config)# wlan edc6 6 edc`	Configures the WLAN profile. Enables or Disables all WLANs and creates the WLAN identifier. The profile-name and the SSID network name should be up to 32 alphanumeric charcters.
Step 3	**ip** {**access-group** | **verify**} **web** *IPv4-ACL-Name* **Example:** `Device(config-wlan)# ip access-group web CPWebauth`	Configures the WLAN web ACL. **Note** WLAN needs to be disabled before performing this operation.
Step 4	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.

Step 7	**security web-auth** {**authentication-list** *authentication-list-name* | **authorization-list** *authorization-list-name* | **on-macfilter-failure** | **parameter-map** *parameter-map-name*}
	Example:
	`Device(config-wlan)# security web-auth authentication-list cp-webauth`
	`Device(config-wlan)# security web-auth parameter-map parMap6`
		Enables web authentication for WLAN. Here,
		• **authentication-list**
		authentication-list-name: Sets the authentication list for IEEE 802.1x.
		• **authorization-list**
		authorization-list-name: Sets the override-authorization list for IEEE 802.1x.
		• **on-macfilter-failure**: Enables Web authentication on MAC filter failure.

	Command or Action	Purpose
		• **parameter-map** *parameter-map-name*: Configures the parameter map. **Note** When **security web-auth** is enabled, you get to map the default **authentication-list** and global **parameter-map**. This is applicable for authentication-list and parameter-map that are not explicitly mentioned.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 9	**exit** **Example:** `Device(config-wlan)# exit`	Exits from the WLAN configuration.
Step 10	**parameter-map type webauth** *parameter-map-name* **Example:** `Device(config)# parameter-map type webauth parMap6`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 11	**parameter-map type webauth** *parameter-map-name* **Example:** `Device(config)# parameter-map type webauth parMap6`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 12	**type webauth** **Example:** `Device(config-params-parameter-map)# type webauth`	Configures the webauth type parameter.
Step 13	**timeout init-state sec** <*timeout-seconds*> **Example:** `Device(config-params-parameter-map)# timeout inti-state sec 3600`	Configures the WEBAUTH timeout in seconds. Valid range for the time in sec parameter is 60 seconds to 3932100 seconds.
Step 14	**redirect for-login** <*URL-String*> **Example:** `Device(config-params-parameter-map)# redirect for-login https://172.16.100.157/portal/login.html`	Configures the URL string for redirect during login.

	Command or Action	Purpose
Step 15	**exit** **Example:** `Device(config-params-parameter-map)# exit`	Exits the parameters configuration.
Step 16	**wireless tag policy** *policy-tag-name* **Example:** `Device(config)# wireless tag policy policy_tag_edc6`	Configures policy tag and enters policy tag configuration mode.
Step 17	**wlan** *wlan-profile-name* **policy** *policy-profile-name* **Example:** `Device(config-policy-tag)# wlan edc6 policy policy_profile_flex`	Attaches a policy profile to a WLAN profile.
Step 18	**end** **Example:** `Device(config-policy-tag)# end`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.

Captive Portal Configuration - Example

The following example shows how you can have APs at different locations, broadcasting the same SSID but redirecting clients to different redirect portals:

Configuring multiple parameter maps pointing to different redirect portal:

```
parameter-map type webauth parMap1
type webauth
timeout init-state sec 21600
redirect for-login
https://172.16.12.3:8080/portal/PortalSetup.action?portal=cfdbce00-2ce2-11e8-b83c-005056a06b27
redirect portal ipv4 172.16.12.3
!
!
parameter-map type webauth parMap11
type webauth
timeout init-state sec 21600
redirect for-login
https://172.16.12.4:8443/portal/PortalSetup.action?portal=094e7270-3808-11e8-9797-02421e4cae0c
redirect portal ipv4 172.16.12.4
!
```

Associating these parameter maps to different WLANs:

```
wlan edc1 1 edc
ip access-group web CPWebauth
no security wpa
no security wpa akm dot1x
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list cp-webauth
security web-auth parameter-map parMap11
```

```
no shutdown
wlan edc2 2 edc
ip access-group web CPWebauth
no security wpa
no security wpa akm dot1x
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list cp-webauth
security web-auth parameter-map parMap1
no shutdown
```

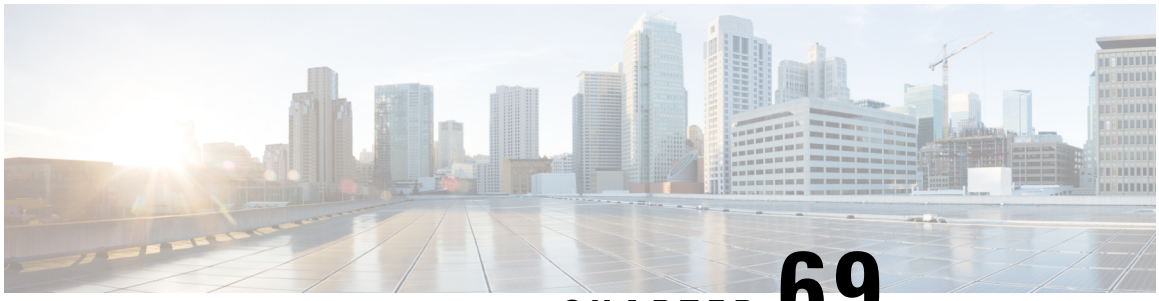
Note All WLANs have identical SSIDs.

Associating WLANs to different policy tags:

```
wireless tag policy policy_tag_edc1
wlan edc1 policy policy_profile_flex
wireless tag policy policy_tag_edc2
wlan edc2 policy policy_profile_flex
```

Assigning these policy tags to the desired APs:

```
ap E4AA.5D13.14DC
policy-tag policy_tag_edc1
site-tag site_tag_flex
ap E4AA.5D2C.3CAC
policy-tag policy_tag_edc2
site-tag site_tag_flex
```



CHAPTER 69

Authentication and Authorization Between Multiple RADIUS Servers

- Information About Authentication and Authorization Between Multiple RADIUS Servers, on page 609
- Configuring 802.1X Security for WLAN with Split Authentication and Authorization Servers, on page 610
- Configuring Web Authentication for WLAN with Split Authentication and Authorization Servers, on page 615
- Verifying Split Authentication and Authorization Configuration, on page 617
- Configuration Examples, on page 618

Information About Authentication and Authorization Between Multiple RADIUS Servers

Cisco Catalyst 9800 Series Wireless Controller uses the approach of request and response transaction with a single RADIUS server that combines both authentication and authorization. You can split the authentication and authorization on the controller between multiple RADIUS servers.

A RADIUS sever can assume the role of either an authentication server, authorization server, or both. In cases where there are disparate RADIUS servers for authentication and authorization, the Session Aware Networking (SANet) component on the controller now allows authentication on one server and authorization on another when a client joins the controller .

Authentication can be done using the Cisco ISE, Cisco Catalyst Center, Free RADIUS, or any third-party RADIUS Server. After successful authentication from an authentication server, the controller relays attributes received from the authentication server to another RADIUS sever designated as authorization server.

The authorization server then performs the following:

- Processes received attributes with the other policies or rules defined on the server.
- Derives attributes as part of the authorization response and returns it to the controller .

Note In a split authentication and authorization configuration, both servers must be available and must successfully authenticate and authorize with an ACCESS-ACCEPT for a session to be accepted by the controller .

Note A maximum of 100 entries is supported in the Authentication/Authorization list created through Cisco Catalyst Center provisioning. The entries beyond 100 do not work even though they can be created.

Configuring 802.1X Security for WLAN with Split Authentication and Authorization Servers

Configuring Explicit Authentication and Authorization Server List (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA**.

Step 2 On the **Authentication Authorization and Accounting** page, click the **Servers/Groups** tab.

Step 3 Click the type of AAA server you want to configure from the following options:

- RADIUS
- TACACS+
- LDAP

In this procedure, the RADIUS server configuration is described.

Step 4 With the **RADIUS** option selected, click **Add**.

Step 5 Enter a name for the RADIUS server and the IPv4 or IPV6 address of the server.

Step 6 Enter the authentication and encryption key to be used between the device and the key string RADIUS daemon running on the RADIUS server. You can choose to use either a PAC key or a non-PAC key.

Step 7 Enter the server timeout value; valid range is 1 to 1000 seconds.

Step 8 Enter a retry count; valid range is 0 to 100.

Step 9 Leave the **Support for CoA** field in **Enabled** state.

Step 10 Click **Save & Apply to Device**.

Step 11 On the **Authentication Authorization and Accounting** page, with **RADIUS** option selected, click the **Server Groups** tab.

Step 12 Click **Add**.

Step 13 In the **Create AAA RADIUS Server Group** window that is displayed, enter a name for the RADIUS server group.

Step 14 From the **MAC-Delimiter** drop-down list, choose the delimiter to be used in the MAC addresses that are sent to the RADIUS servers.

Step 15 From the **MAC Filtering** drop-down list, choose a value based on which to filter MAC addresses.

Step 16 To configure dead time for the server group and direct AAA traffic to alternative groups of servers that have different operational characteristics, in the **Dead-Time** field, enter the amount of time, in minutes, after which a server is assumed to be dead.

Step 17 Choose the servers that you want to include in the server group from the **Available Servers** list and move them to the **Assigned Servers** list.

Step 18 Click **Save & Apply to Device**.

Configuring Explicit Authentication Server List (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **Servers/Groups**.

Step 2 Choose **RADIUS** > **Servers** tab.

Step 3 Click **Add** to add a new server or click an existing server.

Step 4 Enter the **Name**, the **Server Address**, **Key**, **Confirm Key**, **Auth Port** and **Acct Port.** Check the **PAC Key** checkbox and enter the **PAC key** and **Confirm PAC Key**

Step 5 Click **Apply to Device**.

Step 6 Choose **RADIUS** > **Server Groups** and click **Add** to add a new server group or click an existing server group.

Step 7 Enter the **Name** of the server group and choose the servers that you want to include in the server group, from the **Available Servers** list and move them to the **Assigned Servers** list.

Step 8 Click **Apply to Device**.

Configuring Explicit Authentication Server List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server free-radius-authc-server`	Specifies the RADIUS server name.
Step 4	**address ipv4** *address* **auth-port** *auth_port_number* **acct-port** *acct_port_number* **Example:**	Specifies the RADIUS server parameters.

	Command or Action	Purpose
	`Device(config-radius-server)# address ipv4 9.2.62.56 auth-port 1812 acct-port 1813`	
Step 5	[**pac**] **key** *key* **Example:** `Device(config-radius-server)# key cisco`	Specify the authentication and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server.
Step 6	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to the configuration mode.
Step 7	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius authc-server-group`	Creates a radius server-group identification. *server-group* refers to the server group name. The valid range is from 1 to 32 alphanumeric characters. If the IP address of the RADIUS server is not added to the routes defined for the controller, the default route is used. We recommend that you define a specific route to source the traffic from the defined SVI in the AAA server group.
Step 8	**server name** *server-name* **Example:** `Device(config)# server name free-radius-authc-server`	Configures the server name.
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. For more information, see **Configuring AAA for External Authentication**.

Configuring Explicit Authorization Server List (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **Servers/Groups**.

Step 2 Choose **RADIUS** > **Servers** tab.

Step 3 Click **Add** to add a new server or click an existing server.

Step 4 Enter the **Name**, the **Server Address**, **Key**, **Confirm Key**, **Auth Port** and **Acct Port.** Check the **PAC Key** checkbox and enter the **PAC key** and **Confirm PAC Key**

Step 5 Click **Apply to Device**.

Step 6 Choose **RADIUS** > **Server Groups** and click **Add** to add a new server group or click an existing server group.

Step 7 Enter the **Name** of the server group and choose the servers that you want to include in the server group, from the **Available Servers** list and move them to the **Assigned Servers** list.

Step 8 Click **Apply to Device**.

Configuring Explicit Authorization Server List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server cisco-catalyst-center-authz-server`	Specifies the RADIUS server name.
Step 4	**address ipv4** *address* **auth-port** *auth_port_number* **acct-port** *acct_port_number* **Example:** `Device(config-radius-server)# address ipv4 9.4.62.32 auth-port 1812 acct-port 1813`	Specifies the RADIUS server parameters.
Step 5	[**pac**] **key** *key* **Example:** `Device(config-radius-server)# pac key cisco`	Specify the authorization and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server.
Step 6	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to the configuration mode.
Step 7	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius authz-server-group`	Creates a radius server-group identification.
Step 8	**server name** *server-name*	

	Command or Action	Purpose
	Example: `Device(config)# server name cisco-catalyst-center-authz-server`	
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Authentication and Authorization List for 802.1X Security (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.

Step 4 In the **Security** > **AAA** tab, choose the Authentication list from the **Authentication List** drop-down list.

Step 5 Click **Apply to Device**.

Configuring Authentication and Authorization List for 802.1X Security

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-foo 222 foo-ssid`	Enters WLAN configuration sub-mode. • *wlan-name*: Is the name of the configured WLAN. • *wlan-id*: Is the wireless LAN identifier. Range is from 1 to 512. • *SSID-name*: Is the SSID name which can contain 32 alphanumeric characters.

	Command or Action	Purpose
		Note If you have already configured this command, enter **wlan** *wlan-name* command.
Step 4	**security dot1x authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security dot1x authentication-list authc-server-group`	Enables authentication list for dot1x security.
Step 5	**security dot1x authorization-list** *authorize-list-name* **Example:** `Device(config-wlan)# security dot1x authorization-list authz-server-group`	Specifies authorization list for dot1x security. For more information on the **Cisco Digital Network Architecture Center (DNAC)**, see the **DNAC documentation**.
Step 6	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Web Authentication for WLAN with Split Authentication and Authorization Servers

Configuring Authentication and Authorization List for Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.

Step 4 In the **Security** > **Layer2** tab, uncheck the **WPAPolicy**, **AES** and **802.1x** check boxes.

Step 5 Check the **MAC Filtering** check box to enable the feature. With MAC Filtering enabled, choose the Authorization list from the **Authorization List** drop-down list.

Step 6 In the **Security** > **AAA** tab, choose the Authentication list from the **Authentication List** drop-down list.

Step 7 Click **Apply to Device**.

Configuring Authentication and Authorization List for Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-bar 1 bar-ssid`	Enters WLAN configuration sub-mode. • *wlan-name*: Is the name of the configured WLAN. • *wlan-id*: Is the wireless LAN identifier. • *SSID-name*: Is the SSID name which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *wlan-name* command.
Step 4	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 7	**security web-auth** {**authentication-list** *authenticate-list-name* | **authorization-list** *authorize-list-name*}	Enables authentication or authorization list for dot1x security.

	Command or Action	Purpose
	Example: `Device(config-wlan)# security web-auth authentication-list authc-server-group`	**Note** You get to view the following error, if you do not disable WPA security, AKM for dot1x, and WPA2 security: *% switch-1:dbm:wireless:web-auth cannot be enabled. Invalid WPA/WPA2 settings.*
Step 8	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Split Authentication and Authorization Configuration

To view the WLAN details, use the following command:

```
Device# show run wlan
wlan wlan-foo 2 foo-ssid
security dot1x authentication-list authc-server-group
security dot1x authorization-list authz-server-group

wlan wlan-bar 3 bar-ssid
security web-auth authentication-list authc-server-group
security web-auth authorization-list authz-server-group
```

To view the AAA authentication and server details, use the following command:

```
Device# show run aaa
!
aaa authentication dot1x default group radius
username cisco privilege 15 password 0 cisco
!
!
radius server free-radius-authc-server
 address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
 key cisco
!
radius server cisco-catalyst-center-authz-server
 address ipv4 9.4.62.32 auth-port 1812 acct-port 1813
 pac key cisco
!
!
aaa new-model
aaa session-id common
!
```

To view the authentication and authorization list for 802.1X security, use the following command:

```
Device# show wlan name wlan-foo | sec 802.1x
802.1x authentication list name               : authc-server-group
802.1x authorization list name                : authz-server-group
            802.1x                            : Enabled
```

To view the authentication and authorization list for web authentication, use the following command:

```
Device# show wlan name wlan-bar | sec Webauth
    Webauth On-mac-filter Failure             : Disabled
    Webauth Authentication List Name          : authc-server-group
    Webauth Authorization List Name           : authz-server-group
    Webauth Parameter Map                     : Disabled
```

Configuration Examples

Configuring Cisco Catalyst 9800 Series Wireless Controller for Authentication with a Third-Party RADIUS Server: Example

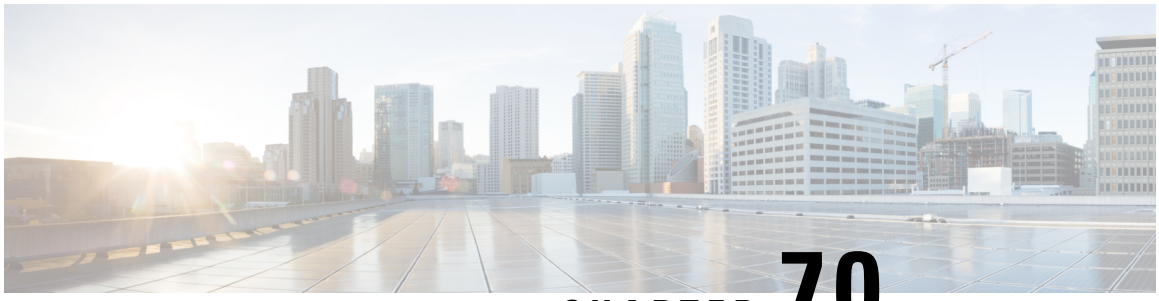
This example shows how to configure Cisco Catalyst 9800 Series Wireless Controller for authentication with a third-party RADIUS server:

```
Device(config)# radius server free-radius-authc-server
Device(config-radius-server)# address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
Device(config-radius-server)# key cisco
Device(config-radius-server)# exit
Device(config)# aaa group server radius authc-server-group
Device(config)# server name free-radius-authc-server
Device(config)# end
```

Configuring Cisco Catalyst 9800 Series Wireless Controller for Authorization with Cisco ISE or Cisco Catalyst Center: Example

This example shows how to configure Cisco Catalyst 9800 Series Wireless Controller for authorization with Cisco ISE or Cisco Catalyst Center:

```
Device(config)# radius server cisco-catalyst-center-authz-server
Device (config-radius-server)# address ipv4 9.4.62.32 auth-port 1812 acct-port 1813
Device (config-radius-server)# pac key cisco
Device (config-radius-server)# exit
Device(config)# aaa group server radius authz-server-group
Device(config)# server name cisco-catalyst-center-authz-server
Device(config)# end
```



CHAPTER 70

AAA Dead-Server Detection

- Information About AAA Dead-Server Detection, on page 619
- Prerequisites for AAA Dead-Server Detection, on page 620
- Restrictions for AAA Dead-Server Detection, on page 620
- Configuring AAA Dead-Server Detection (CLI), on page 620
- Verifying AAA Dead-Server Detection, on page 621

Information About AAA Dead-Server Detection

The AAA Dead-Server Detection feature allows you to configure the criteria to be used to mark a RADIUS server as dead.

If you have more than one RADIUS server, the following concepts come into picture:

- Deadtime—Defines the time in minutes a server marked as DEAD is held in that state. Once the deadtime expires, the controller marks the server as UP (ALIVE) and notifies the registered clients about the state change. If the server is still unreachable after the state is marked as UP and if the DEAD criteria is met, then server is marked as DEAD again for the deadtime interval.

Note You can configure deadtime for each server group or on a global level.

- Dead-criteria—To declare a server as DEAD, you need to configure **dead-criteria** and configure the conditions that determine when a RADIUS server is considered unavailable or dead.

Using this feature will result in less deadtime and quicker packet processing.

Criteria for Marking a RADIUS Server As Dead

The AAA Dead-Server Detection feature allows you to determine the criteria that are used to mark a RADIUS server as dead. That is, you can configure the minimum amount of time, in seconds, that must elapse from the time that the controller last received a valid packet from the RADIUS server to the time the server is marked as dead. If a packet has not been received since the controller booted, and there is a timeout, the time criterion will be treated as though it has been met.

In addition, you can configure the number of consecutive timeouts that must occur on the controller before the RADIUS server is marked as dead. If the server performs both authentication and accounting, both types

of packets are included in the number. Improperly constructed packets are counted as though they are timeouts. Both initial packet transmission and retransmissions are counted. (Each timeout causes one retransmission to be sent.)

Note Both the time criterion and tries criterion must be met for the server to be marked as dead.

The RADIUS dead-server detection configuration will result in the prompt detection of RADIUS servers that have stopped responding. This configuration will also result in the avoidance of servers being improperly marked as dead when they are "swamped" (responding slowly) and the avoidance of the state of servers being rapidly changed from dead to live to dead again. This prompt detection of non-responding RADIUS servers and the avoidance of swamped and dead-to-live-to-dead-again servers will result in less deadtime and quicker packet processing.

Prerequisites for AAA Dead-Server Detection

- You must have access to a RADIUS server.
- You should be familiar with configuring a RADIUS server.
- You should be familiar with configuring Authentication, Authorization, and Accounting (AAA).
- Before a server can be marked as dead, you must configure **radius-server dead-criteria time** *time-in-seconds* **tries** *number-of-tries* to mark the server as DOWN.

  Also, you must configure the **radius-server deadtime** *time-in-mins* to retain the server in DEAD status.

Restrictions for AAA Dead-Server Detection

- Original transmissions are not counted in the number of consecutive timeouts that must occur on the controller before the server is marked as dead--only the number of retransmissions are counted.

Configuring AAA Dead-Server Detection (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the AAA access control model.

	Command or Action	Purpose
Step 3	**radius-server deadtime** *time-in-mins* **Example:** `Device(config)# radius-server deadtime 5`	Defines the time in minutes when a server marked as DEAD is held in that state. Once the deadtime expires, the controller marks the server as UP (ALIVE) and notifies the registered clients about the state change. If the server is still unreachable after the state is marked as UP and if the DEAD criteria is met, then server is marked as DEAD again for the deadtime interval. *time-in-mins*—Valid values range from 1 to 1440 minutes. Default value is zero. To return to the default value, use the **no radius-server deadtime** command. The **radius-server deadtime** command can be configured globally or per aaa group server level. You can use the **show aaa dead-criteria** or **show aaa servers** command to check for dead-server detection. If the default value is zero, deadtime is not configured.
Step 4	**radius-server dead-criteria** [**time** *time-in-seconds*][**tries** *number-of-tries*] **Example:** `Device(config)# radius-server dead-criteria time 5 tries 4`	Declares a server as DEAD and configures the conditions that determine when a RADIUS server is considered unavailable or dead. *time-in-seconds*—Time in seconds during which no response is received from the RADIUS server to consider it as dead. Valid values range from 1 to 120 seconds. *number-of-tries*—Number of transmits to RADIUS server without responses before marking the server as dead. Valid values range from 1 to 100.
Step 5	**end** **Example:** `Device(config)# end`	Exits configuration mode and enters privileged EXEC mode.

Verifying AAA Dead-Server Detection

To verify dead-criteria, use the following command:

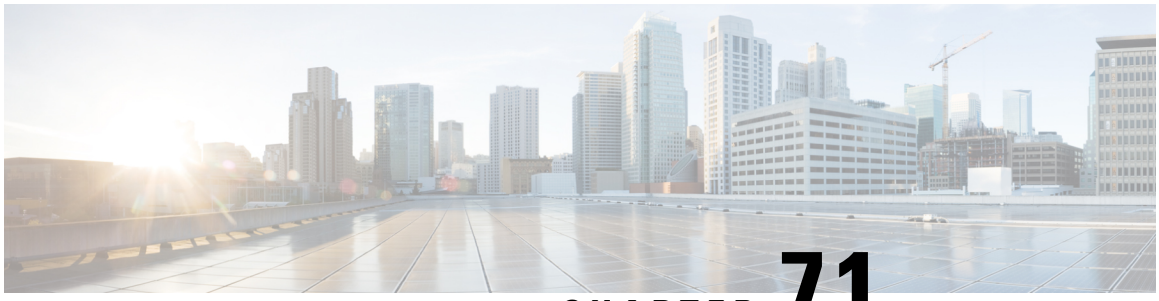
```
Device# show run | s dead-criteria

radius-server dead-criteria time 20 tries 20
```

To verify the dead-criteria details, use the following command:

```
Device# sh aaa dead-criteria radius <server>

sh aaa dead-criteria radius 8.109.0.55
RADIUS Server Dead Criteria:
Server Details:
Address : 8.109.0.55
Auth Port : 1645
Acct Port : 1646
Server Group : radius
Dead Criteria Details:
Configured Retransmits : 3
Configured Timeout : 5
Estimated Outstanding Access Transactions: 2
Estimated Outstanding Accounting Transactions: 0
Dead Detect Time : 30s
Computed Retransmit Tries: 6
Statistics Gathered Since Last Successful Transaction
Max Computed Outstanding Transactions: 3
Max Computed Dead Detect Time: 90s
Max Computed Retransmits : 18
```

To verify the state of servers, number of requests being processed, and so on, use the following command:

```
Device# show aaa servers | s WNCD

Platform State from WNCD (1) : current UP
Platform State from WNCD (2) : current UP
Platform State from WNCD (3) : current UP
Platform State from WNCD (4) : current UP
Platform State from WNCD (5) : current UP, duration 773s, previous duration 0s
Platform Dead: total time 0s, count 0
Quarantined: No
```



CHAPTER 71

RADIUS Server Load Balancing

- Information About RADIUS Server Load Balancing, on page 623
- Prerequisites for RADIUS Server Load Balancing, on page 625
- Restrictions for RADIUS Server Load Balancing, on page 625
- Enabling Load Balancing for a Named RADIUS Server Group (CLI), on page 625

Information About RADIUS Server Load Balancing

RADIUS Server Load Balancing Overview

By default, if two RADIUS servers are configured in a server group, only one is used. The other server acts as standby, if the primary server is declared as dead, the secondary server receives all the load.

If you need both servers to perform transactions actively, you need to enable Load Balancing.

Note By default, load balancing is not enabled on the RADIUS server group.

If you enable load balancing in a RADIUS server group with two or more RADIUS servers, the Server A and Server B receives a AAA transaction. The transaction queues are checked in Server A and Server B. The server with less number of outstanding transactions are assigned the next batch of AAA transaction.

Load balancing distributes batches of transactions to RADIUS servers in a server group. Load balancing assigns each batch of transactions to the server with the lowest number of outstanding transactions in its queue. The process of assigning a batch of transactions is as follows:

1. The first transaction is received for a new batch.
2. All server transaction queues are checked.
3. The server with the lowest number of outstanding transactions is identified.
4. The identified server is assigned the next batch of transactions.

The batch size is a user-configured parameter. Changes in the batch size may impact CPU load and network throughput. As batch size increases, CPU load decreases, and network throughput increases. However, if a large batch size is used, all available server resources may not be fully utilized. As batch size decreases, CPU load increases and network throughput decreases.

Note There is no set number for large or small batch sizes. A batch with more than 50 transactions is considered large and a batch with fewer than 25 transactions is considered small.

Note If a server group contains ten or more servers, we recommend that you set a high batch size to reduce CPU load.

Transaction Load Balancing Across RADIUS Server Groups

You can configure load balancing either per-named RADIUS server group or for the global RADIUS server group. The load balancing server group must be referred to as "radius" in the authentication, authorization, and accounting (AAA) method lists. All public servers that are part of the RADIUS server group are then load balanced.

You can configure authentication and accounting to use the same RADIUS server or different servers. In some cases, the same server can be used for preauthentication, authentication, or accounting transactions for a session. The preferred server, which is an internal setting and is set as the default, informs AAA to use the same server for the start and stop record for a session regardless of the server cost. When using the preferred server setting, ensure that the server that is used for the initial transaction (for example, authentication), the preferred server, is part of any other server group that is used for a subsequent transaction (for example, accounting).

The preferred server is not used if one of the following criteria is true:

- The **load-balance method least-outstanding ignore-preferred-server** command is used.
- The preferred server is dead.
- The preferred server is in quarantine.
- The want server flag has been set, overriding the preferred server setting.

The want server flag, an internal setting, is used when the same server must be used for all stages of a multistage transaction regardless of the server cost. If the want server is not available, the transaction fails.

You can use the **load-balance method least-outstanding ignore-preferred-server** command if you have either of the following configurations:

- Dedicated authentication server and a separate dedicated accounting server
- Network where you can track all call record statistics and call record details, including start and stop records and records that are stored on separate servers

If you have a configuration where authentication servers are a superset of accounting servers, the preferred server is not used.

Note If a third-party RADIUS load balancer is used and RADIUS packets are routed based on the NAS source port, it is recommended to move to any other rule based on the following Attribute-Value Pairs (AVPs):

- If the load balancer uses NAS source port in the Access-Request to load balance, rules may not work as expected as the source port in NAS might change during transaction.
- If the load balancer compares AVPs between Access-Challenge and Access-Request to route packets, you will need to use the AVP value of t-State.
- If the load balancer compares AVPs in Access-Request from NAS, you will need to use one or a combination of the following AVPs:
  - t-State value
  - Calling-Station-ID and NAS IP or Identifier

Prerequisites for RADIUS Server Load Balancing

- Authentication, Authorization, and Accounting (AAA) must be configured on the RADIUS server.
- AAA RADIUS server groups must be configured.
- RADIUS must be configured for functions such as authentication, accounting, or static route download.

Restrictions for RADIUS Server Load Balancing

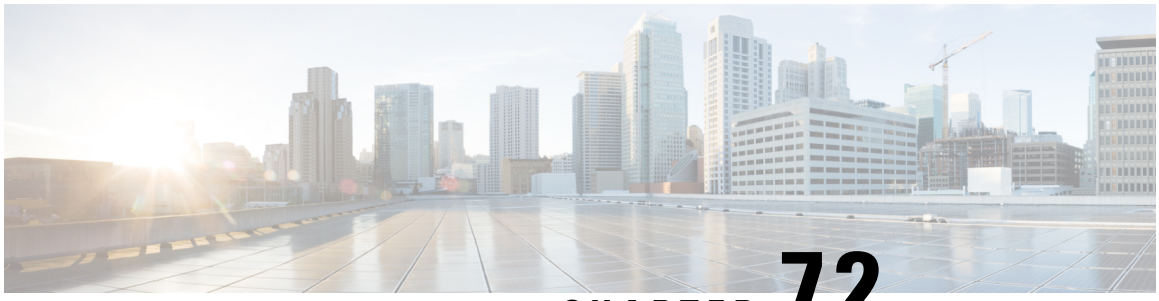
- Incoming RADIUS requests, such as Packet of Disconnect (POD) requests are not supported.
- Load balancing is not supported on proxy RADIUS servers and private server groups.
- Load balancing is not supported on Central Web Authentication (CWA).

Enabling Load Balancing for a Named RADIUS Server Group (CLI)

Procedure

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

	Command or Action	Purpose
Step 2	**aaa group server radius** *group-name* **Example:** `Device(config)# aaa group server radius rad-sg`	Enters server group configuration mode.
Step 3	**server ip-address** [**auth-port port-number**] [**acct-port port-number**] **Example:** `Device(config-sg-radius)# server 192.0.2.238 auth-port 2095 acct-port 2096`	Configures the IP address of the RADIUS server for the group server.
Step 4	**load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**] **Example:** `Device(config-sg-radius)# load-balance method least-outstanding batch-size 30`	Enables the least-outstanding load balancing for a named server group.
Step 5	**end** **Example:** `Device(config-sg)# end`	Exits server group configuration mode and enters privileged EXEC mode.



CHAPTER 72

Secure LDAP

- Information About SLDAP, on page 627
- Prerequisite for Configuring SLDAP, on page 629
- Restrictions for Configuring SLDAP, on page 629
- Configuring SLDAP, on page 629
- Configuring an AAA Server Group (GUI), on page 630
- Configuring a AAA Server Group, on page 631
- Configuring Search and Bind Operations for an Authentication Request, on page 632
- Configuring a Dynamic Attribute Map on an SLDAP Server, on page 633
- Verifying the SLDAP Configuration, on page 633

Information About SLDAP

Transport Layer Security (TLS)

The Transport Layer Security (TLS) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. TLS relies upon certificates, public keys, and private keys to prove the identity of clients.

The certificates are issued by the Certificate Authorities (CAs).

Each certificate includes the following:

- The name of the authority that issued it.
- The name of the entity to which the certificate was issued.
- The public key of the entity.
- The timestamps of the entity that indicate the expiration date of the certificate.

You can find the TLS support for LDAP in the RFC2830 which is an extension to the LDAP protocol.

LDAP Operations

Bind

The bind operation is used to authenticate a user to the server. It is used to start a connection with the LDAP server. LDAP is a connection-oriented protocol. The client specifies the protocol version and authentication information.

LDAP supports the following binds:

- Authenticated bind—An authenticated bind is performed when a root Distinguished Name (DN) and password are available.
- Anonymous bind—In the absence of a root DN and password, an anonymous bind is performed.

In LDAP deployments, the search operation is performed first and the bind operation later. This is because, if a password attribute is returned as part of the search operation, the password verification can be done locally on an LDAP client. Thus, there is no need to perform an extra bind operation. If a password attribute is not returned, the bind operation can be performed later. Another advantage of performing a search operation first and a bind operation later is that the DN received in the search result can be used as the user DN instead of forming a DN by prefixing the username (cn attribute) with the base DN. All entries stored in an LDAP server have a unique DN.

The DN consists of two parts:

- Relative Distinguished Name (RDN)
- Location in the LDAP server where the record resides.

Most of the entries that you store in an LDAP server will have a name, and the name is frequently stored in the Common Name (cn) attribute. Because every object has a name, most objects you store in an LDAP will use their cn value as the basis for their RDN.

Search

A search operation is used to search the LDAP server. The client specifies the starting point (base DN) of the search, the search scope (either the object, its children, or the subtree rooted at the object), and a search filter.

For authorization requests, the search operation is directly performed without a bind operation. The LDAP server can be configured with certain privileges for the search operation to succeed. This privilege level is established with the bind operation.

An LDAP search operation can return multiple user entries for a specific user. In such cases, the LDAP client returns an appropriate error code to AAA. To avoid these errors, you must configure appropriate search filters to match a single entry.

Compare

The compare operation is used to replace a bind request with a compare request for an authentication. The compare operation helps to maintain the initial bind parameters for the connection.

LDAP Dynamic Attribute Mapping

The Lightweight Directory Access Protocol (LDAP) is a powerful and flexible protocol for communication with AAA servers. LDAP attribute maps provide a method to cross-reference the attributes retrieved from a server to Cisco attributes supported by the security appliances.

When a user authenticates a security appliance, the security appliance, in turn, authenticates the server and uses the LDAP protocol to retrieve the record for that user. The record consists of LDAP attributes associated with fields displayed on the user interface of the server. Each attribute retrieved includes a value that was entered by the administrator who updates the user records.

Prerequisite for Configuring SLDAP

If you are using a secure Transport Layer Security (TLS) secure connection, you must configure the X.509 certificates.

Restrictions for Configuring SLDAP

- LDAP referrals are not supported.
- Unsolicited messages or notifications from the LDAP server are not handled.
- LDAP authentication is not supported for interactive (terminal) sessions.

Configuring SLDAP

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ldap server** *name* **Example:** `Device(config)# ldap server server1`	Defines a Lightweight Directory Access Protocol (LDAP) server and enters LDAP server configuration mode.
Step 4	**ipv4** *ipv4-address* **Example:** `Device(config-ldap-server)# ipv4 9.4.109.20`	Specifies the LDAP server IP address using IPv4.
Step 5	**timeout retransmit** *seconds* **Example:** `Device(config-ldap-server)# timeout retransmit 20`	Specifies the number of seconds the Cisco Catalyst 9800 Series Wireless Controller embedded wireless controller waits for a reply to an LDAP request before retransmitting the request.
Step 6	**bind authenticate root-dn password** [**0** *string* | **7** *string*] *string*	Specifies a shared secret text string used between the Cisco Catalyst 9800 Series

	Command or Action	Purpose
	Example: `Device(config-ldap-server)# bind authenticate root-dn CN=ldapipv6user,CN=Users,DC=ca,DC=ssh2,DC=com password Cisco12345`	Wireless Controller embedded wireless controller and an LDAP server. Use the **0** line option to configure an unencrypted shared secret. Use the **7** line option to configure an encrypted shared secret.
Step 7	**base-dn** *string* **Example:** `Device(config-ldap-server)# base-dn CN=Users,DC=ca,DC=ssh2,DC=com`	Specifies the base Distinguished Name (DN) of the search.
Step 8	**mode secure** [**no- negotiation**] **Example:** `Device(config-ldap-server)# mode secure no- negotiation`	Configures LDAP to initiate the TLS connection and specifies the secure mode.
Step 9	**end** **Example:** `Device(config-ldap-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring an AAA Server Group (GUI)

Configuring a device to use AAA server groups helps you to group existing server hosts, select a subset of the configured server hosts and use them for a particular service. A server group is used with a global server-host list. The server group lists the IP addresses of the selected server hosts.

You can create the following server groups:

Procedure

Step 1 RADIUS

a) Choose **Services** > **Security** > **AAA** > **Server Groups** > **RADIUS**.
b) Click the **Add** button. The **Create AAA Radius Server Group** dialog box appears.
c) Enter a name for the RADIUS server group in the **Name** field.
d) Choose a desired delimiter from the **MAC-Delimiter** drop-down list. The available options are colon, hyphen, and single-hyphen.
e) Choose a desired filter from the **MAC-Filtering** drop-down list. The available options are mac and Key.
f) Enter a value in the **Dead-Time (mins)** field to make a server non-operational. You must specify a value between 1 and 1440.
g) Choose any of the available servers from the **Available Servers** list and move them to the **Assigned Servers** list by clicking the > button.
h) Click the **Save & Apply to Device** button.

Step 2 TACACS+

a) Choose **Services** > **Security** > **AAA** > **Server Groups** > **TACACS+**.
b) Click the **Add** button. The **Create AAA Tacacs Server Group** dialog box appears.
c) Enter a name for the TACACS server group in the **Name** field.
d) Choose any of the available servers from the **Available Servers** list and move them to the **Assigned Servers** list by clicking the **>** button.
e) Click the **Save & Apply to Device** button.

Step 3 LDAP

a) Choose **Services** > **Security** > **AAA** > **Server Groups** > **LDAP**.
b) Click the **Add** button. The **Create AAA Ldap Server Group** dialog box appears.
c) Enter a name for the LDAP server group in the **Name** field.
d) Choose any of the available servers from the **Available Servers** list and move them to the **Assigned Servers** list by clicking the **>** button.
e) Click the **Save & Apply to Device** button.

Configuring a AAA Server Group

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**aaa group server ldap** *group-name* **Example:** `Device(config)# aaa group server ldap name1`	Defines the AAA server group with a group name and enters LDAP server group configuration mode. All members of a group must be of the same type, that is, RADIUS, LDAP, or TACACS+.
Step 5	**server** *name* **Example:** `Device(config-ldap-sg)# server server1`	Associates a particular LDAP server with the defined server group. Each security server is identified by its IP address and UDP port number.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Device(config-ldap-sg)# exit`	Exits LDAP server group configuration mode.

Configuring Search and Bind Operations for an Authentication Request

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**ldap server** *name* **Example:** `Device(config)# ldap server server1`	Defines a Lightweight Directory Access Protocol (LDAP) server and enters LDAP server configuration mode.
Step 5	**authentication bind-first** **Example:** `Device(config-ldap-server)# authentication bind-first`	Configures the sequence of search and bind operations for an authentication request.
Step 6	**authentication compare** **Example:** `Device(config-ldap-server)# authentication compare`	Replaces the bind request with the compare request for authentication.
Step 7	**exit** **Example:** `Device(config-ldap-server)# exit`	Exits LDAP server group configuration mode.

Configuring a Dynamic Attribute Map on an SLDAP Server

You must create LDAP attribute maps that map your existing user-defined attribute names and values to Cisco attribute names and values that are compatible with the security appliance. You can then bind these attribute maps to LDAP servers or remove them as required.

Note To use the attribute mapping features correctly, you need to understand the Cisco LDAP and user-defined attribute names and values.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ldap attribute-map** *map-name* **Example:** `Device(config)# ldap attribute-map map1`	Configures a dynamic LDAP attribute map and enters attribute-map configuration mode.
Step 4	**map type** *ldap-attr-type aaa-attr-type* **Example:** `Device(config-attr-map)# map type department supplicant-group`	Defines an attribute map.
Step 5	**exit** **Example:** `Device(config-attr-map)# exit`	Exits attribute-map configuration mode.

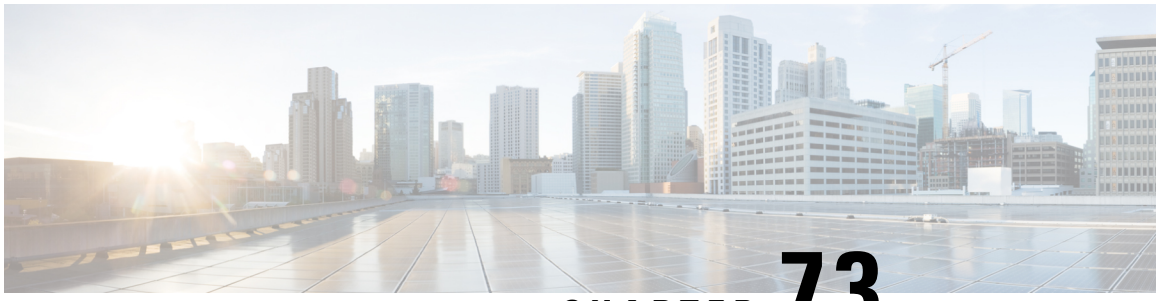
Verifying the SLDAP Configuration

To view details about the default LDAP attribute mapping, use the following command:

```
Device# show ldap attributes
```

To view the LDAP server state information and various other counters for the server, use the following command:

```
Device# show ldap server
```



CHAPTER 73

RADIUS DTLS

- Information About RADIUS DTLS, on page 635
- Prerequisites, on page 637
- Configuring RADIUS DTLS Server, on page 637
- Configuring DTLS Dynamic Author, on page 642
- Enabling DTLS for Client, on page 642
- Verifying the RADIUS DTLS Server Configuration, on page 645
- Clearing RADIUS DTLS Specific Statistics, on page 645

Information About RADIUS DTLS

The Remote Authentication Dial-In User Service (RADIUS) is a client or server protocol that provides centralized security for users attempting to gain management access to a network. The RADIUS protocol is a widely deployed authentication and authorization protocol that delivers a complete Authentication, Authorization, and Accounting (AAA) solution.

RADIUS DTLS Port

The RADIUS port (DTLS server) is used for authentication and accounting. The default DTLS server port is 2083.

You can change the RADIUS DTLS port number using **dtls port** *port_number*. For more information, see the Configuring RADIUS DTLS Port Numbersection.

Shared Secret

You can use **radius/dtls** as the shared secret, if you have enabled DTLS for a specific server.

Handling PAC for CTS Communication

You can download PAC from ISE for CTS communication. Once the PAC is downloaded, you need to encrypt all the CTS attributes with the PAC key instead of the shared secret.

The ISE then decrypts these attributes using PAC.

Session Management

The RADIUS client purely depends on the response from the DTLS server. If the session is ideal for ideal timeout, then the session must be closed.

In case of invalid responses, the sessions must be deleted.

If you need to send the radius packets over DTLS, the DTLS session needs to be re-established with the specific server.

Load Balancing

Multiple DTLS servers and load balancing methods are configured.

You need to select the AAA server to which the request needs to be sent. Then use the DTLS context of the specific server to encrypt the RADIUS packet and send it back.

Connection Timeout

After the encrypted RADIUS packet is sent, you need to start the retransmission timer. If you do not get a response before the retransmission timer expires, the packet is re-encrypted and re-transmitted.

You can continue for number of times as per the **dtls retries** configuration or till the default value. Once the number of tries exceeds the limit, the server becomes unavailable and responses are sent back to the AAA clients.

Note The default connection timeout is 5 seconds.

Connection Retries

As the RADIUS DTLS is UDP based, you need to retry the connection after a specific timeout interval for a specific number of retries.

After all retries are exhausted, the DTLS connection performs the following:

- Is marked as unsuccessful.
- Looks up for the next available server for processing the RADIUS requests.

Note The default connection retries is 5.

Idle Timeout

When the idle timer expires and no transactions exists since the last idle timeout, the DTLS session remains closed.

After you establish the DTLS session, you can start the idle timer. If you start the idle timer for 30 seconds and one of the RADIUS DTLS packet is sent, then after 30 seconds, the idle timer expires and checks for number of RADIUS DTLS transactions.

If the idle timer value exceeds zero, the idle timer resets the transaction counter and restarts the timer.

Note The default idle timeout is 60 seconds.

Handling Server and Server Group Failover

You can configure RADIUS servers with and without DTLS. It is recommended to create AAA server groups with DTLS enabled servers and non-DTLS servers. However, you will not find any such restriction while configuring AAA server groups.

Suppose you choose a DTLS server, the DTLS server establishes connection and RADIUS request packet is sent to the DTLS server. If the DTLS server does not respond after all RADIUS retries, it would fall over to the next configured server in the same server group. If the next server is a DTLS server, the processing of the RADIUS request packet continues with the next server. If the next server is a non-DTLS server, the processing of RADIUS request packet does not happen in that server group. Then the server group failover occurs and the same sequence continues with the next server group, if the next server group is available.

Note You need to use either only DTLS or non-DTLS servers in a server group.

Prerequisites

Support for IOS and BINOS AAA

The AAA server runs in IOS and BINOS platforms. Once you complete the RADIUS DTLS support in IOS, the same needs to be ported to BINOS.

Configuring RADIUS DTLS Server

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server R1`	Specifies the RADIUS server name.

	Command or Action	Purpose
Step 4	**dtls** **Example:** `Device(config-radius-server)# dtls`	Configures DTLS parameters.
Step 5	**end** **Example:** `Device(config-radius-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring RADIUS DTLS Connection Timeout

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server R1`	Specifies the RADIUS server name.
Step 4	**dtls connectiontimeout** *timeout* **Example:** `Device(config-radius-server)# dtls connectiontimeout 1`	Configures RADIUS DTLS connection timeout. Here, *timeout* refers to the DTLS connection timeout value. The valid range is from 1 to 65535.
Step 5	**end** **Example:** `Device(config-radius-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring RADIUS DTLS Idle Timeout

Procedure

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

	Command or Action	Purpose
	`Device# enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server R1`	Specifies the RADIUS server name.
Step 4	**dtls idletimeout** *idle_timeout* **Example:** `Device(config-radius-server)# dtls idletimeout 2`	Configures RADIUS DTLS idle timeout. Here, *idle_timeout* refers to the DTLS idle timeout value. The valid range is from 1 to 65535.
Step 5	**end** **Example:** `Device(config-radius-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Source Interface for RADIUS DTLS Server

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server R1`	Specifies the RADIUS server name.
Step 4	**dtls ip** {**radius source-interface Ethernet-Internal** *interface_number* **Example:** `Device(config-radius-server)# dtls ip radius source-interface Ethernet-Internal 0`	Configures source interface for RADIUS DTLS server. Here, • *interface_number* refers to the Ethernet-Internal interface number. The default value is 0.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config-radius-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring RADIUS DTLS Port Number

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server R1`	Specifies the RADIUS server name.
Step 4	**dtls port** *port_number* **Example:** `Device(config-radius-server)# dtls port 2`	Configures RADIUS DTLS port number. Here, *port_number* refers to the DTLS port number.
Step 5	**end** **Example:** `Device(config-radius-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring RADIUS DTLS Connection Retries

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server R1`	Specifies the RADIUS server name.
Step 4	**dtls retries** *retry_number* **Example:** `Device(config-radius-server)# dtls retries 3`	Configures RADIUS connection retries. Here, *retry_number* refers to the DTLS connection retries. The valid range is from 1 to 65535.
Step 5	**end** **Example:** `Device(config-radius-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring RADIUS DTLS Trustpoint

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server R1`	Specifies the RADIUS server name.

Step 4	**dtls trustpoint** {**client** *LINE* **dtls** | **server** *LINE* **dtls**}
	Example:
	`Device(config-radius-server)# dtls trustpoint client client1 dtls`
	`Device(config-radius-server)# dtls trustpoint server server1 dtls`
		Configures trustpoint for client and server.

Step 5	**end** **Example:** `Device(config-radius-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring DTLS Dynamic Author

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Configures local server profile for RFC 3576 support.
Step 4	**dtls** **Example:** `Device(config-locsvr-da-radius)# dtls`	Configures DTLS source parameters.
Step 5	**end** **Example:** `Device(config-locsvr-da-radius)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Enabling DTLS for Client

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius dynamic-author** **Example:**	Configures local server profile for RFC 3576 support.

	Command or Action	Purpose
	`Device(config)# aaa server radius dynamic-author`	
Step 4	**client** *IP_addr* **dtls** **Example:** `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls`	Enables DTLS for the client.
Step 5	**end** **Example:** `Device(config-locsvr-da-radius)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Client Trustpoint for DTLS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Configures local server profile for RFC 3576 support.
Step 4	**client** *IP_addr* **dtls** {**client-tp** *client-tp-name* | **server-tp** *server-tp-name*} **Example:** `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls client-tp client_tp_name`	Configures client trustpoint for DTLS.
Step 5	**end** **Example:** `Device(config-locsvr-da-radius)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring DTLS Idle Timeout

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Configures local server profile for RFC 3576 support.
Step 4	**client** *IP_addr* **dtls idletimeout** *timeout-interval* {**client-tp** *client_tp_name* | **server-tp** *server_tp_name*} **Example:** `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls idletimeout 62 client-tp dtls_ise`	Configures DTLS idle time. Here, *timeout-interval* refers to the idle timeout interval. The valid range is from 60 to 600.
Step 5	**end** **Example:** `Device(config-locsvr-da-radius)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Server Trustpoint for DTLS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Configures local server profile for RFC 3576 support.
Step 4	**client** *IP_addr* **dtls server-tp** *server_tp_name* **Example:** `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls server-tp dtls_client`	Configures server trust point.
Step 5	**end** **Example:** `Device(config-locsvr-da-radius)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying the RADIUS DTLS Server Configuration

To view information about the DTLS enabled servers, use the following command:

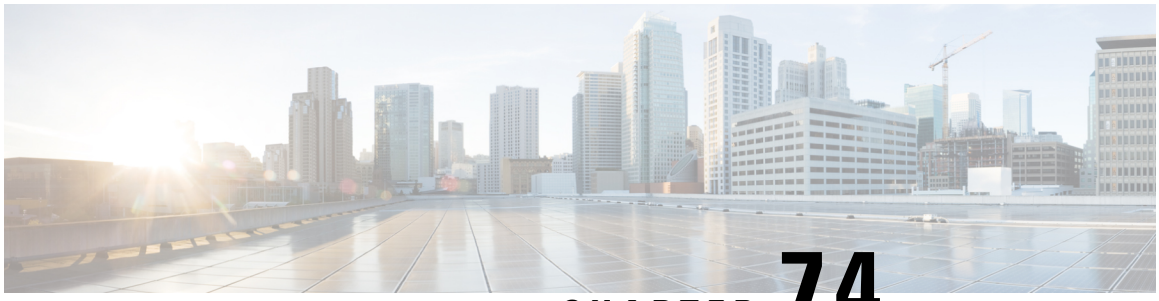
```
Device# show aaa servers
DTLS: Packet count since last idletimeout 1,
Send handshake count 3,
Handshake Success 1,
Total Packets Transmitted 1,
Total Packets Received 1,
Total Connection Resets 2,
Connection Reset due to idle timeout 0,
Connection Reset due to No Response 2,
Connection Reset due to Malformed packet 0,
```

Clearing RADIUS DTLS Specific Statistics

To clear the radius DTLS specific statistics, use the following command:

```
Device# clear aaa counters servers radius {<server-id> | all}
```

Note Here, *server-id* refers to the server ID displayed by **show aaa servers**. The valid range is from 0 to 2147483647.



CHAPTER 74

Internet Protocol Security

- Information about Internet Protocol Security, on page 647
- Internet Key Exchange Version 1 Transform Sets, on page 648
- Configure IPSec Using Internet Key Exchange Version 1, on page 649
- Internet Key Exchange Version 2 Transform Sets, on page 651
- Configure IPSec Using Internet Key Exchange Version 2, on page 652
- IPsec Transforms and Lifetimes, on page 654
- Use of X.509 With Internet Key Exchange Version, on page 655
- IPsec Session Interuption and Recovery, on page 656
- Example: Configure IPSec Using ISAKMP, on page 657
- Verifying IPSec Traffic, on page 657
- Example: Configure IPSec Using Internet Key Exchange Version 2, on page 658
- Verifying IPSec With Internet Key Exchange Version 2 Traffic , on page 659

Information about Internet Protocol Security

Internet Protocol Security (IPsec) is a framework of open standards for ensuring secure private communications over the Internet. Based on standards developed by the Internet Engineering Task Force (IETF), IPsec ensures confidentiality, integrity, and authenticity of data communications across a public network. IPsec provides a necessary component of a standards-based, flexible solution for deploying a network-wide security policy.

Cisco Catalyst 9800 Series Wireless Controller supports IPsec configuration. The support for IPSec secures syslog traffic.

This section provides information about how to configure IPsec between Cisco Catalyst 9800 Series Wireless Controller and syslog (peer IP).

IPsec provides the following network security services:

- Data confidentiality: The IPsec sender can encrypt packets before transmitting them across a network.
- Data integrity: The IPsec receiver can authenticate packets sent by the IPsec sender to ensure that the data has not been altered during transmission.
- Data origin authentication: The IPsec receiver can authenticate the source of the sent IPsec packets. This service is dependent upon the data integrity service.
- Anti-replay: The IPsec receiver can detect and reject replayed packets.

IPsec provides secure *tunnels* between two peers, such as two devices. The administrator defines which packets are considered sensitive and should be sent through these secure tunnels and specifies the parameters that should be used to protect these sensitive packets by specifying the characteristics of these tunnels. When the IPsec peer recognizes a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

More accurately, these *tunnels* are sets of security associations (SAs) that are established between two IPsec peers. The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used by the two peers. SAs are unidirectional and are established per security protocol.

With IPsec, administrators can define the traffic that needs to be protected between two IPsec peers by configuring access lists and applying these access lists to interfaces using crypto map sets. Therefore, traffic may be selected on the basis of the source and destination address, and optionally the Layer 4 protocol and port. (The access lists used for IPsec are only used to determine the traffic that needs to be protected by IPsec, not the traffic that should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface.)

A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence--the device attempts to match the packet to the access list specified in that entry.

When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged as cisco, connections are established, if necessary. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry.

Once established, the set of SAs (outbound to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the device. *Applicable* packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer.

Access lists associated with IPsec crypto map entries also represent the traffic that the device needs protected by IPsec. Inbound traffic is processed against crypto map entries--if an unprotected packet matches a permit entry in a particular access list associated with an IPsec crypto map entry, that packet is dropped because it was not sent as an IPsec-protected packet.

Crypto map entries also include transform sets. A transform set is an acceptable combination of security protocols, algorithms, and other settings that can be applied to IPsec-protected traffic. During the IPsec SA negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

Internet Key Exchange Version 1 Transform Sets

An Internet Key Exchange version 1 (IKEv1) transform set represents a certain combination of security protocols and algorithms. During the IPsec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

Privileged administrators can specify multiple transform sets and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry is used in the IPsec SA negotiation to protect the data flows specified by that crypto map entry's access list.

During IPsec security association negotiations with IKE, peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and applied to the protected traffic as part of both peers' IPsec SAs.

Note If a transform set definition is changed during operation that the change is not applied to existing security associations, but is used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, you can clear all or part of the SA database by using the **clear crypto sa** command.

The following snippet helps to configure IPsec IKEv1 to use AES-CBC-128 for payload encryption. AES-CBC-256 can be selected with *encryption aes 256*:

```
device # conf t
device (config)#crypto isakmp policy 1
device (config-isakmp)# hash sha
device (config-isakmp)# encryption aes
```

Configure IPSec Using Internet Key Exchange Version 1

Follow the procedure given below to configure IPsec IKEv1 to use AES-CBC-128 for payloadencryption:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto isakmp policy** *priority* **Example:** `Device(config)# crypto isakmp policy 1`	Defines an Internet Key Exchange (IKE) policy and assigns a priority to the policy. • *priority*: Uniquely identifies the IKE policy and assigns a priority to the policy. Valid values: 1 to 10,000; 1 is the highest priority.
Step 3	**hash sha** **Example:** `Device(config-isakmp)# hash sha`	Specifies the hash algorithm.
Step 4	**encryption aes** **Example:** `Device(config-isakmp)# encryption aes`	Configures IPsec IKEv1 to use AES-CBC-128 for payload encryption. AES-CBC-256 can be selected with ‘encryption aes 256’.

	Command or Action	Purpose
		Note The authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in section IPsec Transforms and Lifetimes. If AES 128 is selected here, then the highest keysize that can be selected on the device for ESP is AES 128 (either CBC or GCM). Both confidentiality and integrity are configured with the **hash sha** and **encryption aes** commands respectively. As a result, confidentiality-only mode is disabled.
Step 5	**authentication pre-share** **Example:** `Device(config-isakmp)# authentication pre-share`	Configures IPsec to use the specified preshared keys as the authentication method. Preshared keys require that you separately configure these preshared keys.
Step 6	**exit** **Example:** `Device(config-isakmp)# exit`	Exits config-isakmp configuration mode.
Step 7	**crypto isakmp key** *keystring* **address** *peer-address* **Example:** `Device(config)# crypto isakmp key cisco123!cisco123!CISC address 192.0.2.1`	Configures a preshared authentication key. **Note** To ensure a secure configuration, we recommend that you enter the pre-shared keys with at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"). The device supports pre-shared keys up to 127 characters in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time.
Step 8	**group 14** **Example:** `Device(config-isakmp)# group 14`	Specifies the Diffie-Hellman (DH) group identifier as 2048-bit DH group 14 and selects DH Group 14 (2048-bit MODP) for IKE. However, 19 (256-bit Random ECP), 24

	Command or Action	Purpose
		(2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), 15 (3072 bit MODP), and 16 (4096-bit MODP) are also allowed and supported.
Step 9	**lifetime** *seconds* **Example:** `Device(config-isakmp)# lifetime 86400`	Specifies the lifetime of the IKE SA. The default time value for Phase 1 SAs is 24 hours (86400 seconds), but this setting can be changed using the command above with different values. • *seconds*: Time, in seconds, before each SA expires. Valid values: 60 to 86,400; default value: 86,400. **Note** The shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec SAs can be set up more quickly.
Step 10	**crypto isakmp aggressive-mode disable** **Example:** `Device(config-isakmp)# crypto isakmp aggressive-mode disable`	Ensures all IKEv1 Phase 1 exchanges will be handled in the default main mode.
Step 11	**exit** **Example:** `Device(config-isakmp)# exit`	Exits config-isakmp configuration mode.

Internet Key Exchange Version 2 Transform Sets

An Internet Key Exchange Version 2 (IKEv2) proposal is a set of transforms used in the negotiation of IKEv2 SA as part of the IKE_SA_INIT exchange. An IKEv2 proposal is regarded as complete only when it has at least an encryption algorithm, an integrity algorithm, and a Diffie-Hellman (DH) group configured. If no proposal is configured and attached to an IKEv2 policy, then the default proposal is used in the negotiation. The following snippet helps in configuring the IPsec with IKEv2 functionality for the device:

```
device # conf t
device(config)#crypto ikev2 proposal sample
device(config-ikev2-proposal)# integrity sha1
device (config-ikev2-proposal)# encryption aes-cbc-128
device(config-ikev2-proposal)# group 14
device(config-ikev2-proposal)# exit
device(config)# crypto ikev2 keyring keyring-1
device (config-ikev2-keyring)# peer peer1
device (config-ikev2-keyring-peer)# address 192.0.2.4 255.255.255.0
```

```
device (config-ikev2-keyring-peer)# pre-shared-key cisco123!cisco123!CISC
device (config-ikev2-keyring-peer)# exit
device(config)#crypto ikev2 keyring keyring-1
device (config-ikev2-keyring)# peer peer1
device (config-ikev2-keyring-peer)# address 192.0.2.4 255.255.255.0
device (config-ikev2-keyring-peer)# pre-shared-key cisco123!cisco123!CISC
device (config-ikev2-keyring-peer)# exit
device(config)#crypto logging ikev2
```

Configure IPSec Using Internet Key Exchange Version 2

Follow the procedure given below to configure the IPsec with IKEv2:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto ikev2 proposal** *name* **Example:** `Device(config)# crypto ikev2 proposal name`	Defines an IKEv2 proposal name.
Step 3	**integrity sha1** **Example:** `Device(config-ikev2-proposal)# integrity sha1`	Defines an IKEv2 proposal name.
Step 4	**encryption aes-cbc-128** **Example:** `Device(config-ikev2-proposal)# encryption aes-cbc-128`	Configures IPsec IKEv2 to use AES-CBC-128 for payload encryption. AES-CBC-256 can be selected with encryption aes-cbc-256. AES-GCM-128 and AES-GCM-256 can also be selected similarly.

	Command or Action	Purpose
		Note The authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in section IPsec Transforms and Lifetimes. If AES 128 is selected here, then the highest keysize that can be selected on the device for ESP is AES 128 (either CBC or GCM). Both confidentiality and integrity are configured with the **hash sha** and **encryption aes** commands respectively. As a result, confidentiality-only mode is disabled.
Step 5	**group 14** **Example:** `Device(config-ikev2-proposal)# group 14`	Selects DH Group 14 (2048-bit MODP) for IKE. However, 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), 15 (3072 bit MODP), and 16 (4096-bit MODP) are also allowed and supported.
Step 6	**exit** **Example:** `Device(config-ikev2-proposal)# exit`	Exists IKEv2 proposal configuration mode.
Step 7	**crypto ikev2 keyring** *keyring-name* **Example:** `Device(config)# crypto ikev2 keyring keyring-1`	Defines an IKEv2 keyring.
Step 8	**peer** *peer-name* **Example:** `Device(config-ikev2-keyring)# peer peer1`	Defines the peer or peer group.
Step 9	**address {ipv4-address [mask] | ipv6-address prefix}** **Example:** `Device(config-ikev2-keyring)# address 192.0.2.4 255.255.255.0`	Specifies an IPv4 or IPv6 address or range for the peer. **Note** This IP address is the IKE endpoint address and is independent of the identity address.
Step 10	**pre-shared-key** *local* **Example:**	Specifies the preshared key for the peer. You can enter the local or remote keyword to

	Command or Action	Purpose
	`Device(config-ikev2-keyring)# pre-shared-key cisco123!cisco123!CISC`	specify an asymmetric preshared key. By default, the preshared key is symmetric. **Note** To ensure a secure configuration, we recommend that you enter the pre-shared keys with at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"). The device supports pre-shared keys up to 127 characters in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time. HEX keys generated off system can also be input for IKEv2 using the following instead of the pre-shared-key command above: *pre-shared-key hex [hex key]*. For example: pre-shared-key hex 0x6A6B6C. This configures IPsec to use pre-shared keys.
Step 11	**exit** **Example:** `Device(config-ikev2-keyring)# exit`	Exits IKEv2 keyring peer configuration mode.
Step 12	**crypto logging ikev2** **Example:** `Device(config)# crypto logging ikev2`	Enables IKEv2 syslog messages. **Note** The configuration above is not a complete IKE v2 configuration, and that additional settings will be needed.

IPsec Transforms and Lifetimes

Regardless of the IKE version selected, the device must be configured with the proper transform for IPsec ESP encryption and integrity as well as IPsec lifetimes.

`device (config)#` **`crypto ipsec transform-set example esp-aes 128 esp-sha-hmac`**

Note that this configures IPsec ESP to use HMAC-SHA-1 and AES-CBC-128. To change this to the other allowed algorithms the following options can replace **esp-aes 128** in the command above:

Encryption Algorithm	Command
AES-CBC-256	**esp-aes 256**
AES-GCM-128	**esp-gcm 128**
AES-GCM-256	**esp-gcm 256**

Note The size of the key selected here must be less than or equal to the key size selected for the IKE encryption setting. If AES-CBC-128 was selected there for use with IKE encryption, then only AES-CBC-128 or AES-GCM-128 may be selected here.

```
device(config-crypto)# mode tunnel
```

This configures tunnel mode for IPsec. Tunnel is the default, but by explicitly specifying tunnel mode, the device will request tunnel mode and will accept only tunnel mode.

```
device(config-crypto)# mode transport
```

This configures transport mode for IPsec.

```
device(config)# crypto ipsec security-association lifetime seconds 28800
```

The default time value for Phase 2 SAs is 1 hour. There is no configuration required for this setting since the default is acceptable. However to change the setting to 8 hours as claimed in the Security Target the crypto ipsec security-association lifetime command can be used as specified above.

```
device(config)# crypto ipsec security-association lifetime kilobytes 100000
```

This configures a lifetime of 100 MB of traffic for Phase 2 SAs. The default amount for this setting is 2560KB, which is the minimum configurable value for this command. The maximum configurable value for this command is 4GB.

Use of X.509 With Internet Key Exchange Version

Cisco Catalyst 9800 Series Wireless Controller supports RSA and ECDSA based certificates.

Once X.509v3 keys are installed on the device, they can be set for use with IKEv1 with the commands:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto isakmp** *policy-name* **Example:** `Device(config)#crypto isakmp policy 1`	Defines an Internet Key Exchange (IKE) policy and assigns a priority to the policy.

	Command or Action	Purpose
Step 3	**authentication [remote | local] rsa-sig** **Example:** `Device(config-isakmp)#authentication rsa-sig`	Uses RSA based certificates for IKEv1 authentication.
Step 4	**authentication [remote | local] ecdsa-sig** **Example:** `Device(config-isakmp)#authentication ecdsa-sig`	Uses ecdsa based certificates for IKEv1 authentication.

For IKEv2 Commands

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto ikev2 profile sample** **Example:** `Device(config)# crypto ikev2 profile sample`	Defines an Internet Key Exchange (IKE) policy and assigns a profile.
Step 3	**authentication [remote | local] rsa-sig** **Example:** `Device(config-ikev2-profile)# authentication rsa-sig`	Uses RSA based certificates for IKEv1 authentication.
Step 4	**authentication [remote | local] ecdsa-sig** **Example:** `Device(config-ikev2-profile)# authentication ecdsa-sig`	Uses ecdsa based certificates for IKEv1 authentication. Authentication fails if an invalid certificate is loaded.

IPsec Session Interuption and Recovery

If an IPsec session with a peer is unexpectedly interrupted, the connection will be broken. In this scenario, no administrative interaction is required. The IPsec session will be reestablished (a new SA set up) once the peer is back online.

Example: Configure IPSec Using ISAKMP

The following sample outputs display the IPSec **isakmp** configuration:

```
crypto isakmp policy 1
 encr aes 256
 hash sha256
 authentication pre-share
 group 14
 lifetime 28800

crypto isakmp key 0 Cisco!123 address 192.0.2.4
crypto isakmp peer address 192.0.2.4

crypto ipsec transform-set aes-gcm-256 esp-gcm 256
 mode tunnel

crypto map IPSEC_ewlc_to_syslog 1 ipsec-isakmp
 set peer 192.0.2.4
 set transform-set aes-gcm-256
 match address acl_ewlc_to_syslog

interface Vlan15
 crypto map IPSEC_ewlc_to_syslog
end
```

Verifying IPSec Traffic

The following example shows how to verify the IPSec traffic configuration in isakmp configuration:

```
Device# show crypto map
Crypto Map IPv4 "IPSEC_ewlc_to_syslog" 1 ipsec-isakmp
        Peer = 192.0.2.4
        Extended IP access list acl_ewlc_to_syslog
            access-list acl_ewlc_to_syslog permit ip host 192.0.2.2 host 192.0.2.4
        Current peer: 192.0.2.4
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                aes-gcm-256:  { esp-gcm 256  } ,
        }
        Interfaces using crypto map IPSEC_ewlc_to_syslog:
                Vlan15

Device# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.0.2.5       192.0.2.4       QM_IDLE           1011 ACTIVE

IPv6 Crypto ISAKMP SA

Device# show crypto ipsec sa

interface: Vlan15
    Crypto map tag: IPSEC_ewlc_to_syslog, local addr 192.0.2.5

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.0.2.5/255.255.255.255/0/0)
```

```
   remote ident (addr/mask/prot/port): (192.0.2.4/255.255.255.255/0/0)
   current_peer 192.0.2.4 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1626, #pkts encrypt: 1626, #pkts digest: 1626
    #pkts decaps: 1625, #pkts decrypt: 1625, #pkts verify: 1625
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.0.2.5, remote crypto endpt.: 192.0.2.4
     plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb Vlan15
     current outbound spi: 0x17FF2F4C(402599756)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x4B77AD78(1266134392)
        transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 2041, flow_id: HW:41, sibling_flags FFFFFFFF80004048, crypto map:
IPSEC_ewlc_to_syslog
        sa timing: remaining key lifetime (k/sec): (4607904/1933)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x17FF2F4C(402599756)
        transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 2042, flow_id: HW:42, sibling_flags FFFFFFFF80004048, crypto map:
IPSEC_ewlc_to_syslog
        sa timing: remaining key lifetime (k/sec): (4607904/1933)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:
     outbound pcp sas:

Device# show ip access-lists acl_ewlc_to_syslog
Extended IP access list acl_ewlc_to_syslog
    10 permit ip host 192.0.2.5 host 192.0.2.4 (17 matches)
```

Example: Configure IPSec Using Internet Key Exchange Version 2

The following sample outputs display the IPSec **IKEv2** configuration:

```
topology : [192.0.2.6]DUT — (infra) — PEER[192.0.2.9]

ikev2 config in 192.0.2.6 (peer is 192.0.2.9)
hostname for 192.0.2.9: Edison-M1
hostname for 192.0.2.6: prsna-nyquist-192.0.2.6

ip access-list extended ikev2acl
 permit ip host 192.0.2.6 host 192.0.2.9
```

```
crypto ikev2 proposal PH1PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy PH1POLICY
 proposal PH1PROPOSAL

crypto ikev2 keyring PH1KEY
  peer Edison-M1
  address 192.0.2.9
  pre-shared-key Cisco!123Cisco!123Cisco!123


crypto ikev2 profile PH1PROFILE
 match identity remote address 192.0.2.9 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local PH1KEY

crypto ipsec transform-set aes256-sha1 esp-aes 256 esp-sha-hmac
 mode tunnel

crypto map ikev2-cryptomap 1 ipsec-isakmp
 set peer 192.0.2.9
 set transform-set aes256-sha1
 set ikev2-profile PH1PROFILE
 match address ikev2acl

interface Vlan15
 ip address 192.0.2.6 255.255.255.0
 crypto map ikev2-cryptomap
```

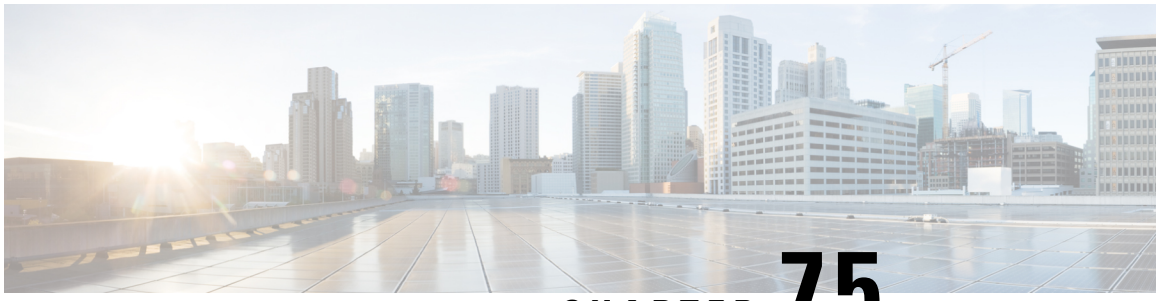
Verifying IPSec With Internet Key Exchange Version 2 Traffic

The following example shows how to verify the IPSec traffic configuration in IKEv2 configuration:

```
Device# show ip access-lists
Extended IP access list ikev2acl
    10 permit ip host 192.0.2.6 host 192.0.2.9 (80 matches)

prsna-nyquist-192.0.2.6#show crypto map
Crypto Map IPv4 "ikev2-cryptomap" 1 ipsec-isakmp
        Peer = 192.0.2.9
        IKEv2 Profile: PH1PROFILE
        Extended IP access list ikev2acl
            access-list ikev2acl permit ip host 192.0.2.6 host 192.0.2.9
        Current peer: 192.0.2.9
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                aes256-sha1:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map ikev2-cryptomap:
                Vlan15
Device# show crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
```

```
1         192.0.2.6/500         192.0.2.9/500          none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK,
Auth verify: PSK
      Life/Active Time: 86400/1002 sec
      CE id: 1089, Session-id: 2
      Status Description: Negotiation done
      Local spi: 271D20169FE91074       Remote spi: 13895472E3B910AF
      Local id: 192.0.2.6
      Remote id: 192.0.2.9
      Local req msg id:  2              Remote req msg id:  0
      Local next msg id: 2              Remote next msg id: 0
      Local req queued:  2              Remote req queued:  0
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      Fragmentation not  configured.
      Dynamic Route Update: disabled
      Extended Authentication not configured.
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes
Device# show crypto ipsec sa detail

interface: Vlan15
    Crypto map tag: ikev2-cryptomap, local addr 192.0.2.6

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.0.2.6/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (192.0.2.9/255.255.255.255/0/0)
   current_peer 192.0.2.9 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 80, #pkts encrypt:80, #pkts digest: 80
    #pkts decaps: 80, #pkts decrypt: 80, #pkts verify: 80
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
    #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
    #pkts invalid prot (recv) 0, #pkts verify failed: 0
    #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
    #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
    ##pkts replay failed (rcv): 0
    #pkts tagged (send): 0, #pkts untagged (rcv): 0
    #pkts not tagged (send): 0, #pkts not untagged (rcv): 0
    #pkts internal err (send): 0, #pkts internal err (recv) 0

     local crypto endpt.: 192.0.2.6, remote crypto endpt.: 192.0.2.9
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Vlan15
     current outbound spi: 0xB546157A(3041269114)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x350925BC(889791932)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 838, flow_id: 838, sibling_flags FFFFFFFF80000040, crypto map:
ikev2-cryptomap
        sa timing: remaining key lifetime (k/sec): (4287660676/2560)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:
```

```
     outbound esp sas:
      spi: 0xB546157A(3041269114)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 837, flow_id: 837, sibling_flags FFFFFFFF80000040, crypto map:
ikev2-cryptomap
        sa timing: remaining key lifetime (k/sec): (4287660672/2560)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```



CHAPTER 75

MAC Filtering

- MAC Filtering, on page 663
- Configuring MAC Filtering for Local Authentication (CLI), on page 664
- Configuring MAC Filtering (GUI), on page 666
- Configuring MAB for External Authentication (CLI), on page 666

MAC Filtering

You can configure the controller to authorize clients based on the client MAC address by using the MAC filtering feature.

When MAC filtering is enabled, the controller uses the MAC address as the client identity. The authentication server has a database of client MAC addresses that are allowed network access. The controller sends the authentication server a RADIUS-access/request frame with a username and password based on the client MAC address as soon as it gets the association request from the client. If authorization succeeds, the controller sends a successful association response to the client. If authorization fails, the controller rejects the client association.

Clients that were authorized with MAC filtering can be re-authenticated through the WLAN session timeout feature.

MAC Filtering Configuration Guidelines

- MAC filtering authentication occurs at the 802.11 association phase and delays the association response until authentication is done. If you use a RADIUS server for MAC filtering, it is advised to keep a low latency between the controller and the RADIUS server. When latency is too high, the client might timeout while waiting for the association response.
- MAC filtering can be combined with other authentication methods such as 802.1X, Pre-Shared Key or it can be used alone.
- MAC addresses can be spoofed and MAC filtering does not consist in a security measure.
- Many clients can use a private MAC address to connect and change it at every session, therefore making it harder to identify devices through their MAC address.

Note If wlan-profile-name is configured for a user, guest user authentication is allowed only from that WLAN.

If wlan-profile-name is not configured for a user, guest user authentication is allowed on any WLAN.

If you want the client to connect to SSID1, but not to SSID2 using mac-filtering, ensure that you configure **aaa-override** in the policy profile.

In the following example, when a client with MAC address 1122.3344.0001 tries to connect to a WLAN, the request is sent to the local RADIUS server, which checks the presence of the client MAC address in its attribute list (FILTER_1 and FILTER_2). If the client MAC address is listed in an attribute list (FILTER_1), the client is allowed to join the WLAN (WLAN_1) that is returned as *ssid attribute* from the RADIUS server. The client is rejected, if the client MAC address is not listed in the attribute list.

Local RADIUS Server Configuration

```
!Configures an attribute list as FILTER_2
aaa attribute list FILTER_2
!Defines an attribute type that is to be added to an attribute list.
attribute type ssid "WLAN_2"

!Username with the MAC address is added to the filter
username 1122.3344.0002 mac aaa attribute list FILTER_2

!
aaa attribute list FILTER_1
attribute type ssid "WLAN_1"
username 1122.3344.0001 mac aaa attribute list FILTER_1
```

Controller Configuration

```
! Sets authorization to the local radius server
aaa authorization network MLIST_MACFILTER local

!A WLAN with the SSID WLAN_2 is created and MAC filtering is set along with security
parameters.
wlan WLAN_2 2 WLAN_2
mac-filtering MLIST_MACFILTER
no security wpa
no security wpa wpa2 ciphers

!WLAN with the SSID WLAN_1 is created and MAC filtering is set along with security parameters.
wlan WLAN_1 1 WLAN_1
mac-filtering MLIST_MACFILTER
no security wpa
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
security web-auth
security web-auth authentication-list WEBAUTH

! Policy profile to be associated with the above WLANs
wireless profile policy MAC_FILTER_POLICY
aaa-override
vlan 504
no shutdown
```

Configuring MAC Filtering for Local Authentication (CLI)

Follow the procedure given below to configure MAB for local authentication.

Before you begin

Configure AAA local authentication.

Configure the username for WLAN configuration (local authentication) using **username** *mac-address* **mac** command.

Note The mac-address must be in the following format: *abcdabcdabcd*

Procedure

	Command or Action	Purpose
Step 1	**wlan** *profile-name wlan-id* **Example:** `wlan CR1_SSID_mab-local-default 1 CR1_SSID_mab-local-default`	Specifies the WLAN name and ID.
Step 2	**mac-filtering default** **Example:** `Device(config-wlan)# mac-filtering default`	Sets MAC filtering support for the WLAN.
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA secuirty.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 6	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 7	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring MAC Filtering (GUI)

Before you begin

Configure AAA external authentication.

Procedure

Step 1 Choose **Configuration** > **Wireless** > **WLANs**.
Step 2 On the **Wireless Networks** page, click the name of the WLAN.
Step 3 In the **Edit WLAN** window, click the **Security** tab.
Step 4 In the **Layer2** tab, check the **MAC Filtering** check box to enable the feature.
Step 5 With MAC Filtering enabled, choose the **Authorization List** from the drop-down list.
Step 6 Save the configuration.

Configuring MAB for External Authentication (CLI)

Follow the procedure given below to configure MAB for external authentication.

Before you begin

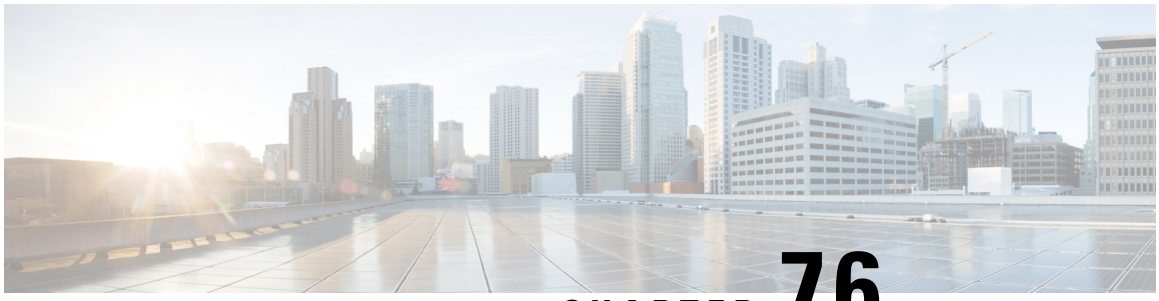
Configure AAA external authentication.

Procedure

	Command or Action	Purpose
Step 1	**wlan** *wlan-name wlan-id ssid-name* **Example:** `wlan CR1_SSID_mab-ext-radius 3 CR1_SSID_mab-ext-radius`	Specifies the WLAN name and ID.
Step 2	**mac-filtering** *list-name* **Example:** `Device(config-wlan)# mac-filtering ewlc-radius`	Sets the MAC filtering parameters. Here, *ewlc-radius* is an example for the *list-name*
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA secuirty.
Step 4	**no security wpa akm dot1x** **Example:**	Disables security AKM for dot1x.

	Command or Action	Purpose
	`Device(config-wlan)# no security wpa akm dot1x`	
Step 5	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 6	**mab request format attribute** {**1 groupsize** *size* **separator** *separator* [**lowercase** | **uppercase**] | **2** {**0** | **7** | **LINE**} **LINE** *password* | **32 vlan access-vlan**} **Example:** `Device(config)# mab request format attribute 1 groupsize 4 separator`	Optional. Configures the delimiter while using MAC filtering in a WLAN. Here, **1**- Specifies the username format used for MAB requests. **groupsize** *size*- Specifies the number of hex digits per group. The valid values range from 1 to 12. **separator** *separator*- Specifies how to separate groups. The separators are comma, semicolon, and full stop. **lowercase**- Specifies the username in lowercase format. **uppercase**- Specifies the username in uppercase format. **2**- Specifies the global password used for all the MAB requests. **0**- Specifies the unencrypted password. **7**- Specifies the hidden password. **LINE**- Specifies the encrypted or unencrypted password. *password*- LINE password. **32**- Specifies the NAS-Identifier attribute. **vlan**- Specifies a VLAN. **access-vlan**- Specifies the configured access VLAN.
Step 7	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 8	**no shutdown** **Example:**	Enables the WLAN.

	Command or Action	Purpose
	`Device(config-wlan)# no shutdown`	



CHAPTER 76

IP Source Guard

- Information About IP Source Guard, on page 669
- Configuring IP Source Guard (GUI), on page 669
- Configuring IP Source Guard, on page 670

Information About IP Source Guard

IP Source Guard (IPSG) is a Layer 2 security feature in the Cisco Catalyst 9800 Series Wireless Controller . It supports both IPv4 and IPv6 wireless clients.

The IPSG feature prevents the wireless controller from forwarding the packets, with the source IP addresses that are not known to it. This security feature is not enabled by default and has to be explicitly configured. It is enabled on a per WLAN basis, and all the wireless clients joining that WLAN inherits this feature.

The wireless controller maintains an IP/MAC pair binding table for the IPSG feature. Using this table, the wireless controller keeps track of IP and MAC address combination (binding) information for all the wireless clients. This binding information is captured as part of the IP learning process. When the feature is enabled on a WLAN, the wireless controller forwards the incoming packets (from the wireless clients) only if it finds a matching binding table entry corresponding to the source IP and MAC address combination of those packets. Otherwise, the packets are dropped.

Configuring IP Source Guard (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click the WLAN.

Step 3 In the **Advanced** tab, check the **IP Source Guard** checkbox.

Step 4 Click **Update & Apply to Device**.

Configuring IP Source Guard

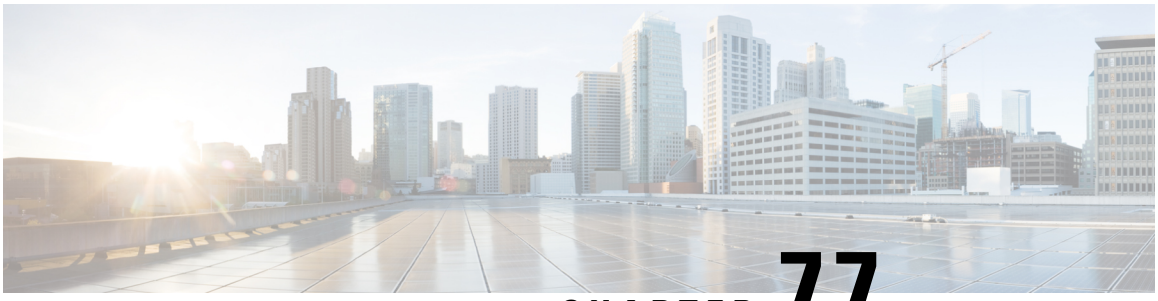
Follow the procedure given below to configure IPSG:

Before you begin

Cisco Catalyst 9800 Series Wireless Controller supports only one IPv4 address for a client and up to 8 IPv6 addresses (including link local addresses) per client.

Procedure

	Command or Action	Purpose
Step 1	**wlan** *profile-name wlan-id ssid* **Example:** `Device(config)# wlan mywlan 34 mywlan-ssid`	Specifies the WLAN name and ID to use. **Note** If a WLAN is not already configured, this step creates the WLAN.
Step 2	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Disables the WLAN.
Step 3	**ip verify source mac-check** **Example:** `Device(config-wlan)# ip verify source mac-check`	Enables the IP Source Guard feature.
Step 4	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.



CHAPTER 77

Managing Rogue Devices

- Rogue Detection, on page 671
- Rogue Location Discovery Protocol (RLDP), on page 681
- Rogue Detection Security Level, on page 687
- Setting Rogue Detection Security-level , on page 688
- Wireless Service Assurance Rogue Events, on page 689

Rogue Detection

Rogue Devices

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain-text or other denial-of-service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of Clear to Send (CTS) frames. This action mimics an access point, informing a particular client to transmit, and instructing all the other clients to wait, which results in legitimate clients being unable to access network resources. Wireless LAN service providers have a strong interest in banning rogue access points from the air space.

Because rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad hoc wireless networks without their IT department's knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. There is an increased chance of enterprise security breach when wireless users connect to access points in the enterprise network.

The following are some guidelines to manage rogue devices:

- The access points are designed to serve associated clients. These access points spend relatively less time performing off-channel scanning: about 50 milliseconds on each channel. If you want to detect a large number of rogue APs and clients with high sensitivity, a monitor mode access point must be used. Alternatively, you can reduce the scan intervals from 180 seconds to a lesser value, for example, 120 or 60 seconds, ensuring that the radio goes off-channel more frequently, which improves the chances of rogue detection. However, the access point continues to spend about 50 milliseconds on each channel.

- Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect many rogue devices.
- Client card implementation might mitigate the effectiveness of containment. This normally happens when a client might quickly reconnect to the network after receiving a "de-association/de-authentication" frame, so it might still be able to pass some traffic. However, the browsing experience of the rogue client would be badly affected when it is contained.
- It is possible to classify and report rogue access points by using rogue states and user-defined classification rules that enable rogues to automatically move between states.
- Each controller limits the number of rogue containments to three and six per radio for access points in the monitor mode.
- When manual containment is performed using configuration, the rogue entry is retained even after the rogue entry expires.
- When a rogue entry expires, the managed access points are instructed to stop any active containment on it.
- To validate a Rogue Client against AAA, add the rogue client MAC to the AAA user-database with relevant delimiter, username, and password being the MAC address with relevant delimiter. The Access-Accept contains the Cisco-AV-pair with one of the following keywords:

  rogue-ap-state=*state*

Note Here, **state** can be of three types, namely: alert, threat, and contain.

For instance, **rogue-ap-state**=*threat*.

If Access-Accept has no AV-Pair rogue-ap-class or an invalid value of rogue-ap-class, such a rogue client state is set to either of the following:

- Contained, if the config is set to autocontain clients or untrusted AP.
- Threat

The Radius Access-Reject for rogue client AAA validation is ignored.

- When Validate Rogue Clients Against AAA is enabled, the controller requests the AAA server for rogue client validation only once. As a result, if rogue client validation fails on the first attempt then the rogue client will not be detected as a threat any more. To avoid this, add the valid client entries in the authentication server before enabling Validate Rogue Clients Against AAA.

Restrictions on Rogue Detection

- Rogue containment is not supported on DFS channels.

A rogue access point is moved to a contained state either automatically or manually. The controller selects the best available access point for containment and pushes the information to the access point. The access point stores the list of containments per radio. For auto containment, you can configure the controller to use only the monitor mode access point. The containment operation occurs in the following two ways:

- The container access point goes through the list of containments periodically and sends unicast containment frames. For rogue access point containment, the frames are sent only if a rogue client is associated.
- Whenever a contained rogue activity is detected, containment frames are transmitted.

Individual rogue containment involves sending a sequence of unicast disassociation and deauthentication frames.

Cisco Prime Infrastructure Interaction and Rogue Detection

Cisco Prime Infrastructure supports rule-based classification and uses the classification rules configured on the controller. The controller sends traps to Cisco Prime Infrastructure after the following events:

- If an unknown access point moves to the Friendly state for the first time, the controller sends a trap to Cisco Prime Infrastructure only if the rogue state is Alert. It does not send a trap if the rogue state is Internal or External.
- If a rogue entry is removed after the timeout expires, the controller sends a trap to Cisco Prime Infrastructure for rogue access points that are categorized as Malicious (Alert, Threat) or Unclassified (Alert). The controller does not remove rogue entries with the following rogue states: Contained, Contained Pending, Internal, and External.

AP Impersonation Detection

The various methods to detect AP impersonation are:

- AP impersonation can be detected if a managed AP reports itself as Rogue. This method is always enabled and no configuration is required.
- AP impersonation detection is based on MFP.

Infrastructure MFP protects 802.11 session management functions by adding message integrity check (MIC) information elements, to the management frames sent by APs (and not those sent by clients), which are then validated by other APs in the network. If infrastructure MFP is enabled, the managed APs check if the MIC information elements are present and if MIC information elements are as expected. If either of these conditions is not fulfilled, the managed AP sends rogue AP reports with updated AP authentication failure counter.

Note Ensure that the **ccx aironet-iesupport** command is run in all the WLAN procedures, else the BSSID will be detected as a rogue.

For AP impersonation detection, Network Time Protocol (NTP) must be enabled instead of CAPWAP based time, under the AP profile.

Configuring Rogue Detection (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 Click the **AP Join Profile Name** to edit the AP join profile properties.

Step 3 In the **Edit AP Join Profile** window, click the **Rogue AP** tab.

Step 4 Check the **Rogue Detection** check box to enable rogue detection.

Step 5 In the **Rogue Detection Minimum RSSI** field, enter the RSSI value.

Step 6 In the **Rogue Detection Transient Interval** field, enter the interval in seconds.

Step 7 In the **Rogue Detection Report Interval** field, enter the report interval value in seconds.

Step 8 In the **Rogue Detection Client Number Threshold** field, enter the threshold for rogue client detection.

Step 9 Check the **Auto Containment on FlexConnect Standalone** check box to enable auto containment.

Step 10 Click **Update & Apply to Device**.

Configuring Rogue Detection (CLI)

Procedure

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

Step 2	**ap profile** *profile-name* **rogue detection min-rssi** *rssi in dBm*
	Example:
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection min-rssi -100`
		Specify the minimum RSSI value that rogues should have for APs to detect and for rogue entry to be created in the device.
		Valid range for the rssi in dBm parameter is –128 dBm to -70 dBm, and the default value is -128 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 3	**ap profile** *profile-name* **rogue detection containment** {**auto-rate** | **flex-rate**}
	Example:
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection containment flex-rate`
		Specifies the rogue containment options. The **auto-rate** option enables auto-rate for containment of rogues. The **flex-rate** option enables rogue containment of standalone flexconnect APs.

	Command or Action	Purpose

Step 4	**ap profile** *profile-name* **rogue detection enable**
	Example:
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection enable`
		Enables rogue detection on all APs.

Step 5	**ap profile** *profile-name* **rogue detection report-interval** *time in seconds*
	Example:
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection report-interval 120`
		Configures rogue report interval for monitor mode Cisco APs.
		The valid range for reporting the interval in seconds is 10 seconds to 300 seconds.

Configuring RSSI Deviation Notification Threshold for Rogue APs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps rogue ap notify-rssi-deviation** **Example:** `Device(config)# wireless wps rogue ap notify-rssi-deviation`	Configures RSSI deviation notification threshold for Rogue APs.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Management Frame Protection (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Wireless Protection Policies**.

Step 2 In the **Rogue Policy** tab, under the **MFP Configuration** section, check the **Global MFP State** check box and the **AP Impersonation Detection** check box to enable the global MFP state and the AP impersonation detection, respectively.

Step 3 In the **MFP Key Refresh Interval** field, specify the refresh interval in hours.

Step 4 Click **Apply**.

Configuring Management Frame Protection (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps mfp** **Example:** `Device(config)# wireless wps mfp`	Configures a management frame protection.

Step 3	**wireless wps mfp** {**ap-impersonation** | **key-refresh-interval**}
	Example:
	`Device(config)# wireless wps mfp ap-impersonation`
	`Device(config)# wireless wps mfp key-refresh-interval`
		Configures ap impersonation detection (or) MFP key refresh interval in hours.
		key-refresh-interval—Refers to the MFP key refresh interval in hours. The valid range is from 1 to 24. Default value is 24.

Step 4	**end** **Example:** `Device(config)# end`	Saves the configuration and exits configuration mode and returns to privileged **EXEC** mode.

Verifying Management Frame Protection

To verify if the Management Frame Protection (MFP) feature is enabled or not, use the following command:

```
Device# show wireless wps summary
Client Exclusion Policy
  Excessive 802.11-association failures   : unknown
  Excessive 802.11-authentication failures: unknown
  Excessive 802.1x-authentication         : unknown
  IP-theft                                : unknown
  Excessive Web authentication failure    : unknown
  Failed Qos Policy                       : unknown

Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

To view the MFP details, use the following command:

```
Device# show wireless wps mfp summary
Management Frame Protection
```

```
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

Verifying Rogue Events

To verify the rogue event history, run the **show wireless wps rogue ap detailed** command:

```
Device# show wireless wps rogue ap detailed d8b1.901c.3cfd

Rogue Event history

Timestamp                  #Times Class/State Event               Ctx
 RC
-------------------------- ------ ----------- ------------------- ------------------------
 ---
05/01/2020 08:37:03.55645  41616  Mal/CPend   FSM_GOTO            ContPending(NotContYet)
 0x0
05/01/2020 08:37:03.55427  28163  Mal/CPend   EXPIRE_TIMER_START  1200s
 0x0
05/01/2020 08:37:03.55380  28163  Mal/CPend   RECV_REPORT         38ed.18cf.83e0/1
 0x0
05/01/2020 08:36:54.659136 7356   Mal/CPend   NO_OP_UPDATE
 0x0
05/01/2020 08:36:33.347132 3185   Mal/CPend   CHANNEL_CHANGE      e4aa.5d44.fec0/2,36->40
 0x0
05/01/2020 08:25:19.573720 247    Mal/CPend   LRAD_EXPIRE         7c21.0e41.0700/0
 0x0
04/30/2020 07:55:37.977450 2      Mal/CPend   PMF_CONTAINMENT  ContPending(PMFDetected) 0x0
04/30/2020 07:55:37.977242 1      Unc/Alert   INIT_TIMER_DONE     0xab9800439e00024f
 0x0
04/30/2020 07:52:33.600332 1      Unk/Init    INIT_TIMER_START    180s
 0x0
04/30/2020 07:52:33.600326 1      Unk/Init    CREATE
 0x0
```

To verify the impersonations detected due to authentication errors, use the following command:

```
Device# show wireless wps rogue ap detailed

Rogue BSSID                             : 0062.ecf3.8d30
Last heard Rogue SSID                   : rogueA
802.11w PMF required                    : No
Is Rogue an impersonator                : Yes
Is Rogue on Wired Network               : No
Classification                          : Malicious
Manually Contained                      : No
State                                   : Threat
First Time Rogue was Reported           : 01/07/2020 15:51:01
Last Time Rogue was Reported            : 01/08/2020 08:08:35

Number of clients                       : 0

Reported By
  AP Name : AP38ED.18CE.45E0
    MAC Address                         : 38ed.18cf.83e0
    Detecting slot ID                   : 0
    Radio Type                          : dot11g, dot11n - 2.4 GHz
    SSID                                : rogueA
    Channel                             : 6 (From DS)
    Channel Width                       : 20 MHz
```

```
RSSI                                : -33 dBm
SNR                                 : 52 dB
ShortPreamble                       : Disabled
Security Policy                     : WPA2/WPA/FT
Last reported by this AP            : 01/08/2020 08:02:53
Authentication Failure Count        : 237
```

Verifying Rogue Detection

This section describes the new command for rogue detection.

The following command can be used to verify rogue detection on the device.

Table 17: Verifying Adhoc Rogues Information

Command	Purpose
show wireless wps rogue adhoc detailed *mac_address*	Displays the detailed information for an Adhoc rogue.
show wireless wps rogue adhoc summary	Displays a list of all Adhoc rogues.

Table 18: Verifying Rogue AP Information

Command	Purpose
show wireless wps rogue ap clients *mac_address*	Displays the list of all rogue clients associated with a rogue.
show wireless wps rogue ap custom summary	Displays the custom rogue AP information.
show wireless wps rogue ap detailed *mac_address*	Displays the detailed information for a rogue AP.
show wireless wps rogue ap friendly summary	Displays the friendly rogue AP information.
show wireless wps rogue ap list *mac_address*	Displays the list of rogue APs detected by a given AP.
show wireless wps rogue ap malicious summary	Displays the malicious rogue AP information.
show wireless wps rogue ap summary	Displays a list of all Rogue APs.
show wireless wps rogue ap unclassified summary	Displays the unclassified rogue AP information.

Table 19: Verifying Rogue Auto-Containment Information

Command	Purpose
show wireless wps rogue auto-contain	Displays the rogue auto-containment information.

Table 20: Verifying Classification Rule Information

Command	Purpose

show wireless wps rogue rule detailed *rule_name*	Displays the detailed information for a classification rule.
show wireless wps rogue rule summary	Displays the list of all rogue rules.

Table 21: Verifying Rogue Statistics

Command	Purpose
show wireless wps rogue stats	Displays the rogue statistics.

Table 22: Verifying Rogue Client Information

Command	Purpose
show wireless wps rogue client detailed *mac_address*	Displays detailed information for a Rogue client.
show wireless wps rogue client summary	Displays a list of all the Rogue clients.

Table 23: Verifying Rogue Ignore List

Command	Purpose
show wireless wps rogue ignore-list	Displays the rogue ignore list.

Examples: Rogue Detection Configuration

This example shows how to configure the minimum RSSI that a detected rogue AP needs to be at, to have an entry created in the device:

```
Device# configure terminal
Device(config)# ap profile profile1
Device(config)# rogue detection min-rssi -100
Device(config)# end
Device# show wireless wps rogue client summary/show wireless wps rogue ap summary
```

This example shows how to configure the classification interval:

```
Device# configure terminal
Device(config)# ap profile profile1
Device(config)# rogue detection min-transient-time 500
Device(config)# end
Device# show wireless wps rogue client summary/show wireless wps rogue ap summary
```

Configuring Rogue Policies (GUI)

Procedure

Step 1 Choose **Configuration > Security > Wireless Protection Policies**.

Step 2 In the **Rogue Policies** tab, use the **Rogue Detection Security Level** drop-down to select the security level.

Step 3 In the **Expiration timeout for Rogue APs (seconds)** field, enter the timeout value.

Step 4 Select the **Validate Rogue Clients against AAA** check box to validate rogue clients against AAA server.

Step 5 Select the **Validate Rogue APs against AAA** check box to validate rogue access points against AAA server.

Step 6 In the **Rogue Polling Interval (seconds)** field, enter the interval to poll the AAA server for rogue information.

Step 7 Select the **Detect and Report Adhoc Networks** check box to enable detection of rogue adhoc networks.

Step 8 In the **Rogue Detection Client Number Threshold** field, enter the threshold to generate SNMP trap.

Step 9 In the **Auto Contain** section, enter the following details.

Step 10 Use the **Auto Containment Level** drop-down to select the level.

Step 11 Select the **Auto Containment only for Monitor Mode APs** check box to limit the auto-containment only to monitor mode APs.

Step 12 Select the **Rogue on Wire** check box to limit the auto-containment only to rogue APs on wire.

Step 13 Select the **Using our SSID** check box to limit the auto-containment only to rogue APs using one of the SSID configured on the controller.

Step 14 Select the **Adhoc Rogue AP** check box to limit the auto-containment only to adhoc rogue APs.

Step 15 Click **Apply**.

Configuring Rogue Policies (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**Example:** `Device(config)# wireless wps rogue security-level custom`	Configures the rogue detection security level. You can select **critical** for highly sensitive deployments, **custom** for customizable security level, **high** for medium-scale deployments, and **low** for small-scale deployments.
Step 3	**wireless wps rogue ap timeout** *number of seconds* **Example:**	Configures the expiration time for rogue entries, in seconds. Valid range for the time in seconds 240 seconds to 3600 seconds.

	Command or Action	Purpose
	`Device(config)# wireless wps rogue ap timeout 250`	
Step 4	**Example:** `Device(config)# wireless wps rogue client aaa`	Configures the use of AAA or local database to detect valid MAC addresses.
Step 5	**Example:** `Device(config)# wireless wps rogue client mse`	Configures the use of MSE to detect valid MAC addresses.
Step 6	**wireless wps rogue client notify-min-rssi** *RSSI threshold* **Example:** `Device(config)# wireless wps rogue client notify-min-rssi -128`	Configures the minimum RSSI notification threshold for rogue clients. Valid range for the RSSI threshold in dB is -128 - dB to -70 dB.
Step 7	**wireless wps rogue client notify-min-deviation** *RSSI threshold* **Example:** `Device(config)# wireless wps rogue client notify-min-deviation 4`	Configures the RSSI deviation notification threshold for rogue clients. Valid range for the RSSI threshold in dB is 0 dB to 10 dB.
Step 8	**wireless wps rogue ap aaa polling-interval** *AP AAA Interval* **Example:** `Device(config)# wireless wps rogue ap aaa polling-interval 120`	Configures rogue AP AAA validation interval. The valid range for the AP AAA interval in seconds is 60 seconds to 86400 seconds.
Step 9	**wireless wps rogue adhoc** **Example:** `Device(config)# wireless wps rogue adhoc`	Enables detecting and reporting adhoc rogue (IBSS).
Step 10	**wireless wps rogue client client-threshold** *threshold* **Example:** `Device(config)# wireless wps rogue client client-threshold 100`	Configures the rogue client per a rogue AP SNMP trap threshold. The valid range for the threshold is 0 to 256.

Rogue Location Discovery Protocol (RLDP)

Rogue Location Discovery Protocol

Rogue Location Discovery Protocol (RLDP) is an active approach, which is used when rogue AP has no authentication (Open Authentication) configured. This mode, which is disabled by default, instructs an active AP to move to the rogue channel and connect to the rogue as a client. During this time, the active AP sends

de-authentication messages to all connected clients and then shuts down the radio interface. Then, it associates to the rogue AP as a client. The AP then tries to obtain an IP address from the rogue AP and forwards a User Datagram Protocol (UDP) packet (port 6352) that contains the local AP and rogue connection information to the controller through the rogue AP. If the controller receives this packet, the alarm is set to notify the network administrator that a rogue AP was discovered on the wired network with the RLDP feature. RLDP has 100 % accuracy in rouge AP detection. It detects Open APs and NAT APs.

Following are some guidelines to manage RLDP:

- Rogue Location Discovery Protocol (RLDP) detects rogue access points that are configured for open authentication.
- RLDP detects rogue access points that use a broadcast Basic Service Set Identifier (BSSID), that is, the access point broadcasts its Service Set Identifier in beacons.
- RLDP detects only those rogue access points that are on the same network. If an access list in the network prevents the sending of RLDP traffic from the rogue access point to the controller , RLDP does not work.
- RLDP does not work on 5-GHz Dynamic Frequency Selection (DFS) channels.
- If RLDP is enabled on mesh APs, and the APs perform RLDP tasks, the mesh APs are dissociated from the controller . The workaround is to disable RLDP on mesh APs.
- If RLDP is enabled on non-monitor APs, client connectivity outages occur when RLDP is in process.

The following steps describe the functioning of RLDP:

1. Identify the closest Unified AP to the rogue using signal strength values.
2. The AP then connects to the rogue as a WLAN client, attempting three associations before timing out.
3. If association is successful, the AP then uses DHCP to obtain an IP address.
4. If an IP address was obtained, the AP (acting as a WLAN client) sends a UDP packet to each of the controller 's IP addresses.
5. If the controller receives even one of the RLDP packets from the client, that rogue is marked as on-wire.

Note The RLDP packets are unable to reach the controller if filtering rules are placed between the controller 's network and the network where the rogue device is located.

The controller continuously monitors all the nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP), if RLDP is enabled, to determine if the rogue is attached to your network.

Controller initiates RLDP on rogue devices that have open authentication. If RLDP uses FlexConnect or local mode access points, then clients are disconnected for that moment. After the RLDP cycle, the clients are reconnected to the access points. As and when rogue access points are seen (auto-configured), the RLDP process is initiated.

You can configure the controller to use RLDP on all the access points or only on the access points configured for the monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded radio frequency (RF) space, allowing monitoring without creating unnecessary interference and without affecting the regular data access point functionality. If you configure the controller to use RLDP on

all the access points, the controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to contain the detected rogue either manually or automatically.

RLDP detects on wire presence of the rogue access points that are configured with open authentication only once, which is the default retry configuration. Retries can be configured using the **wireless wps rogue ap rldp retries** configuration CLI.

You can initiate or trigger RLDP from controller in three ways:

1. Enter the RLDP initiation command manually from the controller CLI.

   wireless wps rogue ap mac-address *mac-address* **rldp initiate**

2. Schedule RLDP from the controller configuration CLI.

   wireless wps rogue ap rldp schedule

3. Auto RLDP. You can configure auto RLDP on controller either from controller CLI or GUI but keep in mind the following guidelines:

   - The auto RLDP option can be configured only when the rogue detection security level is set to custom.
   - Either auto RLDP or schedule of RLDP can be enabled at a time.

Restrictions for RLDP

- RLDP only works with open rogue APs broadcasting their SSID with authentication and encryption disabled.
- RLDP requires that the Managed AP acting as a client is able to obtain an IP address via DHCP on the rogue network.
- Manual RLDP can be used to attempt an RLDP trace on a rogue multiple number of times.
- During RLDP process, the AP is unable to serve clients. This negatively impacts performance and connectivity for local mode APs. To avoid this case, RLDP can be selectively enabled for Monitor Mode AP only.
- RLDP does not attempt to connect to a rogue AP operating in a 5GHz DFS channel.
- RLDP is supported only on Cisco IOS APs.

Configuring RLDP for Generating Alarms (GUI)

Procedure

Step 1 Choose **Configuration > Security > Wireless Protection Policies**.

Step 2 In the **RLDP** tab, use the **Rogue Location Discovery Protocol** drop-down to select one of the following options:

a) **Disable**: Disables RLDP on all the access points. **Disable** is the default option.
b) **All APs**: Enables RLDP on all APs.
c) **Monitor Mode APs**: Enables RLDP only on APs in the monitor mode.

Note The **Schedule RLDP** check box is enabled only if the **Disable** option is selected. The Schedule RLDP check box remains disabled when you select the **All APs** option or the **Monitor Mode APs** option.

Step 3 In the **Retry Count** field, specify the number of retries that should be attempted. The range allowed is between 1 and 5.

Step 4 Click **Apply**.

Configuring an RLDP for Generating Alarms (CLI)

Procedure

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

Step 2	**wireless wps rogue ap rldp alarm-only <monitor-ap-only>**
	Example:
	`Device(config)# wireless wps rogue ap rldp alarm-only`
	`Device(config)# wireless wps rogue ap rldp alarm-only monitor-ap-only`
		Enables RLDP to generate alarms. In this method, the RLDP is always enabled.
		The **monitor-ap-only** keyword is optional.
		The command with just the **alarm-only** keyword enables RLDP without any restriction on the AP mode.
		The command with **alarm-only <monitor-ap-only>** keyword enables RLDP in monitor mode access points only.

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

Configuring a Schedule for RLDP (GUI)

Procedure

Step 1 Choose **Configuration > Security > Wireless Protection Policies**.

Step 2 In the **RLDP** tab, choose the following options from the **Rogue Location Discovery Protocol** drop-down list:

- **Disable (default)**: Disables RLDP on all the access points.

Step 3 In the Retry Count field, specify the number of retries that should be attempted. Provide a valid range between 1 to 5.

Step 4 Check the **Schedule RLDP** check box and then specify the days, start time, and end time for the process to take place.

Step 5 Click **Apply**.

Configuring a Schedule for RLDP (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps rogue ap rldp schedule day** *day* **start** *start-time* **end** *end-time* **Example:** `Device(config)# wireless wps rogue ap rldp schedule day Monday start 10:10:01 end 12:00:00`	Enables RLDP based on a scheduled day, start time, and end time. Here, *day* is the day when the RLDP scheduling can be done. The values are Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. *start-time* is the start time for scheduling RLDP for the day. You need to enter start time in **HH:MM:SS** format. *end-time* is the end time for scheduling RLDP for the day. You need to enter end time in **HH:MM:SS** format.
Step 3	**wireless wps rogue ap rldp schedule** **Example:** `Device(config)# wireless wps rogue ap rldp schedule`	Enables the schedule.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring an RLDP for Auto-Contain (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Wireless Protection Policies**.

Step 2 In the **Rogue Policies** tab, under the **Auto Contain** section, check the **Rogue on Wire** checkbox.

Step 3 Click **Apply**.

Configuring an RLDP for Auto-Contain (CLI)

Procedure

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

Step 2	**wireless wps rogue ap rldp auto-contain** [**monitor-ap-only**]
	Example:
	`Device(config)# wireless wps rogue ap rldp auto-contain`
	`Device(config)# wireless wps rogue ap rldp auto-contain monitor-ap-only`
		Enables RLDP to perform auto-contain. In this method, the RLDP is always enabled.
		The **monitor-ap-only** keyword is optional.
		The command with just the **auto-contain** keyword enables RLDP without any restriction on the AP mode.
		The command with **auto-contain <monitor-ap-only>** keyword enables RLDP in monitor mode access points only.

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

Configuring RLDP Retry Times on Rogue Access Points (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Wireless Protection Policies**.

Step 2 On the **Wireless Protection Policies** page, click the **RLDP** tab.

Step 3 Enter the RLDP retry attempt value for rogue access points in the **Retry Count** field.

The valid range is between 1 and 5.

Step 4 Save the configuration.

Configuring RLDP Retry Times on Rogue Access Points (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps rogue ap rldp retries** *num-entries* **Example:** `Device(config)# wireless wps rogue ap rldp retries 2`	Enables RLDP retry times on rogue access points. Here, *num-entries* is the number of RLDP retry times for each of the rogue access points. The valid range is 1 to 5.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Rogue AP RLDP

The following commands can be used to verify rogue AP RLDP:

Table 24: Verifying Rogue AP Information

Command	Purpose
show wireless wps rogue ap rldp detailed *mac_address*	Displays the RLDP details for a rogue AP.
show wireless wps rogue ap rldp in progress	Displays the list of in-progress RLDP.
show wireless wps rogue ap rldp summary	Displays the summary of RLDP scheduling information.

Rogue Detection Security Level

The rogue detection security level configuration allows you to set rogue detection parameters.

The available security levels are:

- Critical: Basic rogue detection for highly sensitive deployments.
- High: Basic rogue detection for medium-scale deployments.
- Low: Basic rogue detection for small-scale deployments.
- Custom: Default security-level, where all detection parameters are configurable.

Note When in Critical, High or Low, some rogue parameters are fixed and cannot be configured.

The following table shows parameter details for the three predefined levels:

Table 25: Rogue Detection: Predefined Levels

Parameter	Critical	High	Low
Cleanup Timer	3600	1200	240
AAA Validate Clients	Disabled	Disabled	Disabled
Adhoc Reporting	Enabled	Enabled	Enabled
Monitor-Mode Report Interval	10 seconds	30 seconds	60 seconds
Minimum RSSI	-128 dBm	-80 dBm	-80 dBm
Transient Interval	600 seconds	300 seconds	120 seconds
Auto Contain Works only on Monitor Mode APs.	Disabled	Disabled	Disabled
Auto Contain Level	1	1	1
Auto Contain Same-SSID	Disabled	Disabled	Disabled
Auto Contain Valid Clients on Rogue AP	Disabled	Disabled	Disabled
Auto Contain Adhoc	Disabled	Disabled	Disabled
Containment Auto-Rate	Enabled	Enabled	Enabled
Validate Clients with CMX	Enabled	Enabled	Enabled
Containment FlexConnect	Enabled	Enabled	Enabled
RLDP	Monitor-AP if RLDP scheduling is disabled.	Monitor-AP if RLDP scheduling is disabled	Disabled
Auto Contain RLDP	Disabled	Disabled	Disabled

Setting Rogue Detection Security-level

Follow the procedure given below to set the rogue detection security-level:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless wps rogue security-level custom** **Example:** `Device(config)# wireless wps rogue security-level custom`	Configures rogue detection security level as custom.
Step 3	**wireless wps rogue security-level low** **Example:** `Device(config)# wireless wps rogue security-level low`	Configures rogue detection security level for basic rogue detection setup for small-scale deployments.
Step 4	**wireless wps rogue security-level high** **Example:** `Device(config)# wireless wps rogue security-level high`	Configures rogue detection security level for rogue detection setup for medium-scale deployments.
Step 5	**wireless wps rogue security-level critical** **Example:** `Device(config)# wireless wps rogue security-level critical`	Configures rogue detection security level for rogue detection setup for highly sensitive deployments.

Wireless Service Assurance Rogue Events

Wireless Service Assurance (WSA) rogue events, supported in Release 16.12.x and later releases, consist of telemetry notifications for a subset of SNMP traps. WSA rogue events replicate the same information that is part of the corresponding SNMP trap.

For all the exported events, the following details are provided to the wireless service assurance (WSA) infrastructure:

- MAC address of the rogue AP
- Details of the managed AP and the radio that detected the rogue AP with strongest RSSI
- Event-specific data such as SSID, channel for potential honeypot event, and MAC address of the impersonating AP for impersonation event

The WSA rogue events feature can scale up to four times the maximum number of supported APs and half of the maximum number of supported clients.

The WSA rogue events feature is supported on Cisco Catalyst Center and other third-party infrastructure.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**network-assurance enable** **Example:** `Device# network-assurance enable`	Enables wireless service assurance.
Step 3	**wireless wps rogue network-assurance enable** **Example:** `Device# wireless wps rogue network-assurance enable`	Enables wireless service assurance for rogue devices. This ensures that the WSA rogue events are sent to the event queue.

Monitoring Wireless Service Assurance Rogue Events

Procedure

- **show wireless wps rogue stats**

  Example:

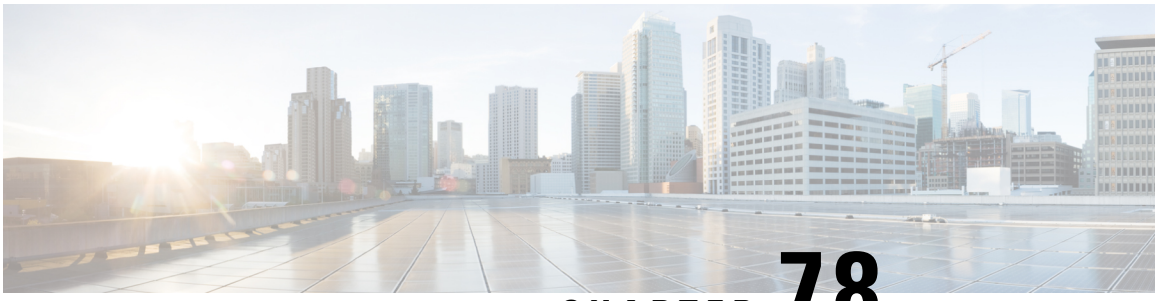
```
Device# show wireless wps rogue stats

WSA Events
  Total WSA Events Triggered            : 9
    ROGUE_POTENTIAL_HONEYPOT_DETECTED   : 2
    ROGUE_POTENTIAL_HONEYPOT_CLEARED    : 3
    ROGUE_AP_IMPERSONATION_DETECTED     : 4
  Total WSA Events Enqueued             : 6
    ROGUE_POTENTIAL_HONEYPOT_DETECTED   : 1
    ROGUE_POTENTIAL_HONEYPOT_CLEARED    : 2
    ROGUE_AP_IMPERSONATION_DETECTED     : 3
```

  In this example, nine events have been triggered, but only six of them have been enqueued. This is because three events were triggered before the WSA rogue feature was enabled.

- **show wireless wps rogue stats internal**

  show wireless wps rogue ap detailed *rogue-ap-mac-addr*

  These commands show information related to WSA events into the event history.



CHAPTER 78

Classifying Rogue Access Points

- Information About Classifying Rogue Access Points, on page 691
- Guidelines and Restrictions for Classifying Rogue Access Points, on page 693
- How to Classify Rogue Access Points, on page 693
- Monitoring Rogue Classification Rules, on page 699
- Examples: Classifying Rogue Access Points, on page 699

Information About Classifying Rogue Access Points

The controller software enables you to create rules that can organize and display rogue access points as Friendly, Malicious, Custom, or Unclassified.

By default, none of the classification rules are used. You need to enable them. Therefore, all unknown access points are categorized as Unclassified. When you create or change a rule, configure conditions, and enable it, all rogue access points are then reclassified. Whenever you change a rule, it is applied to all the access points (friendly, malicious, and unclassified).

Note

- Rule-based rogue classification does not apply to ad hoc rogues and rogue clients.
- You can configure up to 64 rogue classification rules per controller .

When the controller receives a rogue report from one of its managed access points, it responds as follows:

- If the unknown access point is in the friendly MAC address list, the controller classifies the access point as Friendly.
- If the unknown access point is not in the friendly MAC address list, the controller starts applying the rogue classification rules to the access point.
- If the rogue access point is manually classsified, rogue rules are not applied to it.
- If the rogue access point matches the configured rules criteria, the controller classifies the rogue based on the classification type configured for that rule.
- If the rogue access point does not match any of the configured rules, the rogue remains unclassified.

  The controller repeats the previous steps for all the rogue access points.

- If the rogue access point is detected on the same wired network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if there are no configured rules. You can then manually contain the rogue to change the rogue state to Contained. If the rogue access point is not available on the network, the controller marks the rogue state as Alert. You can then manually contain the rogue.
- If desired, you can manually move the access point to a different classification type and rogue state.
- Before performing any classification, the rogue access points are temporarily marked as Pending.

Table 26: Classification Mapping

Rule-Based Classification Type	Rogue State
Custom	• Alert—No action is taken other than notifying the management station. The management station in the controller manages the controller and wired networks. • Contained—The unknown access point is contained. If none of the managed access points are available for containment, the rogue is in Contained Pending state.
Delete	Deletes the rogue access point.
Friendly	• Internal—If the unknown access point poses no threat to WLAN security, you can manually configure it as Friendly, Internal. An example of this would be 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 can manually configure it as Friendly, External. An example of this would be the access point in your neighboring coffee shop. • Alert—No action is taken other than notifying the management station. The management station manages the controller and wired networks.
Malicious	• Alert—No action is taken other than notifying the management station. The management station manages the controller and wired networks. • Threat—The unknown access point is found to be on the network and poses a threat to WLAN security. • Contained—The unknown access point is contained. If none of the managed access points are available for containment, the rogue is in Contained Pending state.
Unclassified	• Alert— No action is taken other than notifying the management station. The management station manages the controller and wired networks. • Contained—The unknown access point is contained. If none of the managed access points are available for containment, the rogue is in contained pending state.

As mentioned earlier, the controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules. Alternatively, you can manually move the unknown access point to a different classification type and rogue state.

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 SNMP traps are sent for containment by rule and every 30 minutes for rogue classification change.
- Rogue rules are applied on every incoming new rogue report in the controller in the order of their priority.
- After a rogue satisfies a rule and is classified, it does not move down the priority list for the same report.
- The rogue classification rules are re-evaluated at every report received by the managed access points. Hence, a rogue access point can move from one state to another, if a different rule matches the last report.
- If a rogue AP is classified as friendly or ignored, all rogue clients associated with it are not tracked.
- 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.

How to Classify Rogue Access Points

Classifying Rogue Access Points and Clients Manually (GUI)

Procedure

Step 1 Choose **Monitoring > Wireless > Rogues**.

Step 2 In the **Unclassified** tab, select an AP to view the detail in the lower pane.

Step 3 Use the **Class Type** drop-down to set the status.

Step 4 Click **Apply**.

Classifying Rogue Access Points and Clients Manually (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps rogue adhoc** {**alert** *mac-addr* | **auto-contain** | **contain** *mac-addr containment-level* | **internal** *mac-addr* | **external** *mac-addr*} **Example:** `Device(config)# wireless wps rogue adhoc alert 74a0.2f45.c520`	Detects and reports the ad hoc rogue. Enter one of these options after you enter the **adhoc** keyword: • **alert**—Sets the ad hoc rogue access point to alert mode. If you choose this option, enter the MAC address for the *mac-addr* parameter. • **auto-contain**—Sets the automatically containing ad hoc rogue to auto-contain mode. • **contain**—Sets the containing ad hoc rogue access point to contain mode. If you choose this option, enter the MAC address for the *mac-addr* parameter and containment level for the *containment-level* parameter. The valid range for *containment-level* is from 1 to 4. • **external**—Sets the ad hoc rogue access point as **external**. If you choose this option, enter the MAC address for the *mac-addr* parameter. • **internal**—Sets the ad hoc rogue access point as **internal**. If you choose this option, enter the MAC address for the *mac-addr* parameter.
Step 3	**wireless wps rogue ap** {**friendly** *mac-addr* **state** [**external** | **internal**] | **malicious** *mac-addr* **state** [**alert** | **contain** *containment-level*]} **Example:**	Configures the rogue access points. Enter one of the following options after the **ap** keyword:

	Command or Action	Purpose
	`Device(config)# wireless wps rogue ap malicious 74a0.2f45.c520 state contain 3`	• **friendly**—Configures the friendly rogue access points. If you choose this option, enter the MAC address for the *mac-addr* parameter. After that enter the **state** keyword followed by either of these options: **internal** or **external**. If you select an **internal** option, it indicates that you trust a foreign access point. If you select an **external** option, it indicates that you acknowledge the presence of a rogue access point. • **malicious**—Configures the malicious rogue access points. If you choose this option, enter the MAC address for the *mac-addr* parameter. After that enter the **state** keyword followed by either of these options: **alert** or **contain**. • **alert**—Sets the malicious rogue access point to **alert** mode. • **contain**—Sets the malicious rogue access point to **contain** mode. If you choose this option, enter the containment level for the *containment-level* parameter. The valid range is from 1 to 4.
Step 4	**wireless wps rogue client** {**contain** *mac-addr containment-level*} **Example:** `Device(config)# wireless wps rogue client contain 74a0.2f45.c520 2`	Configures the rogue clients. Enter the following option after you enter the **client** keyword: **contain**—Contains the rogue client. After you choose this option, enter the MAC address for the *mac-addr* parameter and the containment level for *containment-level* parameter. The valid range for *containment-level* is from 1 to 4.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Rogue Classification Rules (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Wireless Protection Policies**.

Step 2 In the **Wireless Protection Policies** page, choose **Rogue AP Rules** tab.

Step 3 On the **Rogue AP Rules** page, click the name of the **Rule** or click **Add** to create a new one.

Step 4 In the **Add/Edit Rogue AP Rule** window that is displayed, enter the name of the rule in the **Rule Name** field.

Step 5 Choose the rule type from the following **Rule Type** drop-down list options:

- Friendly
- Malicious
- Unclassified
- Custom

Configuring Rogue Classification Rules (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps rogue rule** *rule-name* **priority** *priority* **Example:** `Device(config)# wireless wps rogue rule rule_3 priority 3`	Creates or enables a rule. While creating a rule, you must enter the priority for the rule. **Note** After creating a rule, you can edit the rule and change the priority only for the rogue rules that are disabled. You cannot change the priority for the rogue rules that are enabled. While editing, changing the priority for a rogue rule is optional.

Step 3	**classify** {**friendly state** {**alert** | **external** | **internal**} | **malicious state** {**alert** | **contained** }}
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# classify friendly`
		Specifies the classification that needs to be applied to the rogue access points matching this rule.
		• **friendly**—Configures the friendly rogue access points. After that enter the **state** keyword followed by either of these options: **alert**, **internal**, or **external**. If you select an **internal** option, it indicates that you trust a foreign access point. If you select an **external** option, it indicates that you acknowledge the presence of a rogue access point.

	Command or Action	Purpose
		• **malicious**—Configures the malicious rogue access points. After that enter the state keyword followed by either of these options: alert or contained. • **alert**—Sets the malicious rogue access point to alert mode. • **contained**—Sets the malicious rogue access point to contained mode.

Step 4	**condition** {**client-count** *value* | **duration** *duration_value* | **encryption** | **infrastructure** | **rssi** | **ssid** *ssid_name* | **wildcard-ssid**}
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# condition client-count 5`
		Adds the following conditions to a rule, which the rogue access point must meet:
		• **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, 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 *value* parameter. The valid range is from 1 to 10 (inclusive), and the default value is 0.
		• **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 *duration_value* parameter. The valid range is from 0 to 3600 seconds (inclusive), and the default value is 0 seconds.
		• **encryption**—Requires that the advertised WLAN does not have encryption enabled. You can choose **any** for any type of encryption, **off** for no encryption, **wpa1** for WPA encryption, **wpa2** for WPA2 encryption, **wpa3-owe** for WPA3 OWE encryption, or **wpa3-sae** for WPA3 SAE encryption.
		• **infrastructure**—Requires the SSID to be known to the controller.
		• **rssi**—Requires the rogue access point to be detected with a minimum RSSI value. If the classification is Friendly, the condition requires the rogue access point

	Command or Action	Purpose
		to be detected with a maximum RSSI value. The valid range is from –95 to –50 dBm (inclusive). • **ssid**—Requires the rogue access point to have a specific SSID. You could specify up to 25 different SSIDs. You should specify an SSID that is not managed by the controller. If you choose this option, enter the SSID for the *ssid_name* parameter. The SSID is added to the configured SSID list you just created. • **wildcard-ssid**—Allows you to specify an expression that could match an SSID string. You can specify up to 25 of these SSIDs.

Step 5	**match** {**all** | **any**}
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# match all`
		Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule for the rule to be matched and the rogue access point to adopt the classification type of the rule.

Step 6	**default**
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# default`
		Sets a command to its default.

Step 7	**exit**
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# exit`
	`Device(config)#`
		Exits the sub-mode.

Step 8	**shutdown**
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# shutdown`
		Disables a particular rogue rule. In this example, the rule **rule_3** is disabled.

Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

	Command or Action	Purpose
Step 10	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 11	**wireless wps rogue rule shutdown** **Example:** `Device(config)# wireless wps rogue rule shutdown`	Disables all the rogue rules.
Step 12	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Rogue Classification Rules

You can monitor the rogue classification rules using the following commands:

Table 27: Commands for Monitoring Rogue Classification Rules

Command	Purpose
show wireless wps rogue rule detailed	Displays detailed information of a classification rule.
show wireless wps rogue rule summary	Displays a summary of the classification rules.

Examples: Classifying Rogue Access Points

This example shows how to classify a rogue AP with MAC address 00:11:22:33:44:55 as malicious and mark it for being contained by 2 managed APs:

```
Device# configure terminal
Device(config)# wireless wps rogue ap malicious 0011.2233.4455 state contain 2
```

This example shows how to create a rule that can categorize a rogue AP that is using SSID **my-friendly-ssid**, and it is seen for at least for 1000 seconds as friendly internal:

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# condition ssid my-friendly-ssid
Device(config-rule)# condition duration 1000
Device(config-rule)# match all
Device(config-rule)# classify friendly state internal
Device(config-rule)# no shutdown
```

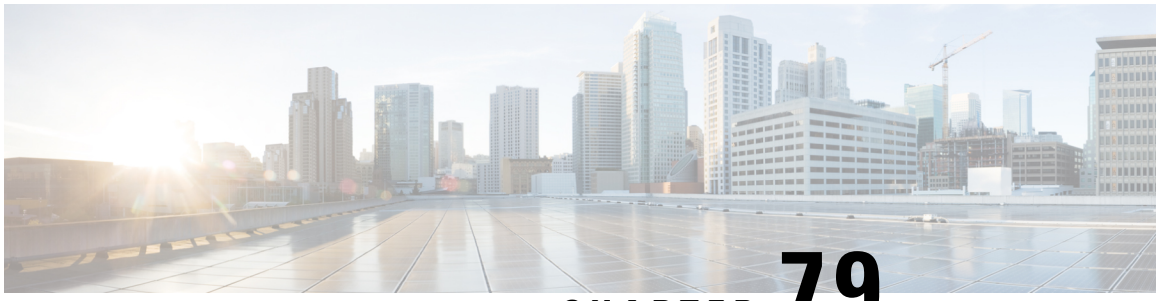
This example shows how to apply a condition that a rogue access point must meet:

```
Device# configure terminal
```

```
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# condition client-count 5
Device(config-rule)# condition duration 1000
Device(config-rule)# no shutdown
Device(config-rule)# end
```

This example shows a condition to classify rogue devices with the controller SSIDs as malicious:

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)#  classify malicious state alert
Device(config-rule)#  condition duration 30
Device(config-rule)#  condition infrastructure ssid
Device(config-rule)#  match all
Device(config-rule)#  no shutdown
Device(config-rule)# end
```



CHAPTER 79

Configuring Secure Shell

- Information About Configuring Secure Shell , on page 701
- Prerequisites for Configuring Secure Shell, on page 703
- Restrictions for Configuring Secure Shell, on page 704
- How to Configure SSH, on page 704
- Monitoring the SSH Configuration and Status, on page 707

Information About Configuring Secure Shell

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

SSH and Device Access

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

SSH functions the same in IPv6 as in IPv4. For IPv6, SSH supports IPv6 addresses and enables secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.

SSH Servers, Integrated Clients, and Supported Versions

The Secure Shell (SSH) Integrated Client feature is an application that runs over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco device to make a secure, encrypted connection to another Cisco device or to any other device running the SSH server. This connection provides functionality similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for secure communication over an unsecured network.

The SSH server and SSH integrated client are applications that run on the switch. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), 3DES, and password authentication.

The switch supports an SSHv1 or an SSHv2 server.

The switch supports an SSHv1 client.

Note The SSH client functionality is available only when the SSH server is enabled.

User authentication is performed like that in the Telnet session to the device. SSH also supports the following user authentication methods:

- TACACS+
- RADIUS
- Local authentication and authorization

SSH Configuration Guidelines

Follow these guidelines when configuring the switch as an SSH server or SSH client:

- An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.
- If the SSH server is running on an active switch and the active switch fails, the new active switch uses the RSA key pair generated by the previous active switch.
- If you get CLI error messages after entering the **crypto key generate rsa** global configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the **crypto key generate rsa** command.
- When generating the RSA key pair, the message No host name specified might appear. If it does, you must configure a hostname by using the **hostname** global configuration command.
- When generating the RSA key pair, the message No domain specified might appear. If it does, you must configure an IP domain name by using the **ip domain-name** global configuration command.
- When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

Secure Copy Protocol Overview

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying switch configurations or switch image files. SCP relies on Secure Shell (SSH), an application and a protocol that provides a secure replacement for the Berkeley r-tools.

For SSH to work, the switch needs an RSA public/private key pair. This is the same with SCP, which relies on SSH for its secure transport.

Because SSH also relies on AAA authentication, and SCP relies further on AAA authorization, correct configuration is necessary.

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.

Note When using SCP, you cannot enter the password into the copy command. You must enter the password when prompted.

Secure Copy Protocol

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying device configurations or switch image files. The behavior of SCP is similar to that of remote copy (rcp), which comes from the Berkeley r-tools suite, except that SCP relies on SSH for security. SCP also requires that authentication, authorization, and accounting (AAA) authorization be configured so the device can determine whether the user has the correct privilege level. To configure the Secure Copy feature, you should understand the SCP concepts.

SFTP Support

SFTP client support is introduced from Cisco IOS XE Gibraltar 16.10.1 release onwards. SFTP client is enabled by default and no separate configuration required.

The SFTP procedures can be invoked using the **copy** command, which is similar to that of **scp** and **tftp** commands. A typical file download procedure using **sftp** command can be carried out as shown below:

copy sftp://*user* :*password* @*server-ip*/*file-name* **flash0://** *file-name*

For more details on the **copy** command, see the following URL:
https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/fund/copy.html

Prerequisites for Configuring Secure Shell

The following are the prerequisites for configuring the switch for secure shell (SSH):

- For SSH to work, the switch needs an Rivest, Shamir, and Adleman (RSA) public/private key pair. This is the same with Secure Copy Protocol (SCP), which relies on SSH for its secure transport.
- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.
- SCP relies on SSH for security.
- SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.
- A user must have appropriate authorization to use SCP.
- A user who has appropriate authorization can use SCP to copy any file in the Cisco IOS File System (IFS) to and from a switch by using the **copy** command. An authorized administrator can also do this from a workstation.
- The Secure Shell (SSH) server requires an IPsec (Data Encryption Standard [DES] or 3DES) encryption software image; the SSH client requires an IPsec (DES or 3DES) encryption software image.)

- Configure a hostname and host domain for your device by using the **hostname** and **ip domain-name** commands in global configuration mode.

Restrictions for Configuring Secure Shell

The following are restrictions for configuring the device for secure shell.

- From Cisco IOS XE Dublin 17.10.x, Key Exchange and MAC algorithms like diffie-hellman-group14-sha1, hmac-sha1, hmac-sha2-256, and hmac-sha2-512 are not supported by default and it may impact some SSH clients that only support these algorithms. However, you can add them manually if required. For information on manually adding these algorithms, see the **SSH Algorithms for Common Criteria Certification** document available at: https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-secure-shell-algorithm-ccc.html
- The switch supports Rivest, Shamir, and Adelman (RSA) authentication.
- SSH supports only the execution-shell application.
- The SSH server and the SSH client are supported only on Data Encryption Standard (DES) (56-bit) and 3DES (168-bit) data encryption software. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.
- The device supports the Advanced Encryption Standard (AES) encryption algorithm with a 128-bit key, 192-bit key, or 256-bit key. However, symmetric cipher AES to encrypt the keys is not supported.
- When using SCP, you cannot enter the password into the **copy** command. You must enter the password when prompted.
- The login banner is not supported in Secure Shell Version 1. It is supported in Secure Shell Version 2.
- The -l keyword and userid :{number} {ip-address} delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for console access.
- To authenticate clients with freeradius over RADSEC, you should generate an RSA key longer than 1024 bit. Use the **crypto key generate rsa general-keys exportable label** *label-name* command to achieve this.

How to Configure SSH

Setting Up the Device to Run SSH

Follow the procedure given below to set up your device to run SSH:

Before you begin

Configure user authentication for local or remote access.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# Device# configure terminal`	Enters global configuration mode.
Step 2	**hostname** *hostname* **Example:** `Device(config)# hostname your_hostname`	Configures a hostname and IP domain name for your device. **Note** Follow this procedure only if you are configuring the device as an SSH server.
Step 3	**ip domain name** *domain_name* **Example:** `Device(config)# ip domain name your_domain`	Configures a host domain for your device.
Step 4	**crypto key generate rsa** **Example:** `Device(config)# crypto key generate rsa`	Enables the SSH server for local and remote authentication on the device and generates an RSA key pair. Generating an RSA key pair for the device automatically enables SSH. We recommend that a minimum modulus size of 1024 bits. When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use. **Note** Follow this procedure only if you are configuring the device as an SSH server.
Step 5	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Configuring the SSH Server

Follow the procedure given below to configure the SSH server:

Note This procedure is only required if you are configuring the device as an SSH server.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip ssh version** [2] **Example:** `Device(config)# ip ssh version 2`	(Optional) Configures the device to run SSH Version 2. If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client.
Step 3	**ip ssh window-size** **Example:** Device(config)# **ip ssh window-size**	Specifies the SSH window size. The recommended window size is 32K or lesser that that. The default window size is 8912. Selecting **window-size** greater than 32K might have some impact on the CPU, until unless: • The network bandwidth is good. • Client can accommodate this size. • No latency in network. **Note** This CLI is recommended only for SCP operations and can be disabled once the copy is done.
Step 4	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*} **Example:** `Device(config)# ip ssh timeout 90 authentication-retries 2`	Configures the SSH control parameters: • Specify the time-out value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After the connection is established, the device uses the default time-out values of the CLI-based sessions. By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After the execution shell starts, the CLI-based session time-out value returns to the default of 10 minutes. • Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 5.

	Command or Action	Purpose
		Repeat this step when configuring both parameters.

Step 5	Use one or both of the following:
	• `line vty` *line_number* [*ending_line_number*]
	• **transport input ssh**
	Example:
	`Device(config)# line vty 1 10`
	or
	`Device(config-line)# transport input ssh`
		(Optional) Configures the virtual terminal line settings.
		• Enters line configuration mode to configure the virtual terminal line settings. For *line_number* and *ending_line_number*, specify a pair of lines. The range is 0 to 15.
		• Specifies that the device prevent non-SSH Telnet connections. This limits the router to only SSH connections.

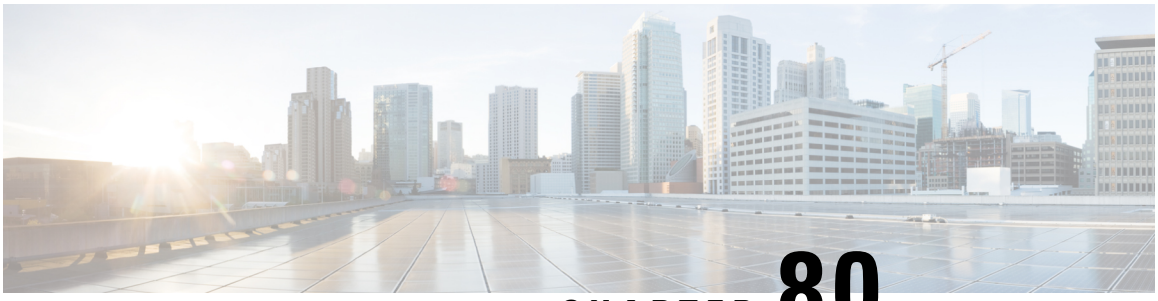
Step 6	**end** **Example:** `Device(config-line)# end`	Returns to privileged EXEC mode.

Monitoring the SSH Configuration and Status

This table displays the SSH server configuration and status.

Table 28: Commands for Displaying the SSH Server Configuration and Status

Command	Purpose
show ip ssh	Shows the version and configuration information for the SSH server.
show ssh	Shows the status of the SSH server.



CHAPTER 80

Private Shared Key

- Information About Private Preshared Key, on page 709
- Configuring a PSK in a WLAN (CLI), on page 710
- Configuring a PSK in a WLAN (GUI), on page 711
- Applying a Policy Profile to a WLAN (GUI), on page 712
- Applying a Policy Profile to a WLAN (CLI), on page 712
- Verifying a Private PSK, on page 713

Information About Private Preshared Key

With the advent of Internet of Things (IoT), the number of devices that connect to the internet has increased multifold. Not all of these devices support the 802.1x supplicant and need an alternate mechanism to connect to the internet. One of the security mechanisms, WPA-PSK, could be considered as an alternative. With the current configuration, the PSK is the same for all the clients that connect to the same WLAN. In certain deployments, such as educational institutions, this results in the key being shared to unauthorized users leading to security breach. This necessitates the need to provision unique PSKs for different clients on a large scale.

Identity PSKs are unique PSKs created for individuals or groups of users on the same SSID. No complex configuration is required for the clients. It provides the same simplicity of PSK, making it ideal for IoT, Bring your own device (BYOD), and guest deployments.

Identity PSKs are supported on most devices, in which 802.1X is not, enabling stronger security for IoT. It is possible to easily revoke access, for a single device or individual without affecting everyone else. Thousands of keys can easily be managed and distributed through the AAA server.

Note Special characters, such as '<' and '>' are not supported in SSID Preshared key.

Note PSK supports whitespace in passwords (before or after or in-between) within double quotes only; single quotes for whitespaces are not supported.

IPSK Solution

During client authentication, the AAA server authorizes the client MAC address and sends the passphrase (if configured) as part of the Cisco-AV pair list. The Cisco Wireless Controller (WLC) receives this as part of the RADIUS response and processes this further for the computation of PSKs.

When a client sends an association request to the SSID broadcast by the corresponding access point, the controller forms the RADIUS request packet with the particular mac address of the client and relays to the RADIUS server.

The RADIUS server performs the authentication and checks whether the client is allowed or not and sends either ACCESS-ACCEPT or ACCESS-REJECT as response to the WLC.

To support Identity PSKs, in addition to sending the authentication response, the authentication server also provides the AV pair passphrase for this specific client. This is used for the computation of the PMK.

The RADIUS server might also provide additional parameters, such as username, VLAN, Quality of Service (QoS), and so on, in the response, that is specific to this client. For multiple devices owned by a single user, the passphrase can remain the same.

Note When the PSK length is less than 15 characters in Federal Information Processing Standard (FIPS), the controller allows the WLAN configuration but displays the following error message on the console:

"AP is allowed to join but corresponding WLAN will not be pushed to the access point"

Configuring a PSK in a WLAN (CLI)

Follow the procedure given below to configure a PSK in a WLAN:

Before you begin

- Security should be configured for a pre-shared key (PSK) in a WLAN.
- If there is no override from the AAA server, the value on the corresponding WLAN is considered for authentication.
- In Federal Information Processing Standard (FIPS) and common criteria mode, ensure that the PSK WLAN has a minimum of 15 ASCII characters, else APs won't join the controller.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# wlan test-profile 4 abc`	Configures the WLAN and SSID.

	Command or Action	Purpose
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures the security type PSK.
Step 5	**security wpa akm psk set-key** *ascii/hex key* **Example:** `Device(config-wlan)# security wpa akm psk set-key asci 0`	Configures the PSK authenticated key management (AKM) shared key. **Note** You must set the **psk set-key** before configuring AKM PSK.
Step 6	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures PSK support.
Step 7	**security wpa wpa2 mpsk** **Example:** `Device(config-wlan)# security wpa wpa2 mpsk`	Configures multi-preshared key (MPSK) support. **Note** AKM PSK should be enabled for MPSK to work.
Step 8	**mac-filtering** *auth-list-name* **Example:** `Device(config-wlan)# mac-filtering test1`	Specifies MAC filtering in a WLAN.

Configuring a PSK in a WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **Wireless Networks** page, click **Security** tab.

Step 3 In the **Layer 2** window that is displayed, go to the **WPA Parameters** section.

Step 4 From the **Auth Key Mgmt** drop-down, select the PSK format and type.

Step 5 Enter the Pre-Shared Key in hexadecimal characters.

- If you selected the PSK format as HEX, the key length must be exactly 64 characters.
- If you selected the PSK format as ASCII, the key length must be in the range of 8-63 characters.

Note that once you have configured the key, these details are not visible even if you click on the eye icon next to the preshared key box, due to security reasons.

Step 6 Click **Save & Apply to Device**.

Applying a Policy Profile to a WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.
Step 2 On the**Manage Tags** page, click **Policy** tab.
Step 3 Click **Add** to view the **Add Policy Tag** window.
Step 4 Enter a name and description for the policy tag.
Step 5 Click **Add** to map WLAN and policy.
Step 6 Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.
Step 7 Click **Save & Apply to Device**.

Applying a Policy Profile to a WLAN (CLI)

Follow the procedure given below to a apply policy profile to a WLAN:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-iot`	Configures the default policy profile.
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Configures AAA override to apply policies coming from the AAA server or ISE the Cisco Identify Services Engine (ISE) server.

Verifying a Private PSK

Use the following **show** commands to verify the configuration of a WLAN and a client:

```
Device# show wlan id 2


WLAN Profile Name     : test_ppsk
===============================================
Identifier                                       : 2
Network Name (SSID)                              : test_ppsk
Status                                           : Enabled
Broadcast SSID                                   : Enabled
Universal AP Admin                               : Disabled
Max Associated Clients per WLAN                  : 0
Max Associated Clients per AP per WLAN           : 0
Max Associated Clients per AP Radio per WLAN     : 0
Number of Active Clients                         : 0
Exclusionlist Timeout                            : 60
CHD per WLAN                                     : Enabled
Interface                                        : default
Multicast Interface                              : Unconfigured
WMM                                              : Allowed
WifiDirect                                       : Invalid
Channel Scan Defer Priority:
  Priority (default)                             : 4
  Priority (default)                             : 5
  Priority (default)                             : 6
Scan Defer Time (msecs)                          : 100
Media Stream Multicast-direct                    : Disabled
CCX - AironetIe Support                          : Enabled
CCX - Diagnostics Channel Capability             : Disabled
Peer-to-Peer Blocking Action                     : Disabled
Radio Policy                                     : All
DTIM period for 802.11a radio                    : 1
DTIM period for 802.11b radio                    : 1
Local EAP Authentication                         : Disabled
Mac Filter Authorization list name               : test1
Accounting list name                             : Disabled
802.1x authentication list name                  : 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 dot1x                             : Disabled
            FT PSK                               : Disabled
            PMF dot1x                            : Disabled
            PMF PSK                              : Disabled
    CCKM TSF Tolerance                           : 1000
    FT Support                                   : Disabled
        FT Reassociation Timeout                 : 20
        FT Over-The-DS mode                      : Enabled
    PMF Support                                  : Disabled
```

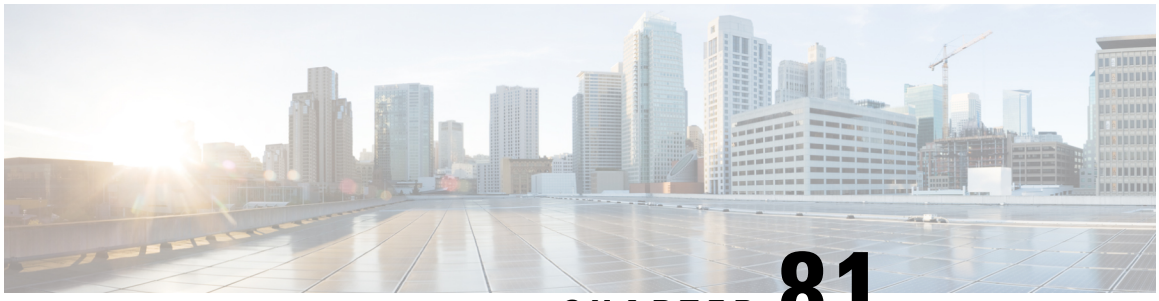
```
        PMF Association Comeback Timeout       : 1
        PMF SA Query Time                      : 200
    Web Based Authentication                   : Disabled
    Conditional Web Redirect                   : Disabled
    Splash-Page Web Redirect                   : Disabled
    Webauth On-mac-filter Failure              : Disabled
    Webauth Authentication List Name           : Disabled
    Webauth Parameter Map                      : Disabled
    Tkip MIC Countermeasure Hold-down Timer    : 60
Call Snooping                                  : Disabled
Passive Client                                 : Disabled
Non Cisco WGB                                  : Disabled
Band Select                                    : Disabled
Load Balancing                                 : Disabled
Multicast Buffer                               : Disabled
Multicast Buffer Size                          : 0
IP Source Guard                                : Disabled
Assisted-Roaming
    Neighbor List                              : Disabled
    Prediction List                            : Disabled
    Dual Band Support                          : Disabled
IEEE 802.11v parameters
    Directed Multicast Service                 : Disabled
    BSS Max Idle                               : Disabled
        Protected Mode                         : Disabled
    Traffic Filtering Service                  : Disabled
    BSS Transition                             : Enabled
        Disassociation Imminent                : Disabled
            Optimised Roaming Timer            : 40
            Timer                              : 200
    WNM Sleep Mode                             : Disabled
802.11ac MU-MIMO                               : Disabled
```

```
Device# show wireless client mac-address a886.adb2.05f9 detail
```

```
Client MAC Address : a886.adb2.05f9
Client IPv4 Address : 9.9.58.246
Client Username : A8-86-AD-B2-05-F9
AP MAC Address : c025.5c55.e400
AP Name: saurabh-3600
AP slot : 1
Client State : Associated
Policy Profile : default-policy-profile
Flex Profile : default-flex-profile
Wireless LAN Id : 6
Wireless LAN Name: SSS_PPSK
BSSID : c025.5c55.e40f
Connected For : 280 seconds
Protocol : 802.11n - 5 GHz
Channel : 60
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Session Timeout : 320 sec (Remaining time: 40 sec)
Input Policy Name  :
Input Policy State : None
Input Policy Source : None
Output Policy Name  :
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
```

```
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Power Save : OFF
Current Rate : m22
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 09/27/2017 16:32:25 IST
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 280 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : PSK
AAA override passphrase: Yes
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : 58
Access VLAN : 58
Anchor VLAN : 0
WFD capable : No
Manged WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface        : capwap_90000005
  IIF ID           : 0x90000005
  Device Type      : Apple-Device
  Protocol Map     : 0x000001
  Authorized       : TRUE
  Session timeout  : 320
  Common Session ID: 1F3809090000005DC30088EA
  Acct Session ID  : 0x00000000
  Auth Method Status List
        Method : MAB
                SM State        : TERMINATE
                Authen Status   : Success
  Local Policies:
        Service Template : wlan_svc_default-policy-profile (priority 254)
                Absolute-Timer   : 320
                VLAN             : 58
  Server Policies:
  Resultant Policies:
                VLAN             : 58
                Absolute-Timer   : 320
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Central
FlexConnect Central Association : No
```

```
Client Statistics:
  Number of Bytes Received : 59795
  Number of Bytes Sent : 21404
  Number of Packets Received : 518
  Number of Packets Sent : 274
  Number of EAP Id Request Msg Timeouts :
  Number of EAP Request Msg Timeouts :
  Number of EAP Key Msg Timeouts :
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -32 dBm
  Signal to Noise Ratio : 58 dB
Fabric status : Disabled
```



CHAPTER 81

Multi-Preshared Key

- Information About Multi-Preshared Key, on page 717
- Restrictions on Multi-PSK, on page 718
- Configuring Multi-Preshared Key (GUI), on page 718
- Configuring Multi-Preshared Key (CLI), on page 721
- Verifying Multi-PSK Configurations, on page 722

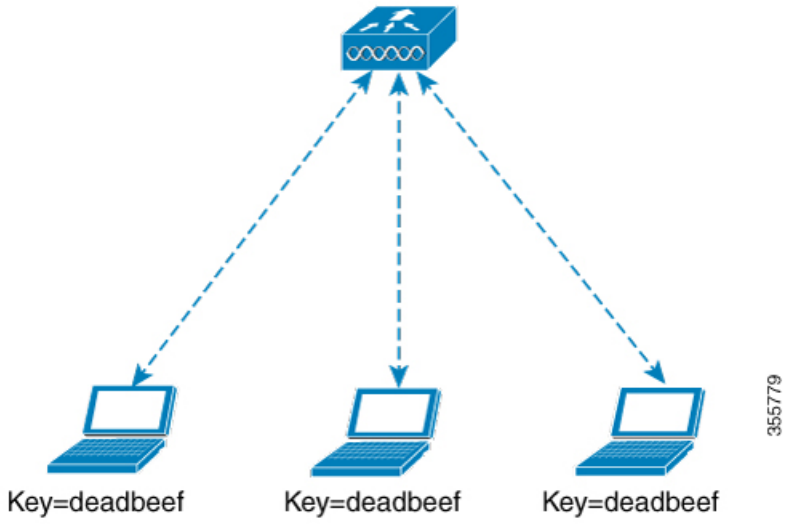
Information About Multi-Preshared Key

Multi-PSK feature supports multiple PSKs simultaneously on a single SSID. You can use any of the configured PSKs to join the network. This is different from the Identity PSK (iPSK), wherein unique PSKs are created for individuals or groups of users on the same SSID.

From 16.10 onwards, each SSID supports five PSKs, which can be extended

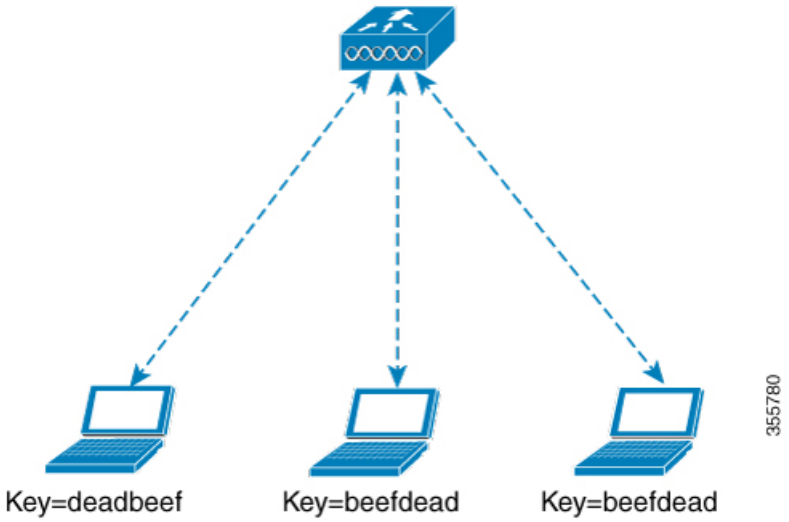
In a traditional PSK, all the clients joining the network use the same password as shown in the below figure.

Figure 14: Traditional PSK



But with multi-PSK, client can use any of the configured pre-shared keys to connect to the network as shown in the below figure.

Figure 15: Multi-PSK



In Multi-PSK, two passwords are configured (deadbeef and beefdead) for the same SSID. In this scenario, clients can connect to the network using either of the passwords.

Restrictions on Multi-PSK

- Central authentication is supported in local, flex, and fabric modes only.
- In central authentication flex mode, the standalone AP allows client join with the highest priority PSK (*priority 0* key). New clients that do not use the highest priority PSK are rejected during the standalone mode.
- Multi-PSK does not support local authentication.

Configuring Multi-Preshared Key (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **Wireless Networks** page, click the name of the WLAN.

Step 3 In the **Edit WLAN** window, click the **Security** tab.

Step 4 In the **Layer2** tab, choose the **Layer2 Security Mode** from the following options:

- None: No Layer 2 security
- 802.1X: WEP 802.1X data encryption type
- WPA + WPA2: Wi-Fi Protected Access
- Static WEP: Static WEP encryption parameters
- Static WEP+802.1X: Both Static WEP and 802.1X parameters

Parameters	Description
802.1X	
WEP Key Size	Choose the key size. The available values are *None*, *40 bits*, and *104 bits*.
WPA + WPA2	
Protected Management Frame	Choose from the following options: • Disabled • Optional • Required
WPA Policy	Check the check box to enable WPA policy.
WPA Encryption	Choose the WPA encryption standard. A WPA encryption standard must be specified if you have enabled WPA policy.
WPA2 Policy	Check the check box to enable WPA2 policy.
WPA2 Encryption	Choose the WPA2 encryption standard. A WPA encryption standard must be specified if you have enabled WPA policy.
Auth Key Mgmt	Choose the rekeying mechanism from the following options: • 802.1X • FT + 802.1X • PSK: You must specify the PSK format and a preshared key • Cisco Centralized Key Management: You must specify a Cisco Centralized Key Management Timestamp Tolerance value • 802.1X + Cisco Centralized Key Management: You must specify a Cisco Centralized Key Management Timestamp Tolerance value • FT + 802.1X + Cisco Centralized Key Management: You must specify a Cisco Centralized Key Management Timestamp Tolerance value
Static WEP	

Parameters	Description
Key Size	Choose the key size from the following options: • 40 bits • 104 bits
Key Index	Choose a key index from 1 to 4. One unique WEP key index can be applied to each WLAN. As there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer2 encryption.
Key Format	Choose the encryption key format as either ASCII or HEX.
Encryption Key	Enter an encryption key that is 13 characters long.
Static WEP + 802.1X	
Key Size	Choose the key size from the following options: • 40 bits • 104 bits
Key Index	Choose a key index from 1 to 4. One unique WEP key index can be applied to each WLAN. As there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer2 encryption.
Key Format	Choose the encryption key format as either ASCII or HEX.
Encryption Key	Enter an encryption key that is 13 characters long.
WEP Key Size	Choose from the following options: • None • 40 bits • 104 bits

Step 5 Click **Save & Apply to Device**.

Configuring Multi-Preshared Key (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# wlan mywlan 1 SSID_name`	Configures WLAN and SSID.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures PSK.
Step 5	**security wpa wpa2 mpsk** **Example:** `Device(config-wlan)# security wpa wpa2 mpsk`	Configures multi-PSK.
Step 6	**priority** *priority_value* **set-key** {**ascii** [**0** | **8**] *pre-shared-key* | **hex** [**0** | **8**] *pre-shared-key*} **Example:** `Device(config-mpsk)# priority 0 set-key ascii 0 deadbeef`	Configures PSK priority and all its related passwords. The *priority_value* ranges from 0 to 4. **Note** You need to configure **priority 0** key for multi-PSK.
Step 7	**no shutdown** **Example:** `Device(config-mpsk)# no shutdown`	Enables WLAN.
Step 8	**exit** **Example:** `Device(config-wlan)# exit`	Exits WLAN configuration mode and returns to configuration mode.

	Command or Action	Purpose
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Multi-PSK Configurations

To verify the configuration of a WLAN and a client, use the following command:

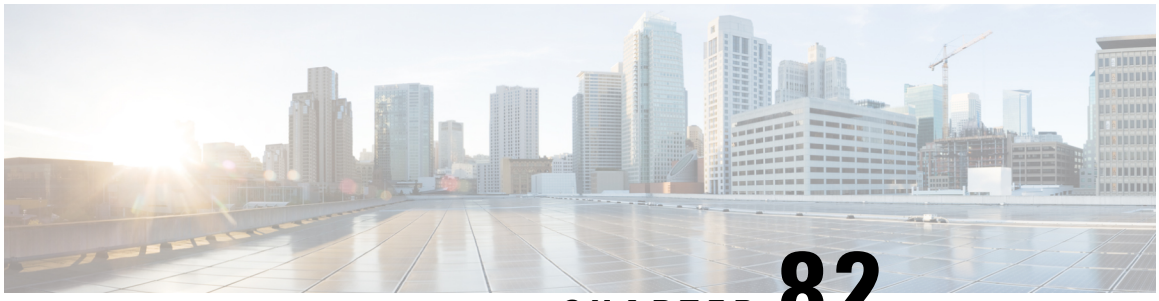
```
Device# show wlan id 8
WLAN Profile Name     : wlan_8
================================================
Identifier                                       : 8
Network Name (SSID)                              : ssid_8
Status                                           : Enabled
Broadcast SSID                                   : Enabled
Universal AP Admin                               : Disabled
Max Associated Clients per WLAN                  : 0
Max Associated Clients per AP per WLAN           : 0
Max Associated Clients per AP Radio per WLAN     : 200
Number of Active Clients                         : 0
CHD per WLAN                                     : Enabled
Multicast Interface                              : Unconfigured
WMM                                              : Allowed
WifiDirect                                       : Invalid
Channel Scan Defer Priority:
  Priority (default)                             : 5
  Priority (default)                             : 6
Scan Defer Time (msecs)                          : 100
Media Stream Multicast-direct                    : Disabled
CCX - AironetIe Support                          : Enabled
CCX - Diagnostics Channel Capability             : Disabled
Peer-to-Peer Blocking Action                     : Disabled
Radio Policy                                     : All
DTIM period for 802.11a radio                    : 1
DTIM period for 802.11b radio                    : 1
Local EAP Authentication                         : Disabled
Mac Filter Authorization list name               : Disabled
Mac Filter Override Authorization list name      : Disabled
Accounting list name                             :
802.1x authentication list name                  : Disabled
802.1x authorization list name                   : Disabled
Security
    802.11 Authentication                        : Open System
    Static WEP Keys                              : Disabled
    802.1X                                       : Disabled
    Wi-Fi Protected Access (WPA/WPA2/WPA3)       : Enabled
        WPA (SSN IE)                             : Disabled
        WPA2 (RSN IE)                            : Enabled
            MPSK                                 : Enabled
            AES Cipher                           : Enabled
            CCMP256 Cipher                       : Disabled
            GCMP128 Cipher                       : Disabled
            GCMP256 Cipher                       : Disabled
        WPA3 (WPA3 IE)                           : Disabled
        Auth Key Management
            802.1x                               : Disabled
            PSK                                  : Enabled
```

```
            CCKM                                    : Disabled
            FT dot1x                                : Disabled
            FT PSK                                  : Disabled
            FT SAE                                  : Disabled
            PMF dot1x                               : Disabled
            PMF PSK                                 : Disabled
            SAE                                     : Disabled
            OWE                                     : Disabled
            SUITEB-1X                               : Disabled
            SUITEB192-1X                            : Disabled
    CCKM TSF Tolerance                              : 1000
    FT Support                                      : Adaptive
        FT Reassociation Timeout                    : 20
        FT Over-The-DS mode                         : Enabled
    PMF Support                                     : Disabled
        PMF Association Comeback Timeout            : 1
        PMF SA Query Time                           : 200
    Web Based Authentication                        : Disabled
    Conditional Web Redirect                        : Disabled
    Splash-Page Web Redirect                        : Disabled
    Webauth On-mac-filter Failure                   : Disabled
    Webauth Authentication List Name                : Disabled
    Webauth Authorization List Name                 : Disabled
    Webauth Parameter Map                           : Disabled
    Tkip MIC Countermeasure Hold-down Timer         : 60
Non Cisco WGB                                       : Disabled
Band Select                                         : Enabled
Load Balancing                                      : Disabled
Multicast Buffer                                    : Disabled
Multicast Buffer Size                               : 0
IP Source Guard                                     : Disabled
Assisted-Roaming
    Neighbor List                                   : Disabled
    Prediction List                                 : Disabled
    Dual Band Support                               : Disabled
IEEE 802.11v parameters
    Directed Multicast Service                      : Disabled
    BSS Max Idle                                    : Disabled
        Protected Mode                              : Disabled
    Traffic Filtering Service                       : Disabled
    BSS Transition                                  : Enabled
        Disassociation Imminent                     : Disabled
            Optimised Roaming Timer                 : 40
            Timer                                   : 200
    WNM Sleep Mode                                  : Disabled
802.11ac MU-MIMO                                    : Disabled
802.11ax paramters
    OFDMA Downlink                                  : unknown
    OFDMA Uplink                                    : unknown
    MU-MIMO Downlink                                : unknown
    MU-MIMO Uplink                                  : unknown
    BSS Color                                       : unknown
    Partial BSS Color                               : unknown
    BSS Color Code                                  :
```

To view the WLAN details, use the following command:

```
Device# show run wlan
wlan wlan_8 8 ssid_8
 security wpa psk set-key ascii 0 deadbeef
 no security wpa akm dot1x
 security wpa akm psk
 security wpa wpa2 mpsk
  priority 0 set-key ascii 0 deadbeef
  priority 1 set-key ascii 0 deaddead
```

```
 priority 2 set-key ascii 0 d123d123
 priority 3 set-key hex 0 02345678901234567890123456789012345678901234567890123456789012345678901234

 priority 4 set-key hex 0 12345678901234567890123456789012345678901234567890123456789012345678901234

no shutdown
```



CHAPTER 82

Multiple Authentications for a Client

- Information About Multiple Authentications for a Client, on page 725
- Configuring Multiple Authentications for a Client, on page 726
- Verifying Multiple Authentication Configurations, on page 732

Information About Multiple Authentications for a Client

Multiple Authentication feature is an extension of Layer 2 and Layer 3 security types supported for client join.

Note You can enable both L2 and L3 authentication for a given SSID.

Note The Multiple Authentication feature is applicable for regular clients only.

Information About Supported Combination of Authentications for a Client

The Multiple Authentications for a Client feature supports multiple combination of authentications for a given client configured in the WLAN profile.

The following table outlines the supported combination of authentications:

Layer 2	Layer 3	Supported
MAB	CWA	Yes
MAB Failure	LWA	Yes
802.1X	CWA	Yes
PSK	CWA	Yes
iPSK + MAB	CWA	Yes
iPSK	LWA	No

MAB Failure + PSK	LWA	No
MAB Failure + PSK	CWA	No

From 16.10.1 onwards, 802.1X configurations on WLAN support web authentication configurations with WPA or WPA2 configuration.

The feature also supports the following AP modes:

- Local
- FlexConnect
- Fabric

Configuring Multiple Authentications for a Client

Configuring WLAN for 802.1X and Local Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.
Step 2 Select the required WLAN from the list of WLANs displayed.
Step 3 Choose **Security** > **Layer2** tab.
Step 4 Select the security method from the **Layer 2 Security Mode** drop-down list.
Step 5 In the **Auth Key Mgmt**, check the **802.1x** check box.
Step 6 Check the **MAC Filtering** check box to enable the feature.
Step 7 After MAC Filtering is enabled, from the **Authorization List** drop-down list, choose an option.
Step 8 Choose **Security** > **Layer3** tab.
Step 9 Check the **Web Policy** check box to enable web authentication policy.
Step 10 From the **Web Auth Parameter Map** and the **Authentication List** drop-down lists, choose an option.
Step 11 Click **Update & Apply to Device**.

Configuring WLAN for 802.1X and Local Web Authentication (CLI)

Procedure

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

	Command or Action	Purpose
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration sub-mode. • *profile-name*: Profile name of the configured WLAN. • *wlan-id*: Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name*: SSID that can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter the **wlan** *profile-name* command.
Step 3	**security dot1x authentication-list** *auth-list-name* **Example:** `Device(config-wlan)# security dot1x authentication-list default`	Enables security authentication list for dot1x security. The configuration is similar for all dot1x security WLANs.
Step 4	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables web authentication.
Step 5	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for dot1x security.
Step 6	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	Maps the parameter map. **Note** If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 7	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Example

```
wlan wlan-test 3 ssid-test
 security dot1x authentication-list default
 security web-auth
 security web-auth authentication-list default
```

```
security web-auth parameter-map WLAN1_MAP
no shutdown
```

Configuring WLAN for Preshared Key (PSK) and Local Web Authentication (GUI)

Procedure

Step 1	Choose **Configuration** > **Tags & Profiles** > **WLANs**.
Step 2	Select the required WLAN.
Step 3	Choose **Security** > **Layer2** tab.
Step 4	Select the security method from the **Layer 2 Security Mode** drop-down list.
Step 5	In the Auth Key Mgmt, uncheck the **802.1x** check box.
Step 6	Check the **PSK** check box.
Step 7	Enter the **Pre-Shared Key** and choose the PSK Format from the **PSK Format** drop-down list and the PSK Type from the **PSK Type** drop-down list.
Step 8	Choose **Security** > **Layer3** tab.
Step 9	Check the **Web Policy** checkbox to enable web authentication policy.
Step 10	Choose the Web Auth Parameter Map from the **Web Auth Parameter Map** drop-down list and the authentication list from the **Authentication List** drop-down list.
Step 11	Click **Update & Apply to Device**.

Configuring WLAN for Preshared Key (PSK) and Local Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration sub-mode. • *profile-name*- Is the profile name of the configured WLAN. • *wlan-id* - Is the wireless LAN identifier. Range is from 1 to 512. • *SSID_Name* - Is the SSID which can contain 32 alphanumeric characters.

	Command or Action	Purpose
		Note If you have already configured this command, enter **wlan** *profile-name* command.
Step 3	**security wpa psk set-key** *ascii/hex key password* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD`	Configures the PSK shared key.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures the PSK support.
Step 6	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables web authentication for WLAN.
Step 7	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list webauth`	Enables authentication list for dot1x security.
Step 8	**security web-auth parameter-map** *parameter-map-name* **Example:** `(config-wlan)# security web-auth parameter-map WLAN1_MAP`	Configures the parameter map. **Note** If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.

Example

```
wlan wlan-test 3 ssid-test
 security wpa psk set-key ascii 0 PASSWORD
 no security wpa akm dot1x
 security wpa akm psk
 security web-auth
 security web-auth authentication-list webauth
 security web-auth parameter-map WLAN1_MAP
```

Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication (GUI)

Procedure

Step 1	Choose **Configuration** > **Tags & Profiles** > **WLANs**.
Step 2	Select the required WLAN.
Step 3	Choose **Security** > **Layer2** tab.
Step 4	Select the security method from the **Layer 2 Security Mode** drop-down list.
Step 5	In the **Auth Key Mgmt**, uncheck the **802.1x** check box.
Step 6	Check the **PSK** check box.
Step 7	Enter the **Pre-Shared Key** and choose the PSK Format from the **PSK Format** drop-down list and the PSK Type from the **PSK Type** drop-down list.
Step 8	Check the **MAC Filtering** check box to enable the feature.
Step 9	With MAC Filtering enabled, choose the Authorization List from the **Authorization List** drop-down list.
Step 10	Choose **Security** > **Layer3** tab.
Step 11	Check the **Web Policy** checkbox to enable web authentication policy.
Step 12	Choose the Web Auth Parameter Map from the **Web Auth Parameter Map** drop-down list and the authentication list from the **Authentication List** drop-down list.
Step 13	Click **Update &Apply to Device**.

Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication

Configuring WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration sub-mode. • *profile-name* - Is the profile name of the configured WLAN. • *wlan-id* - Is the wireless LAN identifier. Range is from 1 to 512.

	Command or Action	Purpose
		• *SSID_Name* - Is the SSID which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *profile-name* command.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**security wpa psk set-key** *ascii/hex key password* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD`	Configures the PSK AKM shared key.
Step 5	**mac-filtering** *auth-list-name* **Example:** `Device(config-wlan)# mac-filtering test-auth-list`	Sets the MAC filtering parameters.

Example

```
wlan wlan-test 3 ssid-test
 no security wpa akm dot1x
 security wpa psk set-key ascii 0 PASSWORD
 mac-filtering test-auth-list
```

Applying Policy Profile to a WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-iot`	Configures the default policy profile.

	Command or Action	Purpose
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Configures AAA override to apply policies coming from the AAA or ISE servers.
Step 4	**nac** **Example:** `Device(config-wireless-policy)# nac`	Configures NAC in the policy profile.
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Shutdown the WLAN.
Step 6	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.

Example

```
wireless profile policy policy-iot
 aaa-override
 nac
 no shutdown
```

Verifying Multiple Authentication Configurations

Layer 2 Authentication

After L2 authentication (Dot1x) is complete, the client is moved to *Webauth Pending* state.

To verify the client state after L2 authentication, use the following commands:

```
Device# show wireless client summary
Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
-------------------------------------------------------------------------------------------------------------------

58ef.68b6.aa60 ewlc1_ap_1   3  Webauth Pending    11n(5)        Dot1x  Local
Number of Excluded Clients: 0

Device# show wireless client mac-address <mac_address> detail

Auth Method Status List

Method: Dot1x
Webauth State: Init
Webauth Method: Webauth
Local Policies:
Service Template: IP-Adm-V6-Int-ACL-global (priority 100)
```

```
URL Redirect ACL: IP-Adm-V6-Int-ACL-global
Service Template: IP-Adm-V4-Int-ACL-global (priority 100)
URL Redirect ACL: IP-Adm-V4-Int-ACL-global
Service Template: wlan_svc_default-policy-profile_local (priority 254)
Absolute-Timer: 1800
VLAN: 50
```

```
Device# show platform software wireless-client chassis active R0

        ID  MAC Address      WLAN  Client     State
------------------------------------------------------------------------------------------
  0xa0000003      58ef.68b6.aa60    3             L3          Authentication
```

```
Device# show platform software wireless-client chassis active F0

    ID     MAC Address   WLAN  Client     State  AOM ID    Status
-------------------------------------------------------------------------------------------------
0xa0000003    58ef.68b6.aa60    3           L3          Authentication.         730.
Done
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary

Client Type Abbreviations:
RG - REGULAR   BLE - BLE
HL - HALO    LI - LWFL INT

Auth State Abbrevations:
UK - UNKNOWN    IP - LEARN    IP IV - INVALID
L3 - L3 AUTH RN - RUN

Mobility State Abbreviations:
UK - UNKNOWN       IN - INIT
LC - LOCAL               AN - ANCHOR
FR - FOREIGN          MT - MTE
IV - INVALID


EoGRE Abbreviations:
N - NON EOGRE Y - EOGRE

CPP IF_H   DP IDX       MAC Address      VLAN   CT   MCVL AS MS E   WLAN      POA
-------------------------------------------------------------------------------------
0X49     0XA0000003    58ef.68b6.aa60     50    RG     0  L3 LC N wlan-test 0x90000003
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath summary
Vlan   DP IDX         MAC Address      VLAN   CT   MCVL AS MS E   WLAN      POA
-------------------------------------------------------------------------------------
0X49   0xa0000003    58ef.68b6.aa60     50    RG     0  L3 LC N wlan-test 0x90000003
```

Layer 3 Authentication

Once L3 authentication is successful, the client is moved to *Run* state.

To verify the client state after L3 authentication, use the following commands:

```
Device# show wireless client summary

Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
-----------------------------------------------------------------------------------------------------

58ef.68b6.aa60   ewlc1_ap_1  3     Run    11n(5)   Web Auth      Local
Number of Excluded Clients: 0
```

```
Device# show wireless client mac-address 58ef.68b6.aa60 detail

Auth Method Status List

Method: Web Auth
Webauth State: Authz
Webauth Method: Webauth
Local Policies:
Service Template: wlan_svc_default-policy-profile_local (priority 254)
Absolute-Timer: 1800
VLAN: 50

Server Policies:

Resultant Policies:
VLAN: 50
Absolute-Timer: 1800
```

```
Device# show platform software wireless-client chassis active R0

ID          MAC Address     WLAN    Client State
-------------------------------------------------
0xa0000001 58ef.68b6.aa60    3          Run
```

```
Device# show platform software wireless-client chassis active f0

ID         MAC Address       WLAN    Client State   AOM ID.  Status
-----------------------------------------------------------------------
0xa0000001 58ef.68b6.aa60.   3          Run         11633    Done
```

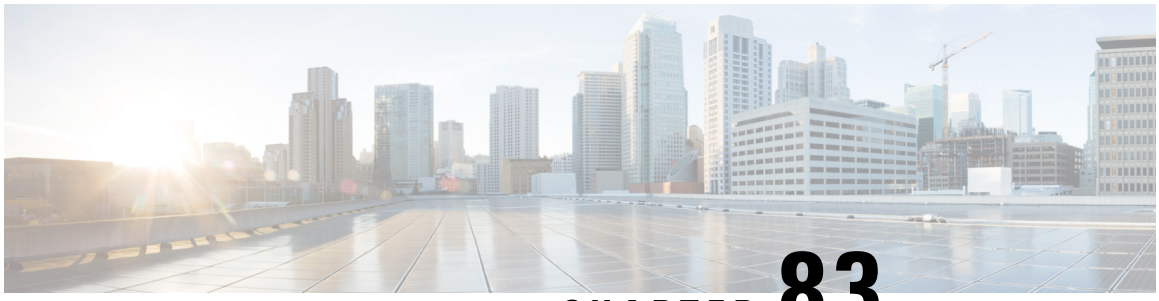
```
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary

Client Type Abbreviations:
RG - REGULAR   BLE - BLE
HL - HALO      LI - LWFL INT

Auth State Abbrevations:
UK - UNKNOWN    IP - LEARN    IP IV - INVALID
L3 - L3 AUTH RN - RUN
Mobility State Abbreviations:
UK - UNKNOWN       IN - INIT
LC - LOCAL         AN - ANCHOR
FR - FOREIGN       MT - MTE
IV - INVALID
EoGRE Abbreviations:
N - NON EOGRE Y - EOGRE

CPP IF_H   DP IDX       MAC Address   VLAN  CT  MCVL AS MS E   WLAN     POA
-------------------------------------------------------------------------------
0X49     0XA0000003    58ef.68b6.aa60  50   RG   0   RN LC N wlan-test 0x90000003
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath summary

Vlan   pal_if_hd1        mac           Input Uidb     Output Uidb
-----------------------------------------------------------------
50     0xa0000003    58ef.68b6.aa60     95929            95927
```

Verifying PSK+Webauth Configuration

```
Device# show wlan summary

Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 12:08:32.941 CEST Tue Oct 6 2020
```

```
Number of WLANs: 1

ID Profile Name SSID Status Security
--------------------------------------------------------------------------------------------------------------------------------

23 Gladius1-PSKWEBAUTH Gladius1-PSKWEBAUTH UP [WPA2][PSK][AES],[Web Auth]
```



CHAPTER 83

Cisco TrustSec

- Information about Cisco TrustSec, on page 737
- Cisco TrustSec Features, on page 738
- Security Group Access Control List, on page 740
- Inline Tagging, on page 741
- Policy Enforcement, on page 741
- SGACL Support for Wireless Guest Access, on page 742
- Enabling SGACL on the AP (GUI), on page 742
- Enabling SGACL on the AP, on page 743
- Enabling SGACL Policy Enforcement Globally (CLI), on page 744
- Enabling SGACL Policy Enforcement Per Interface (CLI), on page 745
- Manually Configure a Device SGT (CLI), on page 745
- Configuring SGACL, Inline Tagging, and SGT in Local Mode (GUI), on page 746
- Configuring SGACL, Inline Tagging, and SGT in Local Mode, on page 746
- Configuring ISE for TrustSec, on page 747
- Verifying Cisco TrustSec Configuration, on page 748

Information about Cisco TrustSec

Cisco TrustSec provides security improvements to Cisco network devices based on the capability to strongly identify users, hosts, and network devices within a network. TrustSec provides topology-independent and scalable access controls by uniquely classifying data traffic for a particular role. TrustSec ensures data confidentiality and integrity by establishing trust among authenticated peers and encrypting links with those peers.

The key component of Cisco TrustSec is the Cisco Identity Services Engine (ISE). Cisco ISE can provision switches with TrustSec Identities and Security Group ACLs (SGACLs), though these may be configured manually on the switch.

Note You should manually clear the CTS environment data using the **clear cts environment-data** command before changing CTS server to a new one. This ensures that you get the updated data while running **show cts environment-data** command.

Cisco TrustSec Features

The table below lists the TrustSec features to be eventually implemented on TrustSec-enabled Cisco switches. Successive general availability releases of TrustSec will expand the number of switches supported and the number of TrustSec features supported per switch.

Cisco TrustSec Feature	Description
802.1AE Tagging (MACsec)	Protocol for IEEE 802.1AE-based wire-rate hop-to-hop Layer 2 encryption. Between MACsec-capable devices, packets are encrypted on egress from the transmitting device, decrypted on ingress to the receiving device, and in the clear within the devices. This feature is only available between TrustSec hardware-capable devices. **Note** This feature is not supported on Catalyst 3850 and Catalyst 3650 switches with
Endpoint Admission Control (EAC)	EAC is an authentication process for an endpoint user or a device connecting to the TrustSec domain. Usually EAC takes place at the access level switch. Successful authentication and authorization in the EAC process results in Security Group Tag assignment for the user or device. Currently EAC can be 802.1X, MAC Authentication Bypass (MAB), and Web Authentication Proxy (WebAuth).
Network Device Admission Control (NDAC)	NDAC is an authentication process where each network device in the TrustSec domain can verify the credentials and trustworthiness of its peer device. NDAC utilizes an authentication framework based on IEEE 802.1X port-based authentication and uses EAP-FAST as its EAP method. Successful authentication and authorization in NDAC process results in Security Association Protocol negotiation for IEEE 802.1AE encryption.
Security Group Access Control List (SGACL)	A Security Group Access Control List (SGACL) associates a Security Group Tag with a policy. The policy is enforced upon SGT-tagged traffic egressing the TrustSec domain.

Cisco TrustSec Feature	Description
Cisco TrustSec SGACL High Availability	Cisco TrustSec Security Group access control lists (SGACLs) support the high availability functionality on switches that support the Cisco StackWise technology. Cisco StackWise technology provides stateful redundancy and allows the switch stack to enforce and process access control entries. There is no Cisco TrustSec-specific configuration to enable this functionality.
Security Association Protocol (SAP)	After NDAC authentication, the Security Association Protocol (SAP) automatically negotiates keys and the cipher suite for subsequent MACSec link encryption between TrustSec peers. SAP is defined in IEEE 802.11i. **Note** This feature is not supported on Catalyst 3850 and Catalyst 3650 switches with
Security Group Tag (SGT)	An SGT is a 16-bit single label indicating the security classification of a source in the TrustSec domain. It is appended to an Ethernet frame or an IP packet.
SGT Exchange Protocol (SXP)	Security Group Tag Exchange Protocol (SXP). With SXP, devices that are not TrustSec-hardware-capable can receive SGT attributes for authenticated users and devices from the Cisco Identity Services Engine (ISE) or the Cisco Secure Access Control System (ACS). The devices can then forward a sourceIP-to-SGT binding to a TrustSec-hardware-capable device will tag the source traffic for SGACL enforcement.

When both ends of a link support 802.1AE MACsec, SAP negotiation occurs. An EAPOL-key exchange occurs between the supplicant and the authenticator to negotiate a cipher suite, exchange security parameters, and manage keys. Successful completion of these tasks results in the establishment of a security association (SA).

Depending on your software version and licensing and link hardware support, SAP negotiation can use one of these modes of operation:

- Galois Counter Mode (GCM)—authentication and encryption
- GCM authentication (GMAC)— GCM authentication, no encryption
- No Encapsulation—no encapsulation (clear text)
- Null—encapsulation, no authentication or encryption

Security Group Access Control List

A security group is a group of users, end-point devices, and resources that share access control policies. Security groups are defined by the administrator in Cisco Identity Services Engine (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, 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), even though 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 numbers on one axis and the destination security group numbers on the other axis. Each cell in the matrix body contains an ordered list of SGACLs, which specify 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, the controller 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 .

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; the user immediately receives permissions to that group.

The size of ACLs are reduced and their maintenance is simplified with the use of role-based permissions. With Cisco TrustSec, the number of Access Control Entities (ACEs) that are configured is determined by the number of permissions specified, resulting in a much smaller number of ACEs.

To know the list of Cisco APs that support SGACL, see the release notes: https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-release-notes-list.html

The scenarios supported for SGACLs on the Cisco Catalyst 9800 Series Wireless Controller are:

- Wireless-to-wireless (within Enterprise network):
  - Flex mode with local switching—SGACL enforcement is done on the egress AP when a packet leaves from a source wireless network to a destination wireless network.
  - Flex mode with central switching—SGACL enforcement is done on the egress AP. To achieve this, controller should export IP address to security group tag (IP-SGT) binding over SGT Exchange Protocol (SXP).

- Wired-to-wireless (DC-to-Enterprise network)—Enforcement takes place when a packet reaches the destination AP.
- Wireless-to-wired (Enterprise network-to-DC)—Enforcement takes place on the uplink switch when a packet reaches the ingress of the wired network.

Guidelines and Restrictions

- SGACL enforcement is carried out on the controller for local mode.
- SGACL enforcement is carried out on an AP for flex-mode APs performing local switching.
- SGACL enforcement for wireless clients is carried out either on the upstream switch or on the border gateway in a Branch-to-DC scenario.
- SGACL enforcement is not supported for non-IP or IP broadcast or multicast traffic.
- Per-WLAN SGT assignment is not supported.
- SGACL enforcement is not carried out for control-plane traffic between an AP and the wireless controller (for upstream or from upstream traffic).
- Non-static SGACL configurations are supported only for dynamic SGACL policies received from ISE.
- Static SGACL configuration on an AP is not supported.

Inline Tagging

Inline tagging is a transport mechanism using which a controller or AP understands the source SGT.

Transport mechanism is of two types:

- Central switching—For centrally switched packets, the controller performs inline tagging of all the packets sourced from wireless clients that are associated with the controller, by tagging it with the Cisco Meta Data (CMD) tag. For packets that are inbound from the distribution system, inline tagging also involves the controller stripping off the CMD header from the packet to learn the S-SGT tag. Thereafter, the controller forwards the packet including the S-SGT, for SGACL enforcement.
- Local switching—To transmit locally switched traffic, an AP performs inline tagging for packets that are associated with the AP and sourced from clients. To receive traffic, the AP handles both locally switched packets and centrally switched packets, uses the 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 an 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.

Policy enforcement can be applied to both central and local switched traffic on an AP. If wired clients communicate with wireless clients, the AP enforces the downstream traffic. If wireless clients communicate with wired clients, the AP enforces the upstream traffic. This way, the AP enforces traffic in both downstream and wireless-to-wireless traffic. You require S-SGT, D-SGT, and ACLs for the enforcement to work. APs get the SGT information for all the 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 because the Listener mode maintains the complete set of IP-SGT bindings. After you enable the enforcement on a an AP, the corresponding policies are downloaded and pushed to the AP.

SGACL Support for Wireless Guest Access

When a client joins the wireless network (WLAN), its session is managed by the Cisco Catalyst 9800 Series Wireless LAN Controller (WLC) that the AP is connected to is the foreign controller. Auto-Anchor Mobility allows a specific WLAN (for example, Guest WLAN) to be anchored to a particular controller, regardless of the client's entry point into the network. Auto-Anchor Mobility is the wireless Guest service where all guest traffic tunnels back to the DMZ controller irrespective of where they associate with the network.

In case of Auto-Anchor mobility, the following apply to Cisco TrustSec support:

- Classification: Occurs during authentication and hence on Foreign for Layer 2 security WLANs and on Anchor for Layer 3 security cases.
- Propagation: Always occurs at the Anchor where the client traffic enters the wired network.
- Enforcement: SGACL download and enforcement occurs on Anchor; the Anchor controller must have the connectivity to Cisco Identity Services Engine (ISE) and be registered as Network Access Server (NAS). Enforcement is not supported on foreign controller even when the enforcement CLI is configured on foreign controller.

This feature is supported in local mode and in Flex Central Switching of the controller. Flex mode with local switching and Fabric mode are not supported in guest scenarios as traffic does not go through the controller.

Roaming of a guest client occurs only at Guest Foreign controller and the Guest Anchor remains fixed. The different types of supported roam are Inter-Controller roaming and Intra-Controller roaming. Roaming under WebAuth pending is a special case which is also supported for Central Web Authentication (CWA) and Local Web Authentication (LWA).

Enabling SGACL on the AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 Click **Add**.

Step 3 In the **General** tab, check **Inline Tagging** and **SGACL Enforcement** check boxes and choose the CTS Profile Name from the **CTS Profile Name** drop-down list.

Step 4 Click **Apply to Device**.

Enabling SGACL on the AP

Note Use the **no** form of the commands given below to disable the configuration. For example, **cts role-based enforcement** disables role-based access control enforcement for APs.

Before you begin

- Security Group Access Control List (SGACL) on an AP can be enabled only when the wireless controller is in flexconnect mode.
- Configure the **cts manual** command on the uplink port to send or receive a tagged packet.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex xyz-flex-profile`	Configures an RF profile and enters RF profile configuration mode.
Step 3	**cts role-based enforcement** **Example:** `Device(config-wireless-flex-profile)# cts role-based enforcement`	Enables role-based access control enforcement for the AP.
Step 4	**cts inline-tagging** **Example:** `Device(config-wireless-flex-profile)# cts inline-tagging`	Enables inline tagging on the AP.
Step 5	**cts profile** *profile-name* **Example:** `Device(config-wireless-flex-profile)# cts profile xyz-profile`	Enables the CTS profile name.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Device(config-wireless-flex-profile)# exit`	Returns to global configuration mode.
Step 7	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site xyz-site`	Configures a site tag and enters site tag configuration mode.
Step 8	**flex-profile** *flex-profile-name* **Example:** `Device(config-site-tag)# flex-profile xyz-flex-profile`	Configures a flex profile.
Step 9	**exit** **Example:** `Device(config-site-tag)# exit`	Returns to global configuration mode.
Step 10	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures an AP and enters AP profile configuration mode.
Step 11	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag xyz-site`	Maps a site tag to an AP.

What to do next

Use the **show cts ap sgt-info** *ap-name*command to verify the SGACL configuration on the AP.

Enabling SGACL Policy Enforcement Globally (CLI)

You must enable SGACL policy enforcement globally on Cisco Catalyst 9800 Series Wireless Controller. The same configuration commands that are used for enforcement of IPv4 traffic apply for IPv6 traffic as well.

Procedure

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

	Command or Action	Purpose
Step 2	**cts role-based enforcement** **Example:** `Device(config)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.

Enabling SGACL Policy Enforcement Per Interface (CLI)

After enabling the SGACL policy enforcement globally, you will have to enable Cisco TrustSec-on the uplink interfaces.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface gigabitethernet** *interface number* **Example:** `Device(config)# interface gigabitethernet 1`	Specifies interface on which to enable or disable SGACL enforcement.
Step 3	**cts role-based enforcement** **Example:** `Device(config-if)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.
Step 4	**do show cts interface** **Example:** `Device(config-if)# do show cts interface`	Verifies that SGACL enforcement is enabled.

Manually Configure a Device SGT (CLI)

In normal Cisco TrustSec operation, the authentication server assigns an SGT to the device for packets originating from the device. You can manually configure an SGT to be used if the authentication server is not accessible, but an authentication server-assigned SGT will take precedence over a manually-assigned SGT.

Procedure

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

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 3	**cts sgt** *sgt-value* **Example:** `Device(config-wireless-policy)# cts stg 200`	Specifies the Security Group Tag (SGT) number. Valid values are from 0 to 65,535.
Step 4	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.

Configuring SGACL, Inline Tagging, and SGT in Local Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the Policy Profile Name. The **Edit Policy Profile** is displayed.

Step 3 Choose **General** tab.

Step 4 In the **CTS Policy** settings, check or uncheck the **Inline Tagging** and **SGACL Enforcement** check boxes, and enter the **Default SGT** value.

Step 5 Click **Update & Apply to Device**.

Configuring SGACL, Inline Tagging, and SGT in Local Mode

Procedure

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

	Command or Action	Purpose
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy xyz-policy-profile`	Creates a policy profile for the WLAN.
Step 3	**cts inline-tagging** **Example:** `Device(config-wireless-policy)# cts inline-tagging`	Enables CTS inline tagging. **Note** You will also need to configure the **cts manual** in the physical interface. If the **cts manual** is configured in the physical interface and **cts inline-tagging** is skipped, the packets will still remain tagged at egress in the controller.
Step 4	**cts role-based enforcement** **Example:** `Device(config-wireless-policy)# cts role-based enforcement`	Enables CTS SGACL enforcement.
Step 5	**cts sgt** *sgt-value* **Example:** `Device(config-wireless-policy)# cts sgt 100`	(Optional) Sets the default Security Group Tag (SGT). **Note** SGT is required for a user session only when the client uses open authentication, and not the ISE server.

Configuring ISE for TrustSec

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**radius server** *server-name* **Example:** `Device(config)# radius server Test-SERVER1`	Specifies the RADIUS server name.
Step 3	**address ipv4** *ip address* **Example:**	Specifies the primary RADIUS server parameters.

	Command or Action	Purpose
	`Device(config-radius-server)# address ipv4 124.3.50.62`	
Step 4	**pac key** *key* **Example:** `Device(config-radius-server)# pac key cisco`	Specify the authentication and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server.
Step 5	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to the configuration mode.
Step 6	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius authc-server-group`	Creates a radius server-group identification.
Step 7	**cts authorization list** *mlist-name* **Example:** `Device(config)# cts authorization list authc-list`	Creates a CTS authorization list.
Step 8	**aaa authorization network** *mlist-name* **group** *name* **Example:** `Device(config)# aaa authorization network default group group1`	Creates an authorization method list for web-based authorization. **Note** Ensure that the ISE IP address configured on your controller is the same as the IP address configured on ISE (**Work Center** > **TrustSec** > **Components** > **Trustsec AAA Servers**)

Verifying Cisco TrustSec Configuration

To display the wireless CTS SGACL configuration summary, use the following command:

```
Device# show wireless cts summary

Local Mode CTS Configuration

Policy Profile Name               SGACL Enforcement     Inline-Tagging   Default-Sgt
-------------------------------------------------------------------------------------
xyz-policy                        DISABLED              ENABLED          0
wireless-policy1                  DISABLED              DISABLED         0
w-policy-profile1                 DISABLED              DISABLED         0
default-policy-profile            DISABLED              DISABLED         0


Flex Mode CTS Configuration
```

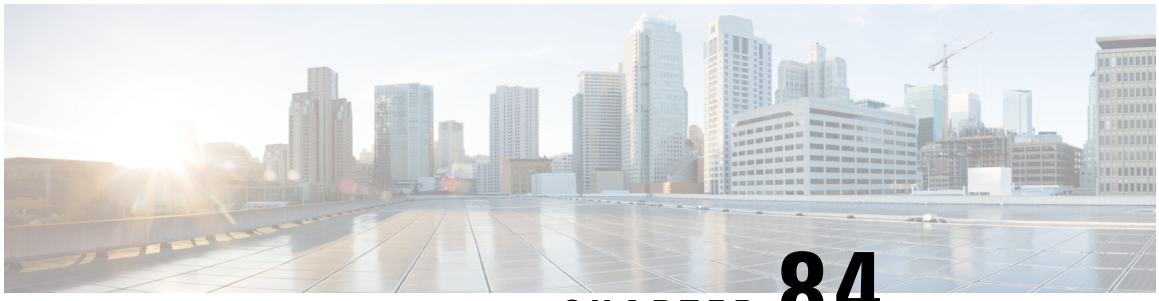
```
Flex Profile Name                SGACL Enforcement     Inline-Tagging
------------------------------------------------------------------------
xyz-flex                         DISABLED              ENABLED
demo-flex                        DISABLED              DISABLED
flex-demo                        DISABLED              DISABLED
xyz-flex-profile                 DISABLED              DISABLED
default-flex-profile             DISABLED              DISABLED
```

To display CTS-specific configuration status for various wireless profiles, use the following command:

```
Device# show cts wireless profile policy xyz-policy

Policy Profile Name           : xyz-policy
CTS
  Role-based enforcement         : ENABLED
  Inline-tagging                 : ENABLED
   Default SGT   : 100

Policy Profile Name            : foo2
CTS
  Role-based enforcement         : DISABLED
  Inline-tagging                 : ENABLED
  Default SGT           : NOT-DEFINED

Policy Profile Name                    : foo3
CTS
  Role-based enforcement         : DISABLED
  Inline-tagging                 : DISABLED
  Default SGT    : 65001
```

To display CTS configuration for a given wireless profile, use the following command:

```
Device# show wireless profile policy detailed xyz-policy

Policy Profile Name           : xyz-policy
Description                   :
Status                        : DISABLED
VLAN                          : 1
Client count                  : 0
Passive Client                : DISABLED
ET-Analytics                  : DISABLED
StaticIP Mobility             : DISABLED
!
.
.
.WGB Policy Params
  Broadcast Tagging           : DISABLED
  Client VLAN                 : DISABLED
Mobility Anchor List
  IP Address                                 Priority
CTS
  Role-based enforcement         : ENABLED
  Inline-tagging                 : ENABLED
  Default SGT                   : NOT-DEFINED
```



CHAPTER 84

SGT Inline Tagging and SXPv4

- Introduction to SGT Inline Tagging on AP and SXPv4, on page 751
- Creating an SXP Profile, on page 751
- Configuring SGT Inline Tagging on Access Points, on page 752
- Configuring an SXP Connection (GUI), on page 752
- Configuring an SXP Connection, on page 753
- Verifying SGT Push to Access Points, on page 754

Introduction to SGT Inline Tagging on AP and SXPv4

The Cisco TrustSec (CTS) builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms.

The Scalable Group Tag (SGT) Exchange Protocol (SXP) is one of the several protocols that support CTS. CTS SXP version 4 (SXPv4) enhances the functionality of SXP by adding a loop detection mechanism to prevent stale binding in the network. In addition, Cisco TrustSec supports SGT inline tagging which allows propagation of SGT embedded in clear-text (unencrypted) ethernet packets.

When a wireless client is connected and is authenticated by ISE, the IP-SGT binding is generated on the controller . The same SGT is pushed to the AP along with the other client details.

For more details on SGT inline tagging on the AP and SXPv4, see the **Cisco TrustSec Configuration Guide** at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-3s/sec-usr-cts-xe-3s-book/sec-cts-sxpv4.html

Creating an SXP Profile

Procedure

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

	Command or Action	Purpose
Step 2	**wireless cts-sxp profile** *profile-name* **Example:** `Device(config)# wireless cts-sxp profile rr-profile`	Configures a wireless CTS profile and enters cts-sxp profile configuration mode.
Step 3	**cts sxp enable** **Example:** `Device(config-cts-sxp-profile)# cts sxp enable`	Enables SXP for Cisco TrustSec.

Configuring SGT Inline Tagging on Access Points

Follow the procedure given below to configure SGT inline tagging on APs:

Before you begin

- The SGTs pushed to the AP for inline tagging will only be from dynamic SGT allocation through ISE authentication. It is not supported for static bindings configured on the controller .
- SGTs will be pushed to an AP only when it is operating in flex mode.

To know the list of Cisco APs that support SGT inline tagging, see the release notes: https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-release-notes-list.html

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex rr-xyz-flex-profile`	Configures a wireless flex profile and enters the wireless flex profile configuration mode.
Step 3	**cts inline-tagging** **Example:** `Device(config-wireless-flex-profile)# cts inline-tagging`	Enables inline-tagging on the AP.

Configuring an SXP Connection (GUI)

Perform the following steps to set SXP global configuration.

Procedure

Step 1 In the **Global** section, select the **SXP Enabled** check box to enable SXP.
Step 2 Enter an IP address in the **Default Source IP** field.
Step 3 Enter a value in the **Reconciliation Period (sec)** field.
Step 4 Enter a value in the **Retry Period (sec)** field.
Step 5 Select the **Set New Default Password** check box. Selecting this check box displays the **Password Type** and **Enter Password** fields.
Step 6 Choose any one of the available types from the **Password Type** drop-down list.
Step 7 Enter a value in the **Enter Password** field.
Step 8 Click the **Apply** button.
Step 9 In the **Peer** section, click the **Add** button.
Step 10 Enter an IP address in the **Peer IP** field.
Step 11 Enter an IP address in the **Source IP** field.
Step 12 Choose any one of the available types from the **Password** drop-down list.
Step 13 Choose any one of the available types from the **Mode of Local Device** drop-down list.
Step 14 Click the **Save & Apply to Device** button.
Step 15 In the **AP** tab, click the **Add** button. The **Add SXP AP** dialog box appears.
Step 16 Enter a name for the profile in the **Profile Name** field.
Step 17 Set the **Status** field to **Enabled** to enable AP.
Step 18 Enter a value in the **Default Password** field.
Step 19 Enter a value (in seconds) for the **CTS Speaker Seconds, CTS Recon Period, CTS Retry Period, CTS Listener Maximum**, and **CTS Listener Minimum**
Step 20 In the **CTS SXP Profile Connections** section, click **Add**.
Step 21 Enter an IP address in the **Peer IP** field.
Step 22 Choose any one of the modes from the **Connection Mode** drop-down list. The available modes are **Both**, **Listener**, and **Speaker**.
Step 23 From the **Password Type** drop-down list, choose either **None** or **Default**.
Step 24 Click the **Add** button.
Step 25 Click the **Save & Apply to Device** button.

Configuring an SXP Connection

Follow the procedure given below to configure an SXP connection:

Procedure

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

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**cts sxp enable** **Example:** `Device(config)# cts sxp enable`	Enables CTS SXP support.
Step 3	**cts sxp connection peer** *ipv4-address* **password none mode local speaker** **Example:** `Device(config)# cts sxp connection peer 1.1.1.1 password none mode local speaker`	Configures the CTS-SXP peer address connection. **Note** The password need not be *none* always and the mode can either be Speaker or Listener, or Both.

What to do next

Use the following command to verify the configuration:

```
Device# show running-config | inc sxp
```

Verifying SGT Push to Access Points

When a wireless client is connected and authenticated by ISE, the IP-SGT binding is generated on the controller . This can be verified using the following commands:

```
Device# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
1.1.1.1                 100     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of active   bindings = 1
```

Use the following command to verify the SXP connections status:

```
Device# show cts sxp connections

 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Not Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set
----------------------------------------------
Peer IP          : 40.1.1.1
Source IP        : 40.1.1.2
Conn status      : On
Conn version     : 4
```

```
Conn capability  : IPv4-IPv6-Subnet
Conn hold time   : 120 seconds
Local mode       : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: none
Hold timer is running
Duration since last state change: 0:00:00:06 (dd:hr:mm:sec)


Total num of SXP Connections = 1
```

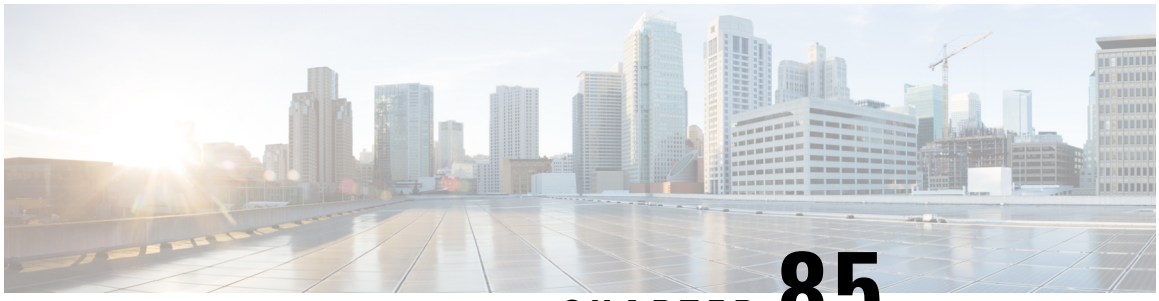
Use the following command to see the bindings learnt over SXP connection:

```
Device# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
1.1.1.1                 100     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of active   bindings = 1
```

Use the following commands on the AP to check the status of inline tagging on the AP and its IP-SGT bindings:

```
AP# show capwap client rcb

AdminState                          : ADMIN_ENABLED
OperationState                      : UP
Name                                : AP2C33.1185.C4D0
SwVer                               : 16.6.230.41
HwVer                               : 1.0.0.0
MwarApMgrIp                         : 9.3.72.38
MwarName                            : mohit-ewlc
MwarHwVer                           : 0.0.0.0
Location                            : default location
ApMode                              : FlexConnect
ApSubMode                           : Not Configured
CAPWAP Path MTU                     : 1485
CAPWAP UDP-Lite                     : Enabled
IP Prefer-mode                      : IPv4
AP Link DTLS Encryption             : OFF
AP TCP MSS Adjust                   : Disabled
LinkAuditing                        : disabled
Efficient Upgrade State             : Disabled
Flex Group Name                     : anrt-flex
AP Group Name                       : default-group
Cisco Trustsec Config
      AP Inline Tagging Mode                : Enabled
! The status can be Enabled or Disabled and is based on the tag that is pushed to the AP.
      AP Sgacl Enforcement                  : Disabled
      AP Override Status                    : Disabled


AP# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information
        IP SGT SOURCE
9.3.74.101  17  LOCAL
```

```
IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of active   bindings = 1

Active IPv6-SGT Bindings Information
                      IP SGT SOURCE
fe80::c1d5:3da2:dc96:757d  17  LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of active   bindings = 1
```



CHAPTER 85

Locally Significant Certificates

- Information About Locally Significant Certificates, on page 757
- Restrictions for Locally Significant Certificates, on page 759
- Provisioning Locally Significant Certificates, on page 759
- Verifying LSC Configuration, on page 768
- Configuring Management Trustpoint to LSC (GUI), on page 769
- Configuring Management Trustpoint to LSC (CLI), on page 769

Information About Locally Significant Certificates

This module explains how to configure the Cisco Catalyst 9800 Series Wireless Controller and Lightweight Access Points (LAPs) to use the Locally Significant Certificate (LSC). If you choose the Public Key Infrastructure (PKI) with LSC, you can generate the LSC on the APs and controllers. You can then use the certificates to mutually authenticate the controllers and the APs.

In Cisco controllers, you can configure the controller to use an LSC. Use an LSC if you want your own PKI to provide better security, have control of your Certificate Authority (CA), and define policies, restrictions, and usages on the generated certificates.

You need to provision the new LSC certificate on the controller and then the Lightweight Access Point (LAP) from the CA Server.

The LAP communicates with the controller using the CAPWAP protocol. Any request to sign the certificate and issue the CA certificates for LAP and controller itself must be initiated from the controller. The LAP does not communicate directly with the CA server. The CA server details must be configured on the controller and must be accessible.

The controller makes use of the Simple Certificate Enrollment Protocol (SCEP) to forward certReqs generated on the devices to the CA and makes use of SCEP again to get the signed certificates from the CA.

The SCEP is a certificate management protocol that the PKI clients and CA servers use to support certificate enrollment and revocation. It is widely used in Cisco and supported by many CA servers. In SCEP, HTTP is used as the transport protocol for the PKI messages. The primary goal of SCEP is the secure issuance of certificates to network devices. SCEP is capable of many operations, but for our release, SCEP is utilized for the following operations:

- CA and Router Advertisement (RA) Public Key Distribution
- Certificate Enrollment

Certificate Provisioning in Controllers

The new LSC certificates, both CA and device certificates, must be installed on the controller.

With the help of SCEP, CA certificates are received from the CA server. During this point, there are no certificates in the controller. After the **get** operation of obtaining the CA certificates, are installed on the controller. The same CA certificates are also pushed to the APs when the APs are provisioned with LSCs.

Note We recommend that you use a new RSA keypair name for the newly configured PKI certificate. If you want to reuse an existing RSA keypair name (that is associated with an old certificate) for a new PKI certificate, do either of the following:

- Do not regenerate a new RSA keypair with an existing RSA keypair name, reuse the existing RSA keypair name. Regenerating a new RSA keypair with an existing RSA keypair name will make all the certificates associated with the existing RSA keypair invalid.
- Manually remove the old PKI certificate configurations first, before reusing the existing RSA keypair name for the new PKI certificate.

Device Certificate Enrollment Operation

For both the LAP and the controller that request a CA-signed certificate, the certRequest is sent as a PKCS#10 message. The certRequest contains the Subject Name, Public Key, and other attributes to be included in the X.509 certificate, and must be digitally signed by the Private Key of the requester. These are then sent to the CA, which transforms the certRequest into an X.509 certificate.

The CA that receives a PKCS#10 certRequest requires additional information to authenticate the requester's identity and verify if the request is unaltered. (Sometimes, PKCS#10 is combined with other approaches, such as PKCS#7 to send and receive the certificate request or response.)

The PKCS#10 is wrapped in a PKCS#7 Signed Data message type. This is supported as part of the SCEP client functionality, while the PKCSReq message is sent to the controller. Upon successful enrollment operation, both the CA and device certificates are available on the controller.

Certificate Provisioning on Lightweight Access Point

In order to provision a new certificate on LAP, while in CAPWAP mode, the LAP must be able to get the new signed X.509 certificate. In order to do this, it sends a certRequest to the controller, which acts as a CA proxy and helps obtain the certRequest signed by the CA for the LAP.

The certReq and the certResponses are sent to the LAP with the LWAPP payloads.

Both the LSC CA and the LAP device certificates are installed in the LAP, and the system reboots automatically. The next time when the system comes up, because it is configured to use LSCs, the AP sends the LSC device certificate to the controller as part of the JOIN Request. As part of the JOIN Response, the controller sends the new device certificate and also validates the inbound LAP certificate with the new CA root certificate.

What to Do Next

To configure, authorize, and manage certificate enrollment with the existing PKI infrastructure for controller and AP, you need to use the LSC provisioning functionality.

Restrictions for Locally Significant Certificates

- LSC workflow is different in FIPS+WLANCC mode. CA server must support Enrollment over Secure Transport (EST) protocol and should be capable of issuing EC certificates in FIPS+WLANCC mode.
- Elliptic Curve Digital Signature Algorithm (ECDSA) cipher works only if both AP and controller are having EC certificates, provisioned with LSC.
- EC certificates (LSC-EC) can be provisioned only if CA server supports EST (and not SCEP).
- FIPS + CC security modes is required to be configured in order to provision EC certificate.

Provisioning Locally Significant Certificates

Configuring RSA Key for PKI Trustpoint

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto key generate rsa** [**exportable**] **general-keys modulus** *key_size* **label** *RSA_key* **Example:** `Device(config)# crypto key generate rsa exportable general-keys modulus 2048 label lsc-tp`	Configures RSA key for PKI trustpoint. **exportable** is an optional keyword. You may or may not want to configure an exportable-key. If selected, you can export the key out of the box, if required • *key_size*: Size of the key modulus. The valid range is from 2048 to 4096. • *RSA_key*: RSA key pair label.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring PKI Trustpoint Parameters

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto pki trustpoint** *trustpoint_name* **Example:** `Device(config)# crypto pki trustpoint microsoft-ca`	Creates a new trustpoint for an external CA server. Here, *trustpoint_name* refers to the trustpoint name.
Step 3	**enrollment url** *HTTP_URL* **Example:** `Device(ca-trustpoint)# enrollment url http://CA_server/certsrv/mscep/mscep.dll`	Specifies the URL of the CA on which your router should send certificate requests. **url** *url*: URL of the file system where your router should send certificate requests. An IPv6 address can be added in the URL enclosed in brackets. For example: http://[2001:DB8:1:1::1]:80. For more enrollment method options, see the enrollment url (ca-trustpoint) command page.
Step 4	**subject-name** *subject_name* **Example:** `Device(ca-trustpoint)# subject-name C=IN, ST=KA, L=Bengaluru, O=Cisco, CN=eagle-eye/emailAddress=support@abc.com`	Creates subject name parameters for the trustpoint.
Step 5	**rsakeypair** *RSA_key key_size* **Example:** `Device(ca-trustpoint)# rsakeypair ewlc-tp1`	Maps RSA key with that of the trustpoint. • *RSA_key*: RSA key pair label. • *key_size*: Signature key length. Range is from 360 to 4096.
Step 6	**revocation** {**crl** | **none** | **ocsp**} **Example:** `Device(ca-trustpoint)# revocation none`	Checks revocation.
Step 7	**end** **Example:** `Device(ca-trustpoint)# end`	Returns to privileged EXEC mode.

Authenticating and Enrolling a PKI Trustpoint (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **PKI Management**.

Step 2 In the **PKI Management** window, click the **Trustpoints** tab.

Step 3 In the **Add Trustpoint** dialog box, provide the following information:

a) In the **Label** field, enter the RSA key label.
b) In the **Enrollment URL** field, enter the enrollment URL.
c) Check the **Authenticate** check box to authenticate the Public Certificate from the enrollment URL.
d) In the **Subject Name** section, enter the **Country Code**, **State**, **Location**, **Organisation**, **Domain Name**, and **Email Address**.
e) Check the **Key Generated** check box to view the available RSA keypairs. Choose an option from the **Available RSA Keypairs** drop-down list.
f) Check the **Enroll Trustpoint** check box.
g) In the **Password** field, enter the password.
h) In the **Re-Enter Password** field, confirm the password.
i) Click **Apply to Device**.

The new trustpoint is added to the trustpoint name list.

Authenticating and Enrolling the PKI Trustpoint with CA Server (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto pki authenticate** *trustpoint_name* **Example:** `Device(config)# crypto pki authenticate microsoft-ca`	Fetches the CA certificate.

Step 3	**yes**
	Example:
	`Device(config)# % Do you accept this certificate? [yes/no]:`
	`yes Trustpoint CA certificate accepted.`	

Step 4	**crypto pki enroll** *trustpoint_name* **Example:**	Enrolls the client certificate.

	Command or Action	Purpose

	`Device(config)# crypto pki enroll microsoft-ca`
	`%`
	`% Start certificate enrollment ..`
	`% Create a challenge password. You will need to verbally`
	`provide this password to the CA Administrator in order to`
	`revoke your certificate. For security reasons your password`
	`will not be saved in the configuration.`
	`Please make a note of it.`	

Step 5	**password** **Example:** `Device(config)# abcd123`	Enters a challenge password to the CA server.
Step 6	**password** **Example:** `Device(config)# abcd123`	Re-enters a challenge password to the CA server.

Step 7	**yes**
	Example:
	`Device(config)# % Include the router serial number`
	`in the subject name? [yes/no]: yes`	

Step 8	**no**
	Example:
	`Device(config)# % Include an IP address`
	`in the subject name? [no]: no`	

Step 9	**yes**
	Example:
	`Device(config)#`
	`Request certificate from CA? [yes/no]: yes`
	`% Certificate request sent to Certificate Authority`
	`% The 'show crypto pki certificate verbose`
	`client' command will show the fingerprint.`	

Step 10	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring AP Join Attempts with LSC Certificate (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **All Access Points** window, click the LSC Provision name.

Step 3 From the **Status** drop-down list, choose a status to enable LSC.

Step 4 From the **Trustpoint Name** drop-down list, choose the trustpoint.

Step 5 In the **Number of Join Attempts** field, enter the number of retry attempts that will be permitted.

Step 6 Click **Apply**.

Configuring AP Join Attempts with LSC Certificate (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision join-attempt** *number_of_attempts* **Example:** `Device(config)# ap lsc-provision join-attempt 10`	Specifies the maximum number of AP join failure attempts with the newly provisioned LSC certificate. When the number of AP joins exceed the specified limit, AP joins back with the Manufacturer Installed Certificate (MIC).
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Subject-Name Parameters in LSC Certificate

Procedure

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

	Command or Action	Purpose
Step 2	**ap lsc-provision subject-name-parameter country** *country-str* **state** *state-str* **city** *city-str* **domain** *domain-str* **org** *org-str* **email-address** *email-addr-str* **Example:** `Device(config)# ap lsc-provision subject-name-parameter country India state Karnataka city Bangalore domain domain1 org Right email-address adc@gfe.com`	Specifies the attributes to be included in the subject-name parameter of the certificate request generated by an AP.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring Key Size for LSC Certificate

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision key-size** { **2048** | **3072** | **4096}**} **Example:** `Device(config)# ap lsc-provision key-size 2048`	Specifies the size of keys to be generated for the LSC on AP.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Trustpoint for LSC Provisioning on an Access Point

Procedure

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

	Command or Action	Purpose
Step 2	**ap lsc-provision trustpoint** *tp-name* **Example:** `Device(config)# ap lsc-provision trustpoint microsoft-ca`	Specifies the trustpoint with which the LCS is provisioned to an AP. *tp-name*: The trustpoint name.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring an AP LSC Provision List (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **All Access Points** window, click the corresponding LSC Provision name.

Step 3 From the **Status** drop-down list, choose a status to enable LSC.

Step 4 From the **Trustpoint Name** drop-down list, choose a trustpoint.

Step 5 In the **Number of Join Attempts** field, enter the number of retry attempts that are allowed.

Step 6 From the **Key Size** drop-down list, choose a key.

Step 7 In the **Edit AP Join Profile** window, click the **CAPWAP** tab.

Step 8 In the **Add APs to LSC Provision List** section, click **Select File** to upload the CSV file that contains AP details.

Step 9 Click **Upload File**.

Step 10 In the **AP MAC Address** field, enter the AP MAC address. and add them. (The APs added to the provision list are displayed in the **APs in provision List** .)

Step 11 In the **Subject Name Parameters** section, enter the following details:

- **Country**
- **State**
- **City**
- **Organisation**
- **Department**
- **Email Address**

Step 12 Click **Apply**.

Configuring an AP LSC Provision List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision mac-address** *mac-addr* **Example:** `Device(config)# ap lsc-provision mac-address 001b.3400.02f0`	Adds the AP to the LSC provision list. **Note** You can provision a list of APs using the **ap lsc-provision provision-list** command. (Or) You can provision all the APs using the **ap lsc-provision** command.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring LSC Provisioning for all the APs (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Access Points** window, expand the **LSC Provision** section.

Step 3 Set **Status** to **Enabled** state.

Note If you set **Status** to **Provision List**, LSC provisioning will be configured only for APs that are a part of the provision list.

Step 4 From the **Trustpoint Name** drop-down list, choose the appropriate trustpoint for all APs.

Step 5 In the **Number of Join Attempts** field, enter the number of retry attempts that the APs can make to join the controller.

Step 6 From the **Key Size** drop-down list, choose the appropriate key size of the certificate:

- **2048**
- **3072**
- **4096**

Step 7 In the **Add APs to LSC Provision List** section, click **Select File** to upload the CSV file that contains the AP details.

Step 8 Click **Upload File**.

Step 9 In the **AP MAC Address** field, enter the AP MAC address. (The APs that are added to the provision list are displayed in the **APs in Provision List** section.)

Step 10 In the **Subject Name Parameters** section, enter the following details:

a. **Country**

b. **State**

c. **City**

d. **Organization**

e. **Department**

f. **Email Address**

Step 11 Click **Apply**.

Configuring LSC Provisioning for All APs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision** **Example:** `Device(config)# ap lsc-provision`	Enables LSC provisioning for all APs. By default, LSC provisioning is disabled for all APs.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring LSC Provisioning for the APs in the Provision List

Procedure

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

	Command or Action	Purpose
Step 2	**ap lsc-provision provision-list** **Example:** `Device(config)# ap lsc-provision provision-list`	Enables LSC provisioning for a set of APs configured in the provision list.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying LSC Configuration

To view the details of the wireless management trustpoint, use the following command:

```
Device# show wireless management trustpoint

Trustpoint  Name : microsoft-ca
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : 9e5623adba5307facf778e6ea2f5082877ea4beb
 Private key Info : Available
```

To view the LSC provision-related configuration details for an AP, use the following command:

```
Device# show ap lsc-provision summary

AP LSC-provisioning : Disabled
Trustpoint used for LSC-provisioning : microsoft-ca
LSC Revert Count in AP reboots : 10

AP LSC Parameters :
Country : IN
State : KA
City : BLR
Orgn : ABC
Dept : ABC
Email : support@abc.com
Key Size : 2048

AP LSC-provision List : Enabled
Total number of APs in provision list: 3

Mac Address
-----------
0038.df24.5fd0
2c5a.0f22.d4ca
e4c7.22cd.b74f
```

Configuring Management Trustpoint to LSC (GUI)

Procedure

Step 1 Choose **Administration** > **Management** > **HTTP/HTTPS**.

Step 2 In the **HTTP Trust Point Configuration** section, set **Enable Trust Point** to the **Enabled** state.

Step 3 From the **Trust Points** drop-down list, choose the appropriate trustpoint.

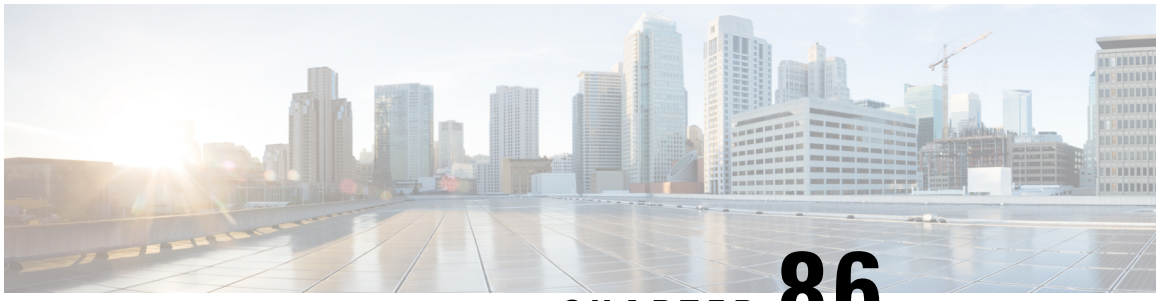
Step 4 Save the configuration.

Configuring Management Trustpoint to LSC (CLI)

After LSC provisioning, the APs will automatically reboot and join at the LSC mode after bootup. Similarly, if you remove the AP LSC provisioning, the APs reboot and join at non-LSC mode.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless management trustpoint** *trustpoint_name* **Example:** `Device(config)# wireless management trustpoint microsoft-ca`	Configures the management trustpoint to LSC.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.



CHAPTER 86

Cisco Umbrella WLAN

- Information About Cisco Umbrella WLAN, on page 771
- Registering Controller to Cisco Umbrella Account, on page 772
- Configuring Cisco Umbrella WLAN, on page 773
- Verifying the Cisco Umbrella Configuration, on page 778

Information About Cisco Umbrella WLAN

The Cisco Umbrella WLAN 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 the following:

- Policy configuration per user group at a single point.
- Policy configuration per network, group, user, device, or IP address.

  The following is the 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.

Registering Controller to Cisco Umbrella Account

Before you Begin

- You should have an account with Cisco Umbrella.
- You should have an API token from Cisco Umbrella.

This section describes the process followed to register the controller to the Cisco Umbrella account.

The controller is registered to Cisco Umbrella server using the Umbrella parameter map. Each of the Umbrella parameter map must have an API token. The Cisco Umbrella responds with the device ID for the controller . The device ID has a 1:1 mapping with the Umbrella parameter map name.

Fetching API token for Controller from Cisco Umbrella Dashboard

From Cisco Umbrella dashboard, verify that your controller shows up under Device Name, along with their identities.

Applying the API Token on Controller

Registers the Cisco Umbrella API token on the network.

DNS Query and Response

Once the device is registered and Umbrella parameter map is configured on WLAN, the DNS queries from clients joining the WLAN are redirected to the Umbrella DNS resolver.

Note This is applicable for all domains not configured in the local domain RegEx parameter map.

The queries and responses are encrypted based on the DNScrypt option in the Umbrella parameter map.

For more information on the Cisco Umbrella configurations, see the Integration for ISR 4K and ISR 1100 – Security Configuration Guide.

Limitations and Considerations

The limitations and considerations for this feature are as follows:

- You will be able to apply the wireless Cisco Umbrella profiles to wireless entities, such as, WLAN or AP groups, if the device registration is successful.
- In case of L3 mobility, the Cisco Umbrella must be applied on the anchor controller always.
- When two DNS servers are configured under DHCP, two Cisco Umbrella server IPs are sent to the client from DHCP option 6. If only one DNS server is present under DHCP, only one Cisco Umbrella server IP is sent as part of DHCP option 6.

Configuring Cisco Umbrella WLAN

To configure Cisco Umbrella on the controller , perform the following:

- You must have the API token from the Cisco Umbrella dashboard.
- You must have the root certificate to establish HTTPS connection with the Cisco Umbrella registration server: api.opendns.com. You must import the root certificate from **digicert.com** to the controller using the **crypto pki trustpool import terminal** command.

Importing CA Certificate to the Trust Pool

Before you begin

The following section covers details about how to fetch the root certificate and establish HTTPS connection with the Cisco Umbrella registration server:

Procedure

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

Step 2	Perform either of the following tasks:
	• **crypto pki trustpool import url** *url*
	`Device(config)# crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b`
	Imports the root certificate directly from the Cisco website.
	Note The Trustpool bundle contains the root certificate of *digicert.com* together with other CA certificates.
	• **crypto pki trustpool import terminal**
	`Device(config)# crypto pki trustpool import terminal`
	Imports the root certificate by executing the import terminal command.
	• Enter PEM-formatted CA certificate from the following location: See the Related Information section to download the CA certificate.	

	Command or Action	Purpose
	-----BEGIN CERTIFICATE----- MIIFjCCA3agAwIBAgIQCJLWpkvF9KlwA3TANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQG EwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQu b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMB4XDTEzMDMwODEyMDAw MFoXDTIzMDMwODEyMDAwMFowTTELMAkGA1UEBhMCVVMxFTATBgNVBAoTDERpZ2lDZXJU IEluYy4xJzAlBgNVBAMTHkRpZ2lDZXJUIFNIQ1VSRSBTZXJ2ZXIgQ0EgRzMwggEiMA0G CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDPv+gyC8LOBUfNZI6qCEGVenZlfuzxBG3/ Fbhp2w1HIQNiSwDaOCSl1ZHalb4J+faONfrfX3YnZlj+ZX1cJwfSj4dK2kbnGd6SG0zh VFLaRX+Sdw+fRtRKQCLjzWxi7n6/8SmKSp+odtXXpC4HvGiqjGoDPz7GEIMePMVcoGtQ mufQ8hAcr6N1kDGcb6LHglv4Subo01yoA0KAWSDu6wn2TWUPwxwG8aONi7gyEJXvxxCy ke73SNkhnaJpAgMBAAGjggFWMIIBUjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRB 5kbS4LkwLCoWX1zGskRUAEa6tDAfBgNVHSMEGDAWgBROIFVBuetPpiS1XHBJ9jCrEWsj qDAOBgNVHQ8BAf8EBAMCAYYwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMHYG CCsGAQUFBwEBBGowaDAkBggrBgEFBQcwAYYYaHR0cDovL29jc3AuZGlnaWNlcnQuY29t MEAGCCsGAQUFBzAChjRodHRwOi8vY2FjZXJ0cy5kaWdpY2VydC5jb20vRGlnaUNlcnRH bG9iYWxSb290Q0EuY3J0MEIGA1UdHwQ7MDkwN6A1oDOGMWh0dHA6Ly9jcmwzLmRpZ2lj ZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAA MCowKAYIKwYBBQUHAgEWHGh0dHBzOi8vd3d3LmRpZ2ljZXJ0LmNvbS9DUFMwDQYJKoZI hvcNAQELBQADggEBAMbuW+rl+cdFYbPe801IdcAkxCPGKwV4a6pMxwpd69P2zLtg/Vj/ 4+Z3p0Wv6ne6L8B/UP/jo4ToSFXsur3hW1Sio7VUCd4Bdz+/TiOghyl9HeKQGskBrgRp L+bvxS6cmObdY+nZ+FLIvvksx3jNDyO3Vhq8ErR3gSGySvWecCMecsGq6tXvzbLkLcR4 VG5SiUVpNk+tDom3ykVDN/7NfrnXO1fTGFUzpbwqbwp1Ub67wtRaZDTJ8ivdCaY0oi3C 1MxTFcuBHmiwfnkFzTZEwhNcW4wzJ5FTAJbUWLbSemN/xffsZGVb9VcwFbXcGCe1YT3t Yr8tCWoxpfVFsIT8dC/+3ZmvBV0KSwlk8a706mihpG1rXI4SINMwSyvcyLzir8SPr2rv SaZMkE4f97Q= -----END CERTIFICATE----- Imports the root certificate by pasting the CA certificate from the **digicert.com**.	
Step 3	**quit** **Example:** `Device(config)# quit`	Imports the root certificate by entering the **quit** command. **Note** You will receive a message after the certificate has been imported.

Creating a Local Domain RegEx Parameter Map

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type regex** *parameter-map-name* **Example:** `Device(config)# parameter-map type regex dns_wl`	Creates a regex parameter map.
Step 3	**pattern** *regex-pattern*	Configures the regex pattern to match.

	Command or Action	Purpose
	Example: `Device(config-profile)# pattern www.google.com`	**Note** The following patterns are supported: • Begins with `.*`. For example: **`.*facebook.com`** • Begins with `.*` and ends with `*` . For example: **`.*google*`** • Ends with `*`. For example: **`www.facebook*`** • No special character. For example: **`www.facebook.com`**
Step 4	**end** **Example:** `Device(config-profile)# end`	Returns to privileged EXEC mode.

Configuring Parameter Map Name in WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.
Step 2 Click on the Policy Profile Name. The **Edit Policy Profile** window is displayed.
Step 3 Choose the **Advanced** tab.
Step 4 In the **Umbrella** settings, from the **Umbrella Parameter Map** drop-down list, choose the parameter map.
Step 5 Enable or disable **Flex DHCP Option for DNS** and **DNS Traffic Redirect** toggle buttons.
Step 6 Click **Update & Apply to Device**.

Configuring the Umbrella Parameter Map

Procedure

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

	Command or Action	Purpose
Step 2	**parameter-map type umbrella global** **Example:** `Device(config)# parameter-map type umbrella global`	Creates an umbrella global parameter map.
Step 3	**token** *token-value* **Example:** `Device(config-profile)# token 5XXXXXXXXCXXXXXXXAXXXXXXXFXXXXCXXXXXXXX`	Configures an umbrella token.
Step 4	**local-domain** *regex-parameter-map-name* **Example:** `Device(config-profile)# local-domain dns_wl`	Configures local domain RegEx parameter map.
Step 5	**resolver** {**IPv4** *X.X.X.X* | **IPv6** *X:X:X:X::X*} **Example:** `Device(config-profile)# resolver IPv6 10:1:1:1::10`	Configures the Anycast address. The default address is applied when there is no specific address configured.
Step 6	**end** **Example:** `Device(config-profile)# end`	Returns to privileged EXEC mode.

Enabling or Disabling DNScrypt (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Threat Defence** > **Umbrella**.

Step 2 Enter the **Registration Token** received from Umbrella. Alternatively, you can click on **Click here to get your Token**to get the token from Umbrella.

Step 3 Enter the **Whitelist Domains** that you want to exclude from filtering.

Step 4 Check or uncheck the **Enable DNS Packets Encryption** check box to encrypt or decrypt the DNS packets.

Step 5 Click **Apply**.

Enabling or Disabling DNScrypt

Procedure

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

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**parameter-map type umbrella global** **Example:** `Device(config)# parameter-map type umbrella global`	Creates an umbrella global parameter map.
Step 3	[**no**] **dnscrypt** **Example:** `Device(config-profile)# no dnscrypt`	Enables or disables DNScrypt. By default, the DNScrypt option is enabled. **Note** Cisco Umbrella DNScrypt is not supported when DNS-encrypted responses are sent in the data-DTLS encrypted tunnel (either mobility tunnel or AP CAPWAP tunnel).
Step 4	**end** **Example:** `Device(config-profile)# end`	Returns to privileged EXEC mode.

Configuring Timeout for UDP Sessions

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type umbrella global** **Example:** `Device(config)# parameter-map type umbrella global`	Creates an umbrella global parameter map.
Step 3	**udp-timeout** *timeout_value* **Example:** `Device(config-profile)# udp-timeout 2`	Configures timeout value for UDP sessions. The *timeout_value* ranges from 1 to 30 seconds. **Note** The **public-key** and **resolver** parameter-map options are automatically populated with the default values. So, you need not change them.
Step 4	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-profile)# end`	

Configuring Parameter Map Name in WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click on the Policy Profile Name. The **Edit Policy Profile** window is displayed.

Step 3 Choose the **Advanced** tab.

Step 4 In the **Umbrella** settings, from the **Umbrella Parameter Map** drop-down list, choose the parameter map.

Step 5 Enable or disable **Flex DHCP Option for DNS** and **DNS Traffic Redirect** toggle buttons.

Step 6 Click **Update & Apply to Device**.

Configuring Parameter Map Name in WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**umbrella-param-map** *umbrella-name* **Example:** `Device(config-wireless-policy)# umbrella-param-map global`	Configures the Umbrella OpenDNS feature for the WLAN.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying the Cisco Umbrella Configuration

To view the Umbrella configuration details, use the following command:

```
Device# show umbrella config
Umbrella Configuration
=======================
Token: 5XXXXXXABXXXXXFXXXXXXXXXXDXXXXXXXXXXXABXX
API-KEY: NONE
OrganizationID: xxxxxxx
Local Domain Regex parameter-map name: dns_bypass
DNSCrypt: Not enabled
Public-key: NONE
UDP Timeout: 5 seconds
Resolver address:
1. 10.1.1.1
2. 5.5.5.5
3. XXXX:120:50::50
4. XXXX:120:30::30
```

To view the Umbrella DNSCrypt details, use the following command:

```
Device# show umbrella dnscrypt
DNSCrypt: Enabled
   Public-key: B111:XXXX:XXXX:XXXX:3E2B:XXXX:XXXX:XXXE:XXX3:3XXX:DXXX:XXXX:BXXX:XXXB:XXXX:FXXX

   Certificate Update Status: In Progress
```

To view the Umbrella global parameter map details, use the following command:

```
Device# show parameter-map type umbrella global
```

To view the regex parameter map details, use the following command:

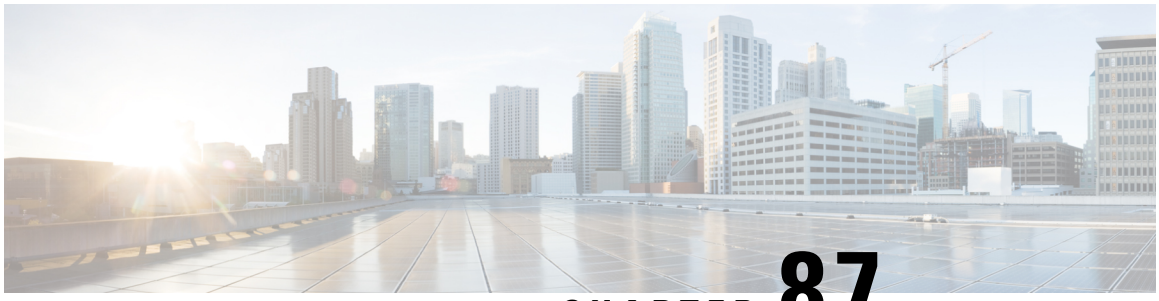
```
Device# show parameter-map type regex <parameter-map-name>
```

To view the Umbrella statistical information, use the following command:

```
Device# show platform hardware chassis active qfp feature umbrella datapath stats
```

To view the Umbrella details on the AP, use the following command:

```
AP#show client opendns summary
Server-IP role
208.67.220.220 Primary
208.67.222.222 Secondary

Server-IP role
2620:119:53::53 Primary
2620:119:35::35 Secondary

Wlan Id DHCP OpenDNS Override Force Mode
0 true false
1 false false
...

15 false false
Profile-name Profile-id
vj-1 010a29b176b34108
global 010a57bf502c85d4
vj-2 010ae385ce6c1256
AP0010.10A7.1000#

Client to profile command

AP#show client opendns address 50:3e:aa:ce:50:17
Client-mac Profile-name
50:3E:AA:CE:50:17 vj-1
AP0010.10A7.1000#
```



CHAPTER 87

FIPS

- FIPS, on page 781
- Guidelines and Restrictions for FIPS, on page 781
- FIPS Self-Tests, on page 782
- Configuring FIPS, on page 783
- Configuring FIPS in HA Setup, on page 783
- Monitoring FIPS, on page 784
- CC, on page 785

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.

With FIPS in enabled state, some passwords and pre-shared keys must have the following minimum lengths:

- For Software-Defined Access Wireless, between the controller and map server, a pre-shared key (for example, the LISP authentication key) is used in authentication of all TCP messages between them. This pre-shared key must be at least 14 characters long.
- The ISAKMP key (for example, the Crypto ISAKMP key) must be at least 14 characters long.

Guidelines and Restrictions for FIPS

- In the controller switches, a legacy key is used to support the legacy APs. However, in FIPS mode, the crypto engine detects the legacy key as a weak key and rejects it by showing the following error message:

"**% Error in generating keys: could not generate test signature.**" We recommend that you ignore such error messages that are displayed during the bootup of the controller (when operating in FIPS mode).

- SSH clients using SHA1 will not be able to access the controller when you enable FIPS.

Note You need to use FIPS compliant SSH clients to access the controller.

- TrustSec is not supported.
- PAC key configuration is not supported.

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

Configuring FIPS

Ensure that both the active and standby controllers have the same FIPS authorization key.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**fips authorization-key** *key* **Example:** `Device(config)# fips authorization-key 12345678901234567890123456789012`	Enables the FIPS mode. The key length should be of 32 hexadecimal characters. To disable FIPS mode on the device, use the **no** form of this command.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

What to do next

You must reboot the controller whenever you enable or disable the FIPS mode. After the controller is rebooted, the APs, as soon as they rejoin the controller, also reboot.

Configuring FIPS in HA Setup

While bringing up HA pair in FIPS mode, you need to configure both active and standby controllers with the same FIPS authorization key independently before forming HA pair.

If you configure FIPS authorization key after forming HA pair, the FIPS authorization key configuration will not be synced with the standby. Rebooting HA pair at this state causes reload loop. To avoid this, you need to perform the following:

- Break the HA pair.
- Configure the same FIPS authorization key independently on both the members.
- Pair up members.

To configure FIPS in HA setup, perform the following:

1. Power off both the members of the stack.
2. Power on only member1, and wait for the controller to come up and prompt for login from the console.
3. Login successfully with your valid credentials, and execute the following commands:

```
Show fips status
```

```
Show fips authorization-key
Show romvar
Show chassis
```

Note Keep the configured FIPS authorization key handy.

4. Configure the FIPS key, if you have not configured one earlier.

```
conf t
fips authorization-key <32 hex char>
```

5. Save and power off the member1.
6. Power on only member2 and wait for the controller to come up and prompt for login from the console.
7. Login successfully with your valid credentials, and execute the following commands:

```
Show fips status
Show fips authorization-key
Show romvar
Show chassis
```

Note Keep the configured FIPS authorization key handy.

8. Configure the FIPS key, if you have not configured one earlier.

Note The key value must be the same in both the members of the stack.

```
conf t
fips authorization-key <32 hex char>
```

9. Save and power off the member2.
10. Power on both the members together, and wait for the stack to form.
11. Monitor any crash or unexpected reload.

Note It is expected that members must not reload due to FIPS issue.

Monitoring FIPS

Use the following commands to view information about FIPS:

Command	Purpose
show fips authorization-key	Displays the installed authorization key.
show fips status	Displays the status of FIPS on the device.

CC

Information About Common Criteria

Common Criteria (CC) is a testing standard that verifies if the device provides security functionalities as claimed by the product developers. The CC certificate is recognised officially in 24 countries.

CC covers a set of requirements, tests, and evaluation methodology that assures that the Target of Evaluation (ToE) complies to a specific protection profile. In our case, the ToE must comply with the following protection profiles:

- Collaborative Protection Profile for Network Devices (NDcPP) v2 dated May 5, 2017
- Wireless Local Area Network (WLAN) Access Systems Extended Package version 1 May 29, 2015

For more information about CC, see

https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/common-criteria.html

Configuring Common Criteria

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wlancc** **Example:** `Device(config)# wireless wlancc`	Configures the Common Criteria mode for the controller. **Note** Reboot the controller after enabling the common criteria mode.
Step 3	**ap dtls-cipher** *ciphersuite* **Example:** `Device(config)# ap dtls-cipher DHE-RSA-AES256-SHA256`	Configures the cipher suite supported by DTLS. **Note** Reboot the controller to activate the selected cipher suite.
Step 4	**ap dtls-version** {**dtls_1_0** | **dtls_1_2**}	Configure DTLS version 1.0 or 1.2.

	Command or Action	Purpose
	Example: `Device(config)# ap dtls-version dtls_1_2`	**Note** Save the configuration and reload the controller for the changes to take effect.
Step 5	**end** **Example:** `Device(config)# end`	Exits the configuration mode and enters the privileged EXEC mode.

Verifying CC Configuration

Use the following **show** command to display the wireless certification configurations:

```
Device# show wireless certification config
Wireless Certification Configurations

WLANCC                                    : Configured
AP DTLS Cipher Suite                      : DHE-RSA-AES128-SHA
                                            DHE-RSA-AES256-SHA
                                            DHE-RSA-AES256-SHA256
                                            ECDHE-ECDSA-AES128-GCM-SHA256
                                            ECDHE-ECDSA-AES256-GCM-SHA384
AP DTLS Version                           : DTLS v1.2
```

Check Points for CC Mode Operation

You need to be aware of the following for CC mode operation:

Table 29: Check Points for CC Mode Operation

Features	Description
Link encryption	Data link encryption is not supported for C91xx wireless mobility express platform.
Link encryption	For non-C91xx wireless mobility express platfoms - Enabling Data link encryption (using ECDHE keypair) would make AP flap continually.
LDAP	Secure LDAP does not support strong ciphers and is not part of CC certification.
Mobility	Mobility between Cisco Catalyst 9800 Series Wireless controllers is possible with LSC as wireless management trustpoint (having RSA based keys).
Mobility	Mobility between AireOS WLC and Cisco Catalyst 9800 Series Wireless controllers is supported (using SUDI and MIC certificates for wireless management trustpoint).

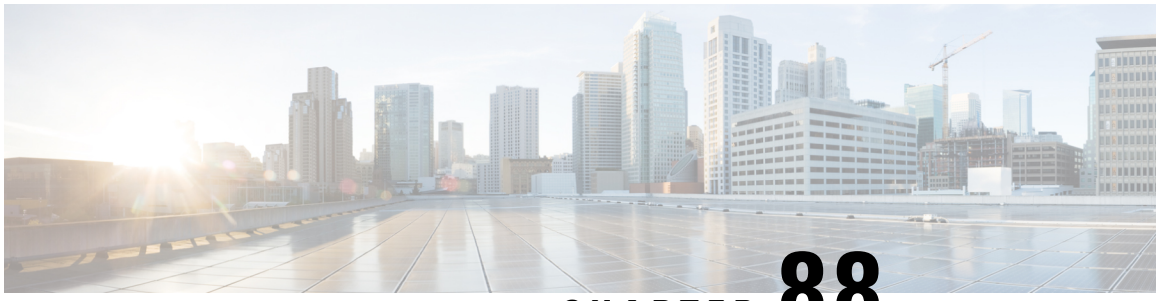
Features	Description
Mobility	Mobility between AireOS WLC and Cisco Catalyst 9800 Series Wireless controllers is not supported (if using LSC certficates for wireless management trustpoint).
CC mode	The **show wireless certification config** command displays the configured values for WLANCC, or AP-dtls-ciphersuite, or AP-dtls-version, and needs reload after re-configuring these parameters.
CC mode	The AES128-SHA option is not supported for AP-dtls-ciphersuite when Cisco Catalyst 9800 Series Wireless Controller is operating in CC mode.
CC mode	The AES128-SHA option is supported for AP-dtls-ciphersuite when Cisco Catalyst 9800 Series Wireless Controller is operating in FIPS mode.
CC mode	If you want your Cisco Catalyst 9800 Series Wireless Controller to operate in CC mode (you need to enable both FIPS mode and CC mode).
LSC	To secure communication between Cisco Catalyst 9800 Series Wireless Controller and LSC server, you need to deploy ESTCA as LSC server (which uses TLS to secure related communication).
LSC	Cisco Catalyst 9800 Series Wireless Controllers do not support HTTPS to secure its communication with the LSC server.
LSC	During LSC provisioning, APs generate EC based keys only when related Cisco Catalyst 9800 Series Wireless Controller is operating in CC mode.
LSC	During LSC provisioning, APs generate RSA based keys when related Cisco Catalyst 9800 Series Wireless Controller is operating in FIPS mode.
LSC	During LSC provisioning, APs generate RSA based keys when related Cisco Catalyst 9800 Series Wireless Controlle is operating in non-FIPS or non-CC mode.
Password Obfuscation	You can use the following commands for password obfuscation: • **key config-key password-encrypt** • **service password-encryption** • **password encryption aes** • **passwd key obfuscate**

Features	Description
CC mode	APs reload immediately, if you change the **wlancc** status.
FIPS mode	APs do not reload immediately, if you change the FIPS status.
Cisco 1562 AP	To assist Cisco 1562 APs join the Cisco Catalyst 9800 Series wireless controller, you need to have the ethernet MAC of the AP in the username list.
AP serial number authorization	Serial number authorization is possible only when Cisco Catalyst 9800 Series wireless controller is in FIPS and CC mode, and with LSC based trustpoints/certficates only (not with SUDI trustpoint).
Display	FIPS suitability displays **Suitable only** if the controller is in CC mode and LSC certificate is compatible. Both wireless management and Certs CN should match the hostname of the controller and length of RSA Key (> 2048) (or) EC keys being used.
RADSEC	RSA key size must contain a minimum of 2048 bits (of certificate under RADSEC) when operating in FIPS or CC mode, else RADSEC fails.

PART VII

Mobility

- Mobility, on page 791
- Static IP Client Mobility, on page 811



CHAPTER 88

Mobility

- Introduction to Mobility, on page 791
- Guidelines and Restrictions, on page 796
- Configuring Mobility (GUI), on page 798
- Configuring Mobility (CLI), on page 799
- Configuring Inter-Release Controller Mobility (GUI), on page 801
- Configuring Inter-Release Controller Mobility, on page 801
- Verifying Mobility, on page 805

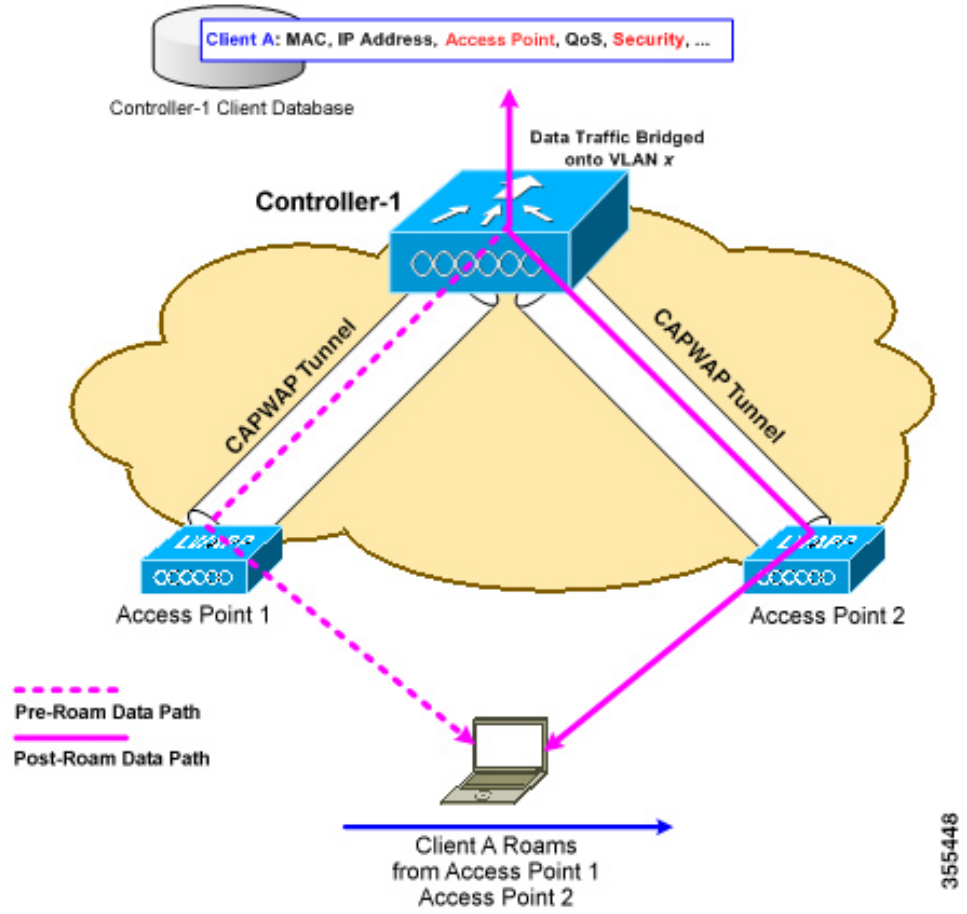
Introduction to Mobility

Mobility or roaming is a wireless LAN client's ability to maintain its association seamlessly from one access point to another access point 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 a wireless client.

Figure 16: Intracontroller Roaming

This figure shows a wireless client that roams from one access point to another access point when both access points are joined to the same controller.

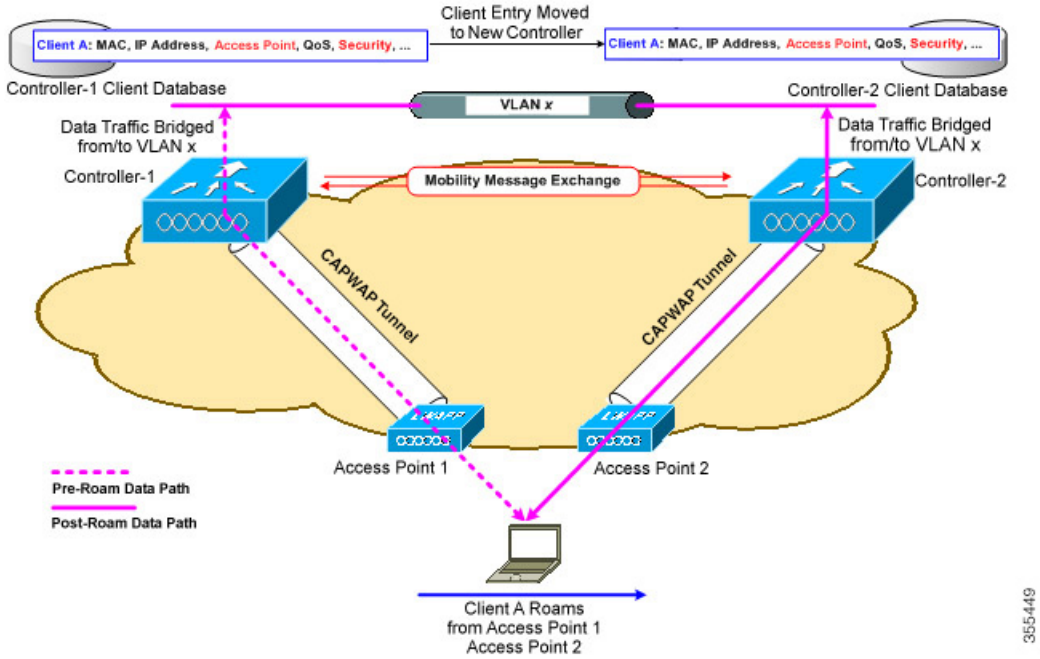


When a wireless client moves its association from one access point to another access point, the controller simply updates the client database with the newly associated access point. If necessary, new security context and associations are established as well.

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.

Figure 17: Intercontroller Roaming

This figure shows intercontroller roaming, which occurs when the wireless LAN interfaces of controllers are on the same IP subnet.



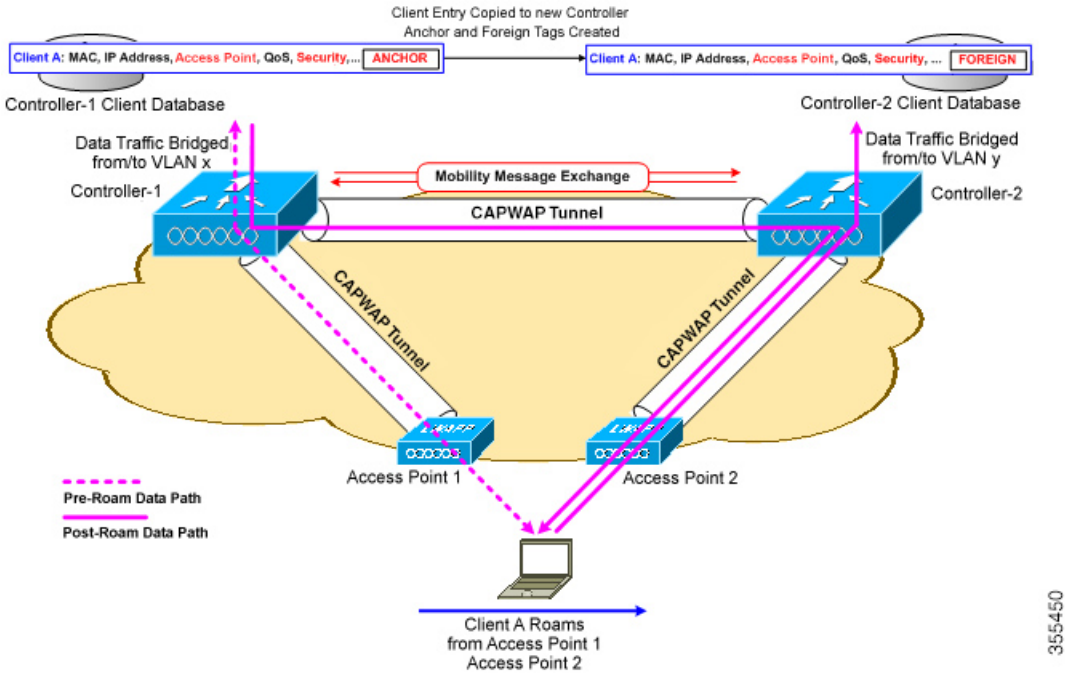
When a client joins an access point associated with a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database entry is updated for the new access point. This process remains transparent to the user.

Note All clients configured with 802.1X/Wi-Fi Protected Access (WPA) security complete a full authentication in order to comply with the IEEE standard.

Important Intersubnet Roaming is not supported for SDA.

Figure 18: Intersubnet Roaming

This figure shows intersubnet roaming, which occurs when the wireless LAN interfaces of controllers are on different IP subnets.



Intersubnet roaming is similar to intercontroller roaming in that, 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.

In intersubnet roaming, WLANs on both anchor and foreign controllers should have the same network access privileges, and no source-based routing or source-based firewalls in place. Otherwise, the clients may have network connectivity issues after the handoff.

In a static anchor setup using controllers and a RADIUS server, if AAA override is enabled to dynamically assign VLAN and QoS, the foreign controller updates the anchor controller with the right VLAN after a Layer 2 authentication (802.1x). For Layer 3 RADIUS authentication, the RADIUS requests for authentication are sent by the anchor controller.

Note The Cisco Catalyst 9800 Series Wireless Controller mobility tunnel is a CAPWAP tunnel with control path (UDP 16666) and data path (UDP 16667). The control path is DTLS encypted by default. Data path DTLS can be enabled when you add the mobility peer.

SDA Roaming

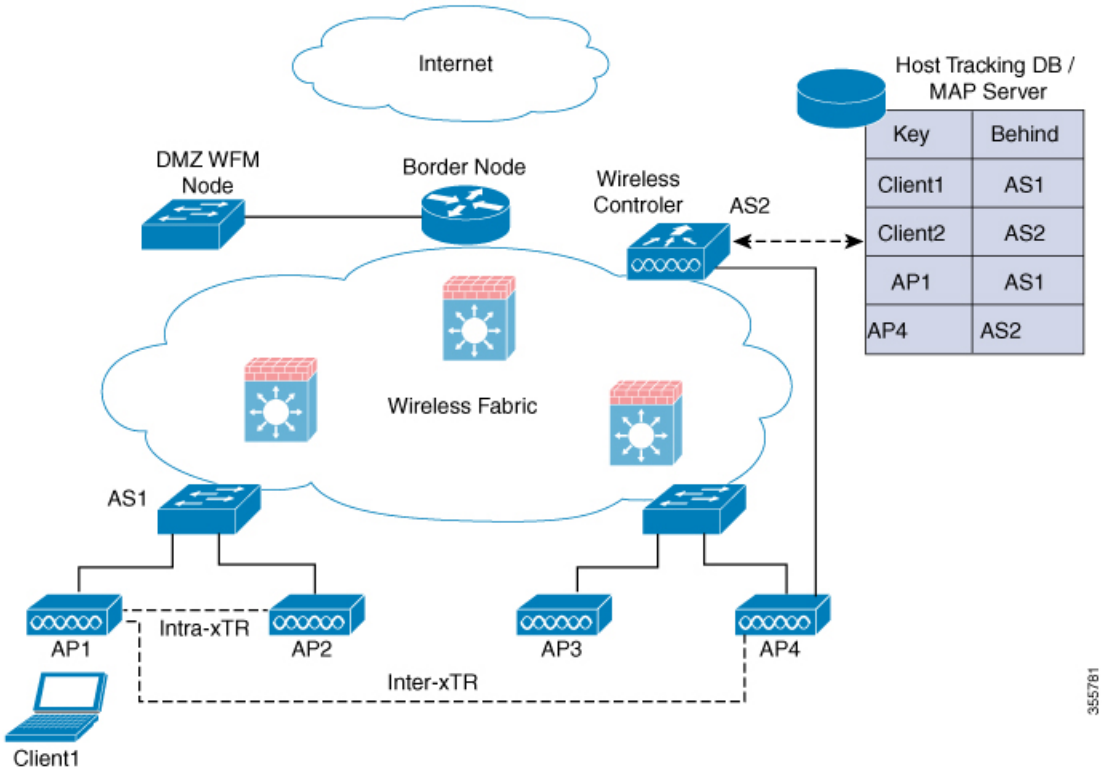
SDA supports two additional types of roaming, which are Intra-xTR and Inter-xTR. In SDA, xTR stands for an access-switch that is a fabric edge node. It serves both as an ingress tunnel router as well as an egress tunnel router.

When a client on a fabric enabled WLAN, roams from an access point to another access point on the same access-switch, it is called Intra-xTR. Here, the local client database and client history table are updated with the information of the newly associated access point.

When a client on a fabric enabled WLAN, roams from an access point to another access point on a different access-switch, it is called Inter-xTR. Here, the map server is also updated with the client location (RLOC) information. Also, the local client database is updated with the information of the newly associated access point.

Figure 19: SDA Roaming

This figure shows inter-xTR and intra-xTR roaming, which occurs when the client moves from one access point to another access point on the same switch or to a different switch in a Fabric topology.



Definitions of Mobility-related Terms

- Point of Attachment—A station's point of attachment is where its data path is initially processed upon entry into the network.
- Point of Presence—A station's point of presence is the place in the network where the station is being advertised.
- Station—A user's device that connects to and requests service from a network.

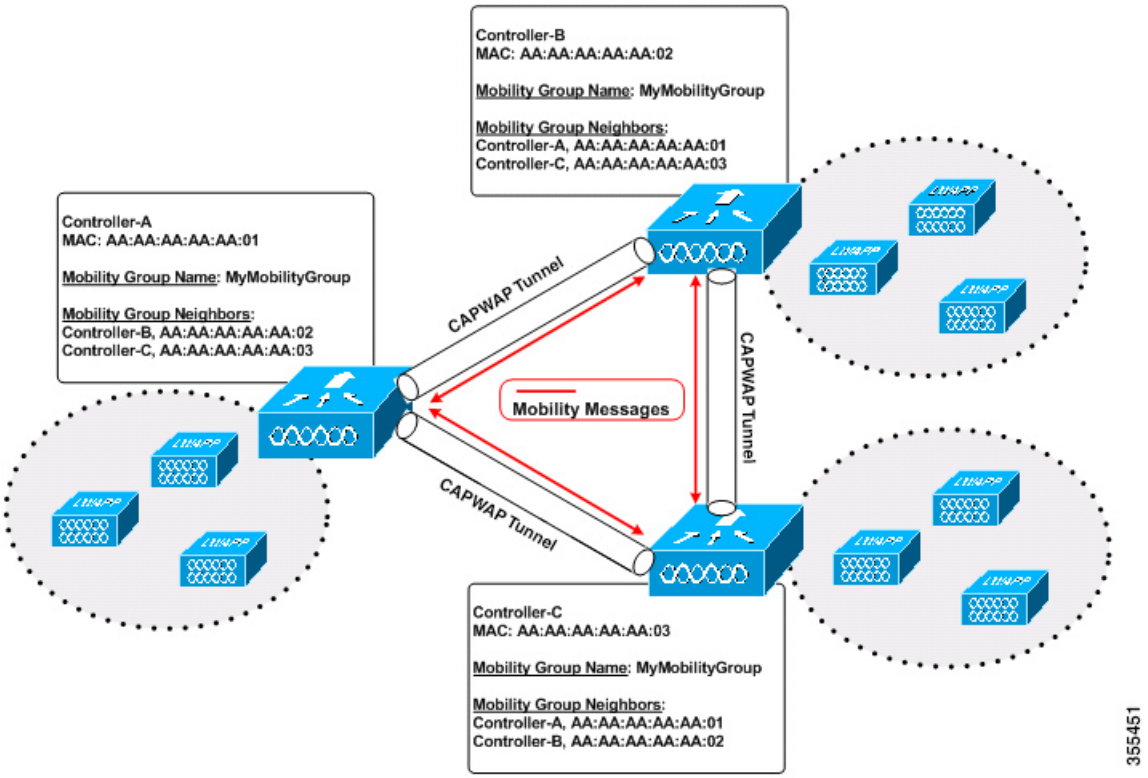
Mobility Groups

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 intercontroller or intersubnet 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 intercontroller wireless LAN roaming and controller redundancy.

Note While moving an AP from one controller to another (when both controllers are mobility peers), a client associated to controller-1 before the move might stay there even after the move. This is due to a timeout period on controller-1, where the client entry is maintained (for the purposes of roaming/re-association scenarios). To avoid the client being anchored in controller-1, remove the mobility peer configuration of the controller.

Figure 20: Example of a Single Mobility Group



As shown in the figure above, each controller is configured with a list of the other members of the mobility group. Whenever a new client joins a controller, the controller sends out a unicast message (or multicast message if mobility multicast is configured) to all of the controllers in the mobility group. The controller to which the client was previously connected passes on the status of the client.

Guidelines and Restrictions

The following AireOS and Cisco Catalyst 9800 Series Wireless Controller platforms are supported for SDA Inter-Controller Mobility (AireOS controller–to-Cisco Catalyst 9800 Series Wireless Controller):

- **AireOS**

- Cisco 3504
- Cisco 5520
- Cisco 8540

- **Cisco Catalyst 9800 Series Wireless Controller**
  - Cisco Catalyst 9800 Wireless Controller for Cloud
  - Cisco Catalyst 9800-80 Wireless Controller
  - Cisco Catalyst 9800-40 Wireless Controller
  - Cisco Catalyst 9800-L Wireless Controller

The following controller platforms are supported for SDA Inter-Controller Mobility:

- **Catalyst Switches**
  - Cisco 9300

- **Cisco Catalyst 9800 Series Wireless Controller**
  - Cisco Catalyst 9800 Wireless Controller for Cloud
  - Cisco Catalyst 9800-40 Wireless Controller

- Ensure that the data DTLS configuration on the Cisco Catalyst 9800 Series Wireless Controller and AireOS are the same, as configuration mismatch is not supported on the Cisco Catalyst 9800 Series Wireless Controller and it causes the mobility data path to go down.
- In intercontroller roaming scenarios, policy profiles having different VLANs is supported as a Layer 3 roaming.
- In AireOS controller, L3 override is not supported in guest VLAN. Hence, the client does not trigger DHCP Discovery on the new VLAN automatically.
- Policy profile name and client VLAN under policy profile can be different across the controllers with the same WLAN profile mapped.
- In intracontroller roaming scenarios, client roaming is supported between same policy profiles, with WLAN mapped.
- If a client roams in web authentication state, the client is considered as a new client on another controller instead of being identified as a mobile client.
- Controllers that are mobility peers must use the same DHCP server to have an updated client mobility move count on intra-VLAN.
- Data DTLS and SSC hash key must be same for mobility tunnels between members.
- Mobility move count is updated under client detail only during inter-controller roaming. Intra-controller roaming can be verified under client stats and mobility history.
- Anchor VLAN in Cisco Catalyst 9800 Series Wireless Controller is represented as Access VLAN on the Cisco AireOS controller.

- When clients are roaming, their mobility role is shown as *Unknown*. This is because the roaming clients are in *IP learn* state, and in such a scenario, there are many client additions to the new instance and deletions in the old instance.
- In inter-controller roaming between 9800 and 9800/AireOS, client roaming is not supported, whenever there is a WLAN profile mismatch.
- Only IPv4 tunnel is supported between Cisco Catalyst 9800 Series Wireless Controller and Cisco AireOS controller.
- Ensure that you configure the mobility MAC address using the **wireless mobility mac-address** command for High-Availability to work.
- If Anchor and Foreign controllers are put in the same Layer 2 network, it creates a loop topology (one path is Layer 3 mobility tunnel between Anchor and Foreign, another path is Layer 2 wired connection between Anchor and Foreign). In this topology, MAC_CONFLICT warning message can be seen on both the Anchor and Foreign controllers. This MAC_CONFLICT warning message is printed once every minute. However,it doesn't have any functionality and performance impact. As a best practice, do not use management VLAN as client VLAN.
-
- If the current AP has 5-GHz slot2 radio on L2 and L3 mobility 5-GHz slot2, the WLAN BSSID is only added to the 11k or 11v neighbor information. As a result, the AP does not have the information of radio properties of the APs belonging to the other controllers. Hence, it can be assumed that the radio properties of the APs belonging to the other controllers are similar to that of the current AP. If the current AP does not have slot2, the other APs cannot be added as a neighbor. In such a scenario, the validation fails and does not add this radio to the neighbor list.
- We recommend that you use the default keepalive count and interval values to reduce convergence time between the Cisco AireOS Wireless Controllers and Cisco Catalyst 9800 Series Wireless Controllers while setting up a mobility tunnel.
- A new client may take up to 3 seconds to join the network when the mobility tunnel is UP and mobility peers are configured. This is because the system sends three mobile messages (one second apart) to find out whether the client is already part of the network.

Configuring Mobility (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mobility**.
The **Wireless Mobility** page is displayed on which you can perform global configuration and peer configuration.

Step 2 In the **Global Configuration** section, perform the following tasks:

a) Enter a name for the mobility group.
b) Enter the multicast IP address for the mobility group.
c) In the **Keep Alive Interval** field, specify 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.

d) Specify the **Mobility Keep Alive Count** amount of time (in seconds) between each ping request sent to a mobility list member. The valid range is 1 to 30 seconds.
e) Enter the DSCP value for the mobility group.
f) Enter the mobility MAC address.
g) Click **Apply**.

Step 3 In the **Peer Configuration** tab, perform the following tasks:

a) In the **Mobility Peer Configuration** section, click **Add**.
b) In the **Add Mobility Peer** window that is displayed, enter the MAC address and IP address for the mobility peer. .
c) Enter the mobility group to which you want to add the mobility peer.
d) Select the required status for **Data Link Encryption**.
e) Specify the **SSC Hash** as required.

SSC hash is required if the peer is a Cisco Catalyst 9800-CL Wireless Controller, which uses self-signed certificate and hence SSC hash is used as an additional validation. SSC hash is not required if peer is an appliance, which will have manufacturing installed certificates (MIC) or device certificates burned in the hardware.

f) Click **Save & Apply to Device**.
g) In the **Non-Local Mobility Group Multicast Configuration** section, click **Add**.
h) Enter the mobility group name.
i) Enter the multicast IP address for the mobility group.
j) Click **Save**.

Configuring Mobility (CLI)

Procedure

	Command or Action	Purpose
Step 1	**wireless mobility group name** *group-name* **Example:** `Device(config)# wireless mobility group name Mygroup`	Creates a mobility group named **Mygroup**.
Step 2	**wireless mobility mac-address** *mac-addr* **Example:** `Device(config)# wireless mobility mac-address 00:0d:ed:dd:25:82`	Configures the MAC address to be used in mobility messages.
Step 3	**wireless mobility dscp** *value-0-to-63* **Example:** `Device(config)# wireless mobility dscp 10`	(Optional) Configures mobility intercontroller DSCP value.

	Command or Action	Purpose
Step 4	**wireless mobility group keepalive interval** *time-in-seconds* **Example:** `Device(config)# wireless mobility group keepalive interval 5`	(Optional) Configures the interval between two keepalives sent to a mobility member. Valid range is between 1 and 30 seconds. **Note** For controllers connected through mobility tunnels, ensure that both controllers have the same keepalive interval value.
Step 5	**wireless mobility group keepalive count** *count* **Example:** `Device(config)# wireless mobility group keepalive count 3`	(Optional) Configures the keepalive retries before a member status is termed DOWN.

Step 6	Use the options given below to configure IPv4 or IPv6.
	• **wireless mobility mac-address** *mac-address* **ip** *peer-ip-address* **group** *group-name* **data-link-encryption**
	• **wireless mobility mac-address** *mac-address* **ip** *peer-ip-address* **group** *group-name*
	Example:
	`Device(config#) wireless mobility mac-address 001E.BD0C.5AFF ip 9.12.32.10 group test-group data-link-encryption`
	`Device(config#) wireless mobility mac-address 001E.BD0C.5AFF ip fd09:9:2:49::55 group scalemobility`
		Adds a peer IPv4 or IPv6 address to a specific group.
		To remove the peer from the local group, use the **no** form of this command.

Step 7	**wireless mobility multicast** {**ipv4** | **ipv6** }*ip-address* or **wireless mobility group multicast-address** *group-name* {**ipv4** | **ipv6** } *ip-address*
	Example:
	`Device(config)# wireless mobility multicast ipv4 224.0.0.4`
	Example:
	`Device(config)# wireless mobility group multicast-address Mygroup ipv4 224.0.0.5`
		(Optional) Configures a multicast IPv4 or IPv6 address for a local mobility group or a nonlocal mobility group.
		Note **Mobility Multicast**—The controller sends a multicast message instead of a unicast message to all the members in the mobility local group or a nonlocal group when a client joins or roams.
		Configures the multicast IPv4 address as 224.0.0.4 for a local mobility group.
		Configures the multicast IPv4 address as 224.0.0.5 for a nonlocal mobility group.

Configuring Inter-Release Controller Mobility (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mobility** > **Global Configuration**.

Step 2 Enter the **Mobility Group Name**, **Multicast IPv4 Address**, **Multicast IPv6 Address**, **Keep Alive Interval (sec)**, **Mobility Keep Alive Count**, **Mobility DSCP Value** and **Mobility MAC Address**.

Step 3 Click **Apply**.

Configuring Inter-Release Controller Mobility

Inter-Release Controller Mobility (IRCM) is a set of features and functionality that enable interworking between controllers running different software releases. IRCM enables seamless mobility and wireless services across controllers running Cisco AireOS and Cisco IOS (for example, Cisco 8540 WLC to Cisco Catalyst 9800 Series Wireless Controller) for features such as Layer 2 and Layer 3 roaming and guest access or termination.

Note To configure IRCM for different combination of AireOS and Catalyst 9800 controllers, see the Cisco Catalyst 9800 Wireless Controller-Aireos IRCM Deployment Guide.

Follow the procedure described to configure mobility peers on the controller:

Before you begin

The Inter-Release Controller Mobility (IRCM) feature is supported by the following Cisco Wireless Controllers.

- For IRCM deployment, we recommended that you configure:
  - Both Cisco AireOS and Cisco Catalyst 9800 Series Controllers as static RF leaders to avoid RF grouping between them.
  - Configure the same RF network name on both the controllers.
- Cisco Catalyst 9800 Series Wireless Controller platforms running Cisco IOS XE Software version 16.10.1 or later.
- Supports the following Cisco AireOS Wireless Controllers running Cisco AireOS 8.5.14x.x IRCM image based on the 8.5 Maintenance Release software:
  - Cisco 3504 Wireless Controllers
  - Cisco 5508 Wireless Controllers
  - Cisco 5520 Wireless Controllers
  - Cisco 8510 Wireless Controllers

- Cisco 8540 Wireless Controllers

- By design, Cisco Catalyst 9800 Wireless Controllers does not have the Primary Mode configuration exposed that is to be sent in the Discovery Response. The controller always sends the Discovery Response with the Primary Mode enabled.
- Supported Cisco AireOS Wireless Controllers running AireOS 8.8.111.0 and later. The following controllers are supported:
  - Cisco 3504 Wireless Controllers
  - Cisco 5520 Wireless Controllers
  - Cisco 8540 Wireless Controllers

Note If the peer Cisco Catalyst 9800 Series Wireless Controller is virtual, configure the hash using command:

```
config mobility group member hash 172.20.227.73
3f93a86cee2039e9c3aada1822ad74b89fea30c1
```

```
config mobility group member hash 172.20.227.73
3f93a86cee2039e9c3aada1822ad74b89fea30c1
```

Optionally enable data tunnel encryption using command:

```
config mobility group member data-dtls 00:0c:29:a8:d5:77
enable/disable
```

The hash configure above can be obtained by running the following command on the Cisco Catalyst 9800 Series Wireless Controller:

```
show wireless management trustpoint
Trustpoint Name : ewlc-tp1
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : 3f93a86cee2039e9c3aada1822ad74b89fea30c1
Private key Info : Available
```

- The IRCM feature is not supported on the following Cisco AireOS Wireless Controllers:
  - Cisco 2504 Wireless Controllers
  - Cisco Flex 7510 Wireless Controllers
  - Cisco WiSM 2

- IPv6 is not supported for SDA IRCM for fabric client roaming. IPv6 is supported for IRCM for non-fabric client roaming.
- Ensure that you use AireOS controller that supports Encrypted Mobility feature.

- AVC is not supported for IRCM.
- In mixed deployments (Catalyst 9800 and AireOS Controllers), the WLAN profile name and the policy profile name must be the same. This is due to AireOS not knowing about the policy profile and therefore only sends or receives the WLAN name as both the policy profile and WLAN profile.
- Mobility group multicast is not supported because AireOS does not support mobility multicast in encrypted mobility.
- There could be instances where the total number of clients count shown may be more than those supported on the roaming scale. This inconsistency is observed when the client roaming rate is very high, as the system requires time to update the records. Here, the clients presented on multiple wncds for a very short time are counted more than once. We recommend that you provide sufficient time for the process to obtain a consistent data before using one of the following methods: show CLIs, WebUI, Cisco Catalyst Center, or SNMP.
- Link Local bridging is not supported. Ensure that you disable it also on the peer AireOS controller.
- IRCM is not supported in FlexConnect and FlexConnect+Bridge modes.

The following client features support IPv6 client mobility between AireOS controllers and Cisco Catalyst 9800 Series Wireless Controller: Accounting, L3 Security (Webauth), Policy (ACL and QoS), IP address assignment and learning through SLAAC and DHCPv6, IPv6 Source Guard, multiple IPv6 address learning, IPv6 multicast, and SISF IPv6 features (RA Guard, RA Throttling, DHCPv6 Guard, and ND Suppress).ß

The following IPv6 features are not supported on Cisco Catalyst 9800 Series Wireless Controller:

- Configurable IPv6 timers
- RA Guard enabled on AP
- Global IPv6 disable

Note

- IPv6 CWA is not supported for both AireOS controllers and Cisco Catalyst 9800 Series Wireless Controller.
- Only eight IPv6 addresses are supported per client.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	Use the options given below to configure IPv4 or IPv6. • **wireless mobility group member mac-address** *mac-address* **ip** *peer-ip* **group** *group-name***data-link-encryption**	Adds a peer IPv4 or IPv6 address to a specific group. To remove the peer from the local group, use the **no** form of this command.

	Command or Action	Purpose

	• **wireless mobility group member mac-address** *mac-address* **ip** *peer-ip-address* **group** *group-name*
	Example:
	`Device(config#) wireless mobility group member mac-address 001E.BD0C.5AFF ip 9.12.32.10 group test-group data-link-encryption`
	`Device(config#) wireless mobility group member mac-address 001E.BD0C.5AFF ip fd09:9:2:49::55 group scalemobility`	

Step 3	**wireless mobility group name** *group-name* **Example:** `Device(config#) wireless mobility group name test-group`	Adds a name for the local group. The default local group name is "default".
Step 4	**wireless mobility mac-address** *mac-address* **Example:** `Device(config#) wireless mobility mac-address 000d.bd5e.9f00`	(Optional) Configures the MAC address to be used in mobility messages.
Step 5	**wireless mobility group member ip** *peer-ip* **Example:** `Device(config#) wireless mobility group member ip 9.12.32.15`	Adds a peer in the local group. To remove the peer from the local group, use the **no** form of this command.
Step 6	**wireless mobility dscp** *dscp-value* **Example:** `Device(config#) wireless mobility dscp 52`	(Optional) Configures DSCP. The default value is 48.
Step 7	**wireless mobility group keepalive count** *count* **Example:** `Device(config#) wireless mobility group keepalive count 10`	Configures the mobility control and data path keepalive count. The default value is 3.
Step 8	**wireless mobility group keepalive interval** *interval* **Example:** `Device(config#) wireless mobility group keepalive interval 30`	Configures the mobility control and data path keepalive interval. The default value is 10. **Note** For controllers connected through mobility tunnels, ensure that both controllers have the same keepalive interval value.

Verifying Mobility

To display the summary of the mobility manager, use the following command:

```
Device# show wireless mobility summary
```

To display mobility peer information, use the following command:

```
Device# show wireless mobility peer ip 10.0.0.8
```

To display the list of access points known to the mobility group, use the following command:

```
Device# show wireless mobility ap-list
```

To display statistics for the mobility manager, use the following command:

```
Device# show wireless statistics mobility
Mobility event statistics:
     Joined as
         Local                          : 0
         Foreign                        : 0
         Export foreign                 : 2793
         Export anchor                  : 0
     Delete
         Local                          : 2802
         Remote                         : 0
     Role changes
         Local to anchor                : 0
         Anchor to local                : 0
     Roam stats
         L2 roam count                  : 0
         L3 roam count                  : 0
         Flex client roam count         : 0
         Inter-WNCd roam count          : 0
         Intra-WNCd roam count          : 0
         Remote inter-cntrl roam count  : 0
         Remote WebAuth pending roams   : 0
     Anchor Request
         Sent                           : 0
           Grant received               : 0
           Deny received                : 0
         Received                       : 0
           Grant sent                   : 0
           Deny  sent                   : 0
     Handoff Status Received
         Success                        : 0
         Group mismatch                 : 0
         Client unknown                 : 0
         Client blacklisted             : 14
         SSID mismatch                  : 0
         Denied                         : 0
     Handoff Status Sent
         Success                        : 0
         Group mismatch                 : 0
         Client unknown                 : 0
         Client blacklisted             : 0
         SSID mismatch                  : 0
         Denied                         : 0
     Export Anchor
         Request Sent                   : 2812
```

```
          Response Received             :
              Ok                        : 2793
              Deny - generic            : 19
              Client blacklisted        : 0
              Client limit reached      : 0
              Profile mismatch          : 0
              Deny - unknown reason     : 0
          Request Received              : 0
          Response Sent                 :
              Ok                        : 0
              Deny - generic            : 0
              Client blacklisted        : 0
              Client limit reached      : 0
              Profile mismatch          : 0
MM mobility event statistics:
     Event data allocs                  : 17083
     Event data frees                   : 17083
     FSM set allocs                     : 2826
     FSM set frees                      : 2816
     Timer allocs                       : 8421
     Timer frees                        : 8421
     Timer starts                       : 14045
     Timer stops                        : 14045
     Invalid events                     : 0
     Internal errors                    : 0
     Delete internal errors             : 0
     Roam internal errors               : 0


MMIF mobility event statistics:
     Event data allocs                  : 17088
     Event data frees                   : 17088
     Invalid events                     : 0
     Event schedule errors              : 0
     MMIF internal errors:
       IPC failure                      : 0
       Database failure                 : 0
       Invalid parameters               : 0
       Mobility message decode failure  : 0
       FSM failure                      : 0
       Client handoff success           : 0
       Client handoff failure           : 14
       Anchor Deny                      : 0
       Remote delete                    : 0
       Tunnel down delete               : 0
       MBSSID down                      : 0
       Unknown failure                  : 0
```

To display counters for all messages in mobility, use the following command:

```
Device# show wireless stats mobility messages
MM datagram message statistics:
  Message Type               Built  Tx    Rx    Processed  Tx Error  Rx Error  Forwarded
Retry  Drops  Allocs  Frees

------------------------------------------------------------------------------------------------------------------

  Mobile Announce            0      0     0     0          0         0         25350
5624   0      2826    2826
  Mobile Announce Nak        0      0     0     0          0         0         0
0      0      0       0
  Static IP Mobile Annc      0      0     0     0          0         0         0
0      0      0       0
  Static IP Mobile Annc Rsp  0      0     0     0          0         0         0
0      0      0       0
```

```
  Handoff                     0      0     14    14          0          0          0
0       0       42      42
  Handoff End                 0      0     0     0           0          0          2783
0       0       2783    2783
  Handoff End Ack             0      0     2783  2783        0          0          0
0       0       8349    8349
  Anchor Req                  0      0     0     0           0          0          0
0       0       0       0
  Anchor Grant                0      0     0     0           0          0          0
0       0       0       0
  Anchor Xfer                 0      0     0     0           0          0          0
0       0       0       0
  Anchor Xfer Ack             0      0     0     0           0          0          0
0       0       0       0
  Export Anchor Req           0      0     0     0           0          0          2812
0       0       2812    2812
  Export Anchor Rsp           0      0     2812  2812        0          0          0
0       0       8436    8436
  AAA Handoff                 0      0     0     0           0          0          0
0       0       0       0
  AAA Handoff Ack             0      0     0     0           0          0          0
0       0       0       0
  IPv4 Addr Update            0      0     2792  0           0          0          0
0       0       2792    2792
  IPv4 Addr Update Ack        2792   2792  0     0           0          0          0
0       0       2792    2792
  IPv6 ND Packet              0      0     0     0           0          0          0
0       0       0       0
  IPv6 Addr Update            0      0     5587  0           0          0          0
0       0       5587    5587
  IPv6 Addr Update Ack        5587   5587  0     0           0          0          0
0       0       5587    5587
  Client Add                  0      0     0     0           0          0          0
0       0       0       0
  Client Delete               0      0     0     0           0          0          0
0       0       0       0
  AP List Update            25585  25585  8512  8512        2          1          0
0       0       34098   34098
  Client Device Profile Info 0       0     0     0           0          0          0
0       0       0       0
  PMK Update                  0      0     0     0           0          0          0
0       0       0       0
  PMK Delete                  0      0     0     0           0          0          0
0       0       0       0
  PMK 11r Nonce Update        0      0     0     0           0          0          0
0       0       0       0
  Device cache Update         0      0     0     0           0          0          0
0       0       0       0
  HA SSO Announce             0      0     0     0           0          0          0
0       0       0       0
  HA SSO Announce Resp        0      0     0     0           0          0          0
0       0       0       0
  Mesh Roam Request           0      0     0     0           0          0          0
0       0       0       0
  Mesh Roam Response          0      0     0     0           0          0          0
0       0       0       0
  Mesh AP PMK Time Upd        0      0     0     0           0          0          0
0       0       0       0
  Mesh AP PMK Time Upd Ack    0      0     0     0           0          0          0
0       0       0       0
  Mesh AP Channel List        0      3     1     0           0          1          0
0       0       2       2
  Mesh AP Channel List Resp   0      0     0     0           0          0          0
0       0       0       0
```

```
  AP upgrade                  0      0     0     0          0         0         0
0      0      0       0
  Keepalive Ctrl Req       34080  34080  17031  17031      0         0         0
0      0      51111   51111
  Keepalive Ctrl Resp      17031  17031  34067  34067      0         0         0
0      0      51098   51098
  Keepalive Data Req/Resp  238527  238527  221451  221451  0         0         0
0      0      459978  459978
```

To display mobility information of the client, use the following command:

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 detail
```

To display roaming history of the active client in the subdomain, use the following command:

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 mobility history
```

To display client-specific statistics for the mobility manager, use the following command:

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 stats mobility
```

To verify whether intercontroller roam is successful, use the following commands:

- **show wireless client mac** *mac-address* **detail**: (on the roamed-to Controller) Displays the roam type as L2 and the roam count is incremented by 1.
- **show wireless client summary** : (on the roamed-from controller) The client entry will not be there in the ouput.

Verifying SDA Mobility

To verify whether intracontroller, intra-xTR roam is successful, use the following commands:

- **show wireless client summary**: Displays the new AP if the client has roamed across the APs on the same xTR.
- **show wireless client mac** *mac-address* **detail**: Displays the same RLOC as before the roam.

To verify whether intracontroller, inter-xTR roam is successful, use the following commands:

- **show wireless fabric client summary**: Displays the new AP if the client has roamed across the APs on a different xTR.
- **show wireless client mac** *mac-address* **detail**: Displays the RLOC of the new xTR to which the client has roamed to.

To check client status before and after intracontroller roaming, perform the following steps:

1. Check if client is on the old AP, using **show wireless client summary** command on the controller.
2. Check whether the client MAC is listed against the old AP, using **show mac addr dyn** command on the xTR1.
3. Check whether the client IP is registered from current xTR1, and client MAC is registered from both current xTR1, and WLC1, using **show lisp site detail** command on the MAP server.
4. After the intra-WLC roam, check whether the client is on the new AP, using the **show wireless client summary** and **show mac addr dyn** commands on the WLC1 and xTR1.

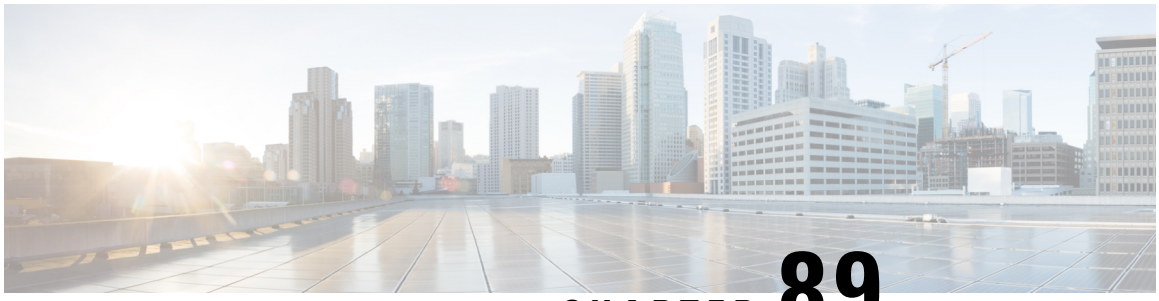
5. After the Inter-xTR Roam (old and new APs on different xTRs), check whether the client is on the new AP (connected to the new xTR2), using the **show wireless client summary** and **show mac addr dyn** commands on the WLC1 and xTR2.
6. Check whether the client is registered from the new xTR2, using the **show lisp site detail** command on the MAP server.

Verifying Roaming on MAP Server for SDA

To verify roaming information for SDA, use the following commands:

Run the following command on the MAP server, before and after the roam, to check whether the client IP is registered from current xTR, and client MAC is registered from both current xTR, and WLC.

```
Device# show lisp site detail
```



CHAPTER 89

Static IP Client Mobility

- Information About Static IP Client Mobility, on page 811
- Restrictions, on page 811
- Configuring Static IP Client Mobility (GUI), on page 812
- Configuring Static IP Client Mobility (CLI), on page 812
- Verifying Static IP Client Mobility, on page 813

Information About Static IP Client Mobility

At times, you may want to configure static IP addresses for wireless clients. When these wireless clients move about in a network, they might 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. However, now, you can enable static IP mobility for clients with static IP addresses.

Static IP clients with static IP addresses can be associated with other controllers in which 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.

Restrictions

- This feature is not supported on the Fabric and Cisco Catalyst 9800 Wireless Controller for Switch platforms.
- IPv6 is not supported.
- FlexConnect mode is not supported.
- WebAuth (LWA and CWA) is not supported.
- Supported only Open, Dot1x, and PSK authentication mechanisms.
- Supports only on the WLANs that are exclusive of the mobility anchor configuration. If the mobility anchor is already configured on a WLAN, and if static IP mobility is enabled, the feature is not supported.
- Supported only when all the peers are configured for the static IP mobility that is enabled.
- IRCM is not supported.

Configuring Static IP Client Mobility (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy** page, click the policy profile name or click **Add** to create a new one.

Step 3 Click the **Mobility** tab.

Step 4 Set the **Static IP Mobility** field to **Enabled** state.

Step 5 Click **Update & Apply to Device**.

Configuring Static IP Client Mobility (CLI)

Follow the procedure given below to configure static IP client mobility:

Before you begin

- Configure the SVI interface (L3 VLAN interface) to service the static IP client on at least one of the peer controllers in the network.
- For clients to join a controller, the VLAN (based on the VLAN number in the policy profile configuration) should be configured on the device.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy-name* **Example:** `Device(config)# wireless profile policy static-ip-policy`	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 3	**static-ip-mobility** **Example:** `Device(config-wireless-policy)# static-ip-mobility`	Enables static IP mobility.

Verifying Static IP Client Mobility

Use the following commands to verify the static IP client mobility configuration:

```
Device# show wireless profile policy detailed static-ip-policy


Policy Profile Name           : static-ip-policy
Description                   :
Status                        : DISABLED
VLAN                          : 1
Wireless management interface VLAN        : 34
Passive Client                : DISABLED
ET-Analytics                  : DISABLED
StaticIP Mobility             : DISABLED
WLAN Switching Policy
  Central Switching           : ENABLED
  Central Authentication      : ENABLED
  Central DHCP                : DISABLED
  Flex NAT PAT            : DISABLED
  Central Assoc               : DISABLED
WLAN Flex Policy
  VLAN based Central Switching          : DISABLED
WLAN ACL
  IPv4 ACL                    : Not Configured
  IPv6 ACL                    : Not Configured
  Layer2 ACL                  : Not Configured
  Preauth urlfilter list      : Not Configured
  Postauth urlfilter list     : Not Configured
WLAN Timeout
  Session Timeout             : 1800
  Idle Timeout                : 300
  Idle Threshold              : 0
WLAN Local Profiling
  Subscriber Policy Name      : Not Configured
  RADIUS Profiling            : DISABLED
  HTTP TLV caching            : DISABLED
  DHCP TLV caching            : DISABLED
WLAN Mobility
  Anchor                      : DISABLED
AVC VISIBILITY                : Disabled
Flow Monitor IPv4
  Flow Monitor Ingress Name   : Not Configured
  Flow Monitor Egress Name    : Not Configured
Flow Monitor IPv6
  Flow Monitor Ingress Name   : Not Configured
  Flow Monitor Egress Name    : Not Configured
NBAR Protocol Discovery       : Disabled
Reanchoring                   : Disabled
Classmap name for Reanchoring
  Reanchoring Classmap Name   : Not Configured
QOS per SSID
  Ingress Service Name        : Not Configured
  Egress Service Name         : Not Configured
QOS per Client
  Ingress Service Name        : Not Configured
  Egress Service Name         : Not Configured
Umbrella information
  Ciso Umbrella Parameter Map : Not Configured
Autoqos Mode                  : None
Call Snooping                 : Disabled
Fabric Profile
```

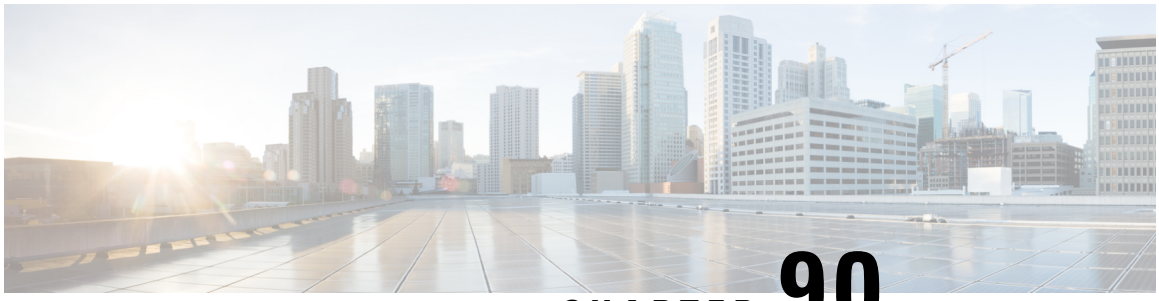
```
  Profile Name                : Not Configured
Accounting list
  Accounting List               : Not Configured
DHCP
  required                    : DISABLED
  server address              : 0.0.0.0
 Opt82
  DhcpOpt82Enable             : DISABLED
  DhcpOpt82Ascii              : DISABLED
  DhcpOpt82Rid                : DISABLED
  APMAC                       : DISABLED
  SSID                        : DISABLED
  AP_ETHMAC                   : DISABLED
  APNAME                      : DISABLED
  POLICY TAG                  : DISABLED
  AP_LOCATION                 : DISABLED
  VLAN_ID                     : DISABLED
Exclusionlist Params
  Exclusionlist               : ENABLED
  Exclusion Timeout           : 60
AAA Policy Params
  AAA Override                : DISABLED
  NAC                         : DISABLED
  AAA Policy name             : default-aaa-policy
WGB Policy Params
  Broadcast Tagging           : DISABLED
  Client VLAN                 : DISABLED
Mobility Anchor List
  IP Address                                    Priority
  -------------------------------------------------------
```

```
Device# show run | section profile policy

wireless profile policy default-policy-profile
 central switching
 description "default policy profile"
 static-ip-mobility
 vlan 50
 no shutdown
```

PART VIII

High Availability

- High Availability, on page 817



CHAPTER 90

High Availability

- Feature History for High Availability, on page 817
- Information About High Availability, on page 817
- Prerequisites for High Availability, on page 818
- Restrictions on High Availability, on page 819
- Configuring High Availability (CLI), on page 820
- Disabling High Availability, on page 822
- System and Network Fault Handling, on page 822
- Verifying High Availability Configurations, on page 828
- Verifying AP or Client SSO Statistics, on page 829
- Verifying High Availability, on page 831

Feature History for High Availability

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Table 30: Feature History for High Availability

Release	Feature	Feature Information
Cisco IOS XE Amsterdam 17.1.1s	Redundant Management Interface	The Redundancy Management Interface (RMI) is used as a secondary link between the active and standby controllers. This interface is the same as the Wireless Management Interface and the IP address on this interface is configured in the same subnet as the Wireless Management Interface.

Information About High Availability

High Availability (HA) allows you to reduce the downtime of wireless networks that occurs due to the failover of controllers. The HA Stateful Switch Over (SSO) capability on the controller allows AP to establish a CAPWAP tunnel with the active controller. The active controller shares a mirror copy of the AP and client database with the standby controller. The APs won't go into the discovery state and clients don't disconnect

when the active controller fails. The standby controller takes over the network as the active controller. Only one CAPWAP tunnel is maintained between the APs and the controller that is in an active state.

HA supports full AP and client SSO. Client SSO is supported only for clients that have completed the authentication and DHCP phase, and have started passing traffic. With Client SSO, the client information is synced to the standby controller when the client associates to the controller or when the client parameters change. Fully authenticated clients, for example, the ones in RUN state, are synced to the standby. Thus, client reassociation is avoided on switchover making the failover seamless for the APs and clients, resulting in zero client service downtime and zero SSID outage. This feature reduces major downtime in wireless networks due to failure conditions such as box failover, network failover, or power outage on the primary site.

Note

Note You can configure FIPS in HA setup. For information, see the Configuring FIPS in HA Setup.

Prerequisites for High Availability

External Interfaces and IPs

Because all the interfaces are configured only on the Active box, but are synchronized with the Standby box, the same set of interfaces are configured on both controllers. From external nodes, the interfaces connect to the same IP addresses, irrespective of the controllers they are connected to.

For this purpose, the APs, clients, DHCP, Cisco PrimeInfrastructure, Cisco DNA Centre, and Cisco Identity Services Engine (ISE) servers, and other controller members in the mobility group always connect to the same IP address. The SSO switchover is transparent to them. But if there are TCP connections from external nodes to the controller, the TCP connections need to be reset and reestablished.

HA Interfaces

The HA interface serves the following purposes:

- Provides connectivity between the controller pair before an IOSd comes up.
- Provides IPC transport across the controller pair.
- Enables redundancy across control messages exchanged between the controller pair. The control messages can be HA role resolution, keepalives, notifications, HA statistics, and so on.

You can select either SFP or RJ-45 connection for HA port. Supported Cisco SFPs are:

- GLC-SX-MMD
- GLC-LH-SMD

When either SFP or RJ-45 connection is present, HA works between the two controllers. The SFP HA connectivity takes priority over RJ-45 HA connectivity. If SFP is connected when RJ-45 HA is up and running, the HA pair reloads. The reload occurs even if the link between the SFPs isn't connected.

Restrictions on High Availability

- For a fail-safe SSO, wait till you receive the switchover event after completing configuration synchronization on the standby controller. If the standby controller has just been booted up, we recommend that you wait *x* minutes before the controller can handle switchover events without any problem. The value of *x* can change based on the platform. For example, a Cisco 9800-80 Series Controller running to its maximum capacity can take up to 24 minutes to complete the configuration synchronization before being ready for SSO. You can use the **show wireless stats redundancy config database** command to view the database-related statistics.
- The flow states of the NBAR engine are lost during a switchover in an HA scenario in local mode. Because of this, the classification of flows will restart, leading to incorrect packet classification as the first packet of the flow is missed.
- The HA connection supports only IPv4.
- Switchover and an active reload and forces a high availability link down from the new primary.
- Two HA interfaces (RMI and RP) must be configured on the same subnet, and the subnet cannot be shared with any other interfaces on the device.
- It is not possible to synchronize a TCP session state because a TCP session cannot survive after a switchover, and needs to be reestablished.
- The Client SSO does not address clients that have not reached the RUN state because they are removed after a switchover.
- Statistics tables are not synced from active to standby controller.
- Machine snapshot of a VM hosting controller HA interfaces is not supported. It may lead to a crash in the HA controller.
- Mobility-side restriction: Clients which are not in RUN state will be forcefully reauthenticated after switchover.
- The following application classification may not be retained after the SSO:
    - AVC limitation—After a switchover, the context transfer or synchronization to the Standby box does not occur and the new active flow needs to be relearned. The AVC QoS does not take effect during classification failure.
    - A voice call cannot be recognized after a switchover because a voice policy is based on RTP or RTCP protocol.
    - Auto QoS is not effective because of AVC limitation.
- The active controller and the standby controller must be paired with the same interface for virtual platforms. For hardware appliance, there is a dedicated HA port.
- Static IP addressing can synch to standby, but the IP address cannot be used from the standby controller.
- You can map a dedicated HA port to a 1 GB interface only.
- To use EtherChannels in HA mode in releases until, and including, Cisco IOS XE Gibraltar 16.12.x, ensure that the channel mode is set to On.

- Etherchannel Auto-mode is not supported in HA mode in releases until, and including, Cisco IOS XE Gibraltar 16.12.x.
- LACP and PAGP is not supported in HA mode in releases until, and including, Cisco IOS XE Gibraltar 16.12.x.
- When the controller works as a host for spanning tree, ensure that you configure portfast trunk in the uplink switch using s**panning-tree port type edge trunk** or **spanning-tree portfast trunk** command to ensure faster convergence.
- The **clear chassis redundancy** and **write erase** commands will not reset the chassis priority to the default value.
- While configuring devices in HA, the members must not have wireless trustpoint with the same name and different keys. In such a scenario, if you form an HA pair between the two standalone controllers, the wireless trustpoint does not come up after a subsequent SSO. The reason being the *rsa keypair* file exists but it is incorrect as the *nvram:private-config* file is not synched with the actual *WLC_WLC_TP* key pair.

  As a best practice, before forming an HA, it is recommended to delete the existing certificates and keys in each of the controllers which were previously deployed as standalone.
- After a switchover, when the recovery is in progress, do not configure the WLAN or WLAN policy. In case you configure, the controller can crash.
- After a switchover, clients that are not in RUN state and not connected to an AP are deleted after 300 seconds.

Configuring High Availability (CLI)

Before you begin

The active and standby controller should be in the same mode, either Install mode or Bundle mode, with same image version. We recommend that you use Install mode.

Procedure

	Command or Action	Purpose
Step 1	**chassis** *chassis-num* **priority** *chassis-priority* **Example:** `Device# chassis 1 priority 1`	(Optional) Configures the priority of the specified device. **Note** The new device priority will be effective after the next reboot. • *chassis-num*—Enter the chassis number. The range is from 1 to 2. • *chassis-priority*—Enter the chassis priority. The range is from 1 to 2. The default value is 1.

	Command or Action	Purpose
		Note When both the devices boot up at the same time, the device with higher priority(2) becomes active, and the other one becomes standby. If both the devices are configured with the same priority value, the one with the smaller MAC address acts as active and its peer acts as standby. You can get the **chassis-num** details by running the **show chassis** command.
Step 2	**chassis ha-interface GigabitEthernet** *num* **local-ip** *local-chassis-ip-addr network-mask* **remote-ip** *remote-chassis-ip-addr* **Example:** `Device# chassis ha-interface GigabitEthernet 2 local-ip 1.1.1.2 255.255.255.0 remote-ip 1.1.1.3`	Configures the chassis HA interface. **Note** This command is issued on both the devices of redundancy pair. • *num*—GigabitEthernet interface number. The range is from 0 to 32. • *local-chassis-ip-addr*—Enter the IP address of the local chassis HA interface. • *network-mask*—Enter the network mask or prefix length in the */nn* or *A.B.C.D* format. • *remote-chassis-ip-addr*—Enter the remote chassis IP address. **Note** Reload the devices for the changes to become effective.
Step 3	**chassis redundancy keep-alive timer** *timer* **Example:** `Device# chassis redundancy keep-alive timer 6`	Configures the peer keepalive timeout value. Time interval is set in multiple of 100 ms (enter 1 for default).
Step 4	**chassis redundancy keep-alive retries** *retry-value* **Example:** `Device# chassis redundancy keep-alive retries 8`	Configures the peer keepalive retry value before claiming peer is down. Default value is 5.

Disabling High Availability

If the controller is configured using RP method of SSO configuration, use the following command to clear all the HA-related parameters, such as local IP, remote IP, HA interface, mask, timeout, and priority:

clear chassis redundancy

If the controller is configured using RMI method, use the following command:

no redun-management interface vlan chassis

Note Reload the devices for the changes to take effect.

After the HA unpairing, the standby controller startup configuration and the HA configuration will be cleared and standby will go to Day 0.

Before the command is executed, the user is prompted with the following warning on the active controller:

```
Device# clear chassis redundancy

WARNING: Clearing the chassis HA configuration will result in both the chassis move into
Stand Alone mode. This involves reloading the standby chassis after clearing its HA
configuration and startup configuration which results in standby chassis coming up as a
totally
clean after reboot. Do you wish to continue? [y/n]? [yes]:

*Apr 3 23:42:22.985: received clear chassis.. ha_supported:1yes
WLC#
*Apr 3 23:42:25.042: clearing peer startup config
*Apr 3 23:42:25.042: chkpt send: sent msg type 2 to peer..
*Apr 3 23:42:25.043: chkpt send: sent msg type 1 to peer..
*Apr 3 23:42:25.043: Clearing HA configurations
*Apr 3 23:42:26.183: Successfully sent Set chassis mode msg for chassis 1.chasfs file updated
*Apr 3 23:42:26.359: %IOSXE_REDUNDANCY-6-PEER_LOST: Active detected chassis 2 is no
longer standby
```

On the standby controller, the following messages indicate that the configuration is being cleared:

```
Device-stby#

*Apr 3 23:40:40.537: mcprp_handle_spa_oir_tsm_event: subslot 0/0 event=2
*Apr 3 23:40:40.537: spa_oir_tsm subslot 0/0 TSM: during state ready, got event 3(ready)
*Apr 3 23:40:40.537: @@@ spa_oir_tsm subslot 0/0 TSM: ready -> ready
*Apr 3 23:42:25.041: Removing the startup config file on standby

!Standby controller is reloaded after clearing the chassis.
```

System and Network Fault Handling

If the standby controller crashes, it reboots and comes up as the standby controller. Bulk sync follows causing the standby to become hot. If the active controller crashes, the standby becomes active. The new active controller assumes the role of primary and tries to detect a dual active.

The following matrices provide a clear picture of the conditions the controller switchover would trigger:

Table 31: System and Network Fault Handling

System Issues				
Trigger	**RP Link Status**	**Peer Reachability through RMI**	**Switchover**	**Result**
Critical process crash	Up	Reachable	Yes	Switchover happens
Forced switchover	Up	Reachable	Yes	Switchover happens
Critical process crash	Up	Unreachable	Yes	Switchover happens
Forced switchover	Up	Unreachable	Yes	Switchover happens
Critical process crash	Down	Reachable	No	No action. One controller in recovery mode.
Forced switchover	Down	Reachable	N/A	No action. One controller in recovery mode.
Critical process crash	Down	Unreachable	No	Double fault – as mentioned in Network Error handling
Forced switchover	Down	Unreachable	N/A	Double fault – as mentioned in Network Error handling

RP Link	Peer Reachability Through RMI	Gateway From Active	Gateway From Standby	Switchover	Result
Up	Reachable	Reachable	Reachable	No SSO	No action

RP Link	Peer Reachability Through RMI	Gateway From Active	Gateway From Standby	Switchover	Result
Up	Reachable	Reachable	Unreachable	No SSO	No action. Standby is not ready for SSO in this state, as it does not have gateway reachability. The standby is shown to be in standby-recovery mode. If the RP goes down, standby (in recovery mode) becomes active.
Up	Reachable	Unreachable	Reachable	SSO	Gateway reachability message is exchanged over the RMI + RP links. Active reboots so that the standby becomes active.
Up	Reachable	Unreachable	Unreachable	No SSO	With this, when the active SVI goes down, the standby SVI also goes down. A switchover is then triggered. If the new active discovers its gateway to be reachable, the system stabilizes in the Active - Standby Recovery mode. Otherwise, switchovers happen in a ping-pong fashion.
Up	Unreachable	Reachable	Reachable	No SSO	No action

RP Link	Peer Reachability Through RMI	Gateway From Active	Gateway From Standby	Switchover	Result
Up	Unreachable	Reachable	Unreachable	No SSO	Standby is not ready for SSO in this state as it does not have gateway reachability. Standby moves in to recovery mode as LMP messages are exchanged over the RP link.
Up	Unreachable	Unreachable	Reachable	SSO	Gateway reachability message is exchanged over RP link. Active reboots so that standby becomes active.
Up	Unreachable	Unreachable	Unreachable	No SSO	With this, when the active SVI goes down, the standby SVI also goes down. A switchover is then triggered. If the new active discovers its gateway to be reachable, the system stabilizes in Active - Standby Recovery mode. Otherwise, switchovers happen in a ping-pong fashion.

RP Link	Peer Reachability Through RMI	Gateway From Active	Gateway From Standby	Switchover	Result
Down	Reachable	Reachable	Reachable	No SSO	Standby becomes active with (old) active going in to active-recovery mode. Configuration mode is disabled in active-recovery mode. All interfaces will be ADMIN DOWN with the wireless management interface having RMI IP. The controller in the active-recovery mode will reload to become standby when the RP link comes UP.
Down	Reachable	Reachable	Unreachable	No SSO	Same as above.

RP Link	Peer Reachability Through RMI	Gateway From Active	Gateway From Standby	Switchover	Result
Down	Reachable	Unreachable	Reachable	RP link down, then active loses GW, then there won't be any SSO. GW down, within 8 seconds, RP link goes down, then there would be a SSO.	Gateway reachability message is exchanged over RP+RMI links. Old-Active goes to active-recovery mode. The configuration mode is disabled in active-recovery mode. All interfaces will be ADMIN DOWN with the wireless management interface having RMI IP. The controller in active-recovery will reload to become standby (or standby-recovery if gateway reachabilty is still not available) when the RP link comes up.
Down	Reachable	Unreachable	Unreachable	No SSO	Standby goes to standby-recovery.

RP Link	Peer Reachability Through RMI	Gateway From Active	Gateway From Standby	Switchover	Result
Down	Unreachable	Reachable	Reachable	SSO	Double fault – this may result in a network conflict as there will be two active controllers. Standby becomes active. Old active also exists. Role negotiation has to happen once the connectivity is restored and keep the active that came up last.
Down	Unreachable	Reachable	Unreachable	SSO	Same as above.
Down	Unreachable	Unreachable	Reachable	SSO	Same as above.
Down	Unreachable	Unreachable	Unreachable	SSO	Same as above.

Verifying High Availability Configurations

To view the HA configuration details, use the following command:

```
Device# show romvar
ROMMON variables:
 LICENSE_BOOT_LEVEL =
 MCP_STARTUP_TRACEFLAGS = 00000000:00000000
 BOOTLDR =
 CRASHINFO = bootflash:crashinfo_RP_00_00_20180202-034353-UTC
 STACK_1_1 = 0_0
 CONFIG_FILE =
 BOOT =
bootflash:boot_image_test,1;bootflash:boot_image_good,1;bootflash:rp_super_universalk9.vwlc.bin,1;

 RET_2_RTS =
 SWITCH_NUMBER = 1
 CHASSIS_HA_REMOTE_IP = 10.0.1.9
 CHASSIS_HA_LOCAL_IP = 10.0.1.10
 CHASSIS_HA_LOCAL_MASK = 255.255.255.0
 CHASSIS_HA_IFNAME = GigabitEthernet2
 CHASSIS_HA_IFMAC = 00:0C:29:C9:12:0B
 RET_2_RCALTS =
 BSI = 0
 RANDOM_NUM = 647419395
```

Verifying AP or Client SSO Statistics

To view the AP SSO statistics, use the following command:

```
Device# show wireless stat redundancy statistics ap-recovery wnc all
AP SSO Statistics

Inst    Timestamp     Dura(ms)   #APs  #Succ  #Fail  Avg(ms)  Min(ms)  Max(ms)
-------------------------------------------------------------------------------
   0    00:06:29.042        98     34     34      0        2        1       35
   1    00:06:29.057        56     33     30      3        1        1       15
   2    00:06:29.070        82     33     33      0        2        1       13


Statistics:

WNCD Instance   : 0
No. of AP radio recovery failures          : 0
No. of AP BSSID recovery failures          : 0
No. of CAPWAP recovery failures            : 0
No. of DTLS recovery failures              : 0
No. of reconcile message send failed       : 0
No. of reconcile message successfully sent : 34
No. of Mesh BSSID recovery failures: 0
No. of Partial delete cleanup done : 0
.
.
.
```

To view the Client SSO statistics, use the following command:

```
Device# show wireless stat redundancy client-recovery wncd all
Client SSO statistics
---------------------

WNCD instance  : 1
Reconcile messages received from AP                    : 1
Reconcile clients received from AP                     : 1
Recreate attempted post switchover                     : 1
Recreate attempted by SANET Lib                        : 0
Recreate attempted by DOT1x Lib                        : 0
Recreate attempted by SISF Lib                         : 0
Recreate attempted by SVC CO Lib                       : 1
Recreate attempted by Unknown Lib                      : 0
Recreate succeeded post switchover                     : 1
Recreate Failed post switchover                        : 0
Stale client entries purged post switchover            : 0

Partial delete during heap recreate                    : 0
Partial delete during force purge                      : 0
Partial delete post restart                            : 0
Partial delete due to AP recovery failure              : 0
Partial delete during reconcilation                    : 0

Client entries in shadow list during SSO               : 0
Client entries in shadow default state during SSO      : 0
Client entries in poison list during SSO               : 0

Invalid bssid during heap recreate                     : 0
Invalid bssid during force purge                       : 0
BSSID mismatch with shadow rec during reconcilation    : 0
BSSID mismatch with shadow rec reconcilation(WGB client): 0
```

```
BSSID mismatch with dot11 rec during heap recreate      : 0

AID mismatch with dot11 rec during force purge          : 0
AP slotid mismatch during reconcilation                 : 0
Zero aid during heap recreate                           : 0
AID mismatch with shadow rec during reconcilation       : 0
AP slotid mismatch shadow rec during reconcilation      : 0
Client shadow record not present                        : 0
```

To view the mobility details, use the following command:

```
Device# show wireless stat redundancy client-recovery mobilityd
Mobility Client Deletion Reason Statistics
------------------------------------------
Mobility Incomplete State         : 0
Inconsistency in WNCD & Mobility  : 0
Partial Delete                    : 0

General statistics
--------------------
Cleanup sent to WNCD, Missing Delete case   : 0
```

To view the Client SSO statistics for SISF, use the following command:

```
Device# show wireless stat redundancy client-recovery sisf
Client SSO statistics for SISF
-------------------------------
Number of recreate attempted post switchover    : 1
Number of recreate succeeded post switchover    : 1
Number of recreate failed because of no mac     : 0
Number of recreate failed because of no ip      : 0
Number of ipv4 entry recreate success           : 1
Number of ipv4 entry recreate failed            : 0
Number of ipv6 entry recreate success           : 0
Number of ipv6 entry recreate failed            : 0
Number of partial delete received               : 0
Number of client purge attempted                : 0
Number of heap and db entry purge success       : 0
Number of purge success for db entry only       : 0
Number of client purge failed                   : 0
Number of garp sent                             : 1
Number of garp failed                           : 0
Number of IP entries validated in cleanup       : 0
Number of IP entry address errors in cleanup    : 0
Number of IP entry deleted in cleanup           : 0
Number of IP entry delete failed in cleanup     : 0
Number of IP table create callbacks on standby  : 0
Number of IP table modify callbacks on standby  : 0
Number of IP table delete callbacks on standby  : 0
Number of MAC table create callbacks on standby : 1
Number of MAC table modify callbacks on standby : 0
Number of MAC table delete callbacks on standby : 0
```

To view the HA redundancy summary, use the following command:

```
Device# show wireless stat redundancy summary
HA redundancy summary
---------------------

AP recovery duration (ms)        : 264
SSO HA sync timer expired        : No
```

Verifying High Availability

Table 32: Commands for Monitoring Chassis and Redundancy

Command Name	Description
show chassis	Displays the chassis information. **Note** When the peer timeout and retries are configured, the **show chassis ha-status** command output may show incorrect values. To check the peer keep-alive timer and retries, use the following commands: • **show platform software stack-mgr chassis active r0 peer-timeout** • **show platform software stack-mgr chassis standby r0 peer-timeout**
show redundancy	Displays details about Active box and Standby box.
show redundancy switchover history	Displays the switchover counts, switchover reason, and the switchover time.

To start the packet capture in the redundancy HA port (RP), use the following commands:

- test wireless redundancy packetdump start
- test wireless redundancy packetdump stop
- test wireless redundancy packetdump start filter port 2300

```
Device# test wireless redundancy packetdump start
Redundancy Port PacketDump Start
Packet capture started on RP port.

Device# test wireless redundancy packetdump stop
Redundancy Port PacketDump Start
Packet capture started on RP port.
Redundancy Port PacketDump Stop
Packet capture stopped on RP port.
Device# dir bootflash:
Directory of bootflash:/
1062881  drwx           151552  Oct 20 2020 23:15:25 +00:00  tracelogs
47       -rw-           20480  Oct 20 2020 23:15:24 +00:00  haIntCaptureLo.pcap
1177345  drwx             4096  Oct 20 2020 19:56:14 +00:00  certs
294337   drwx             8192  Oct 20 2020 19:56:05 +00:00  license_evlog
15       -rw-              676  Oct 20 2020 19:56:01 +00:00  vlan.dat
14       -rw-               30  Oct 20 2020 19:55:16 +00:00  throughput_monitor_params
13       -rw-           134808  Oct 20 2020 19:54:57 +00:00  memleak.tcl
1586145  drwx             4096  Oct 20 2020 19:54:45 +00:00  .inv
1103761  drwx             4096  Oct 20 2020 19:54:39 +00:00  dc_profile_dir
17       -r--              114  Oct 20 2020 19:54:17 +00:00  debug.conf
1389921  drwx             4096  Oct 20 2020 19:54:17 +00:00  .installer
46       -rw-       1104760207  Oct 20 2020 19:26:41 +00:00  leela_katar_rping_test.SSA.bin
49057    drwx             4096  Oct 20 2020 16:11:21 +00:00  .prst_sync
```

```
45      -rw-       1104803200  Oct 20 2020 15:39:19 +00:00
C9800-L-universalk9_wlc.2020-10-20_14.57_yavadhan.SSA.bin
269809  drwx             4096  Oct 19 2020 23:41:49 +00:00  core
44      -rw-       1104751981  Oct 19 2020 17:42:12 +00:00
C9800-L-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20201018_053825_2.SSA.bin
43      -rw-       1104286975  Oct 16 2020 12:05:47 +00:00
C9800-L-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20201010_001654_2.SSA.bin

Device# test wireless redundancy packetdump start filter port 2300
Redundancy Port PacketDump Start
Packet capture started on RP port with port filter 2300.
```

To check connection between the two HA Ports (RP) and check if there are any drops, delays, or jitter in the connection, use the following command:

```
Device# test wireless redundancy rping
Redundancy Port ping
PING 169.254.64.60 (169.254.64.60) 56(84) bytes of data.
64 bytes from 169.254.64.60: icmp_seq=1 ttl=64 time=0.083 ms
64 bytes from 169.254.64.60: icmp_seq=2 ttl=64 time=0.091 ms
64 bytes from 169.254.64.60: icmp_seq=3 ttl=64 time=0.074 ms

--- 169.254.64.60 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2041ms
rtt min/avg/max/mdev = 0.074/0.082/0.091/0.007 ms
test wireless redundancy
```

To see the HA port interface setting status, use the **show platform hardware slot R0 ha_port interface stats** command.

```
Device# show platform hardware slot R0 ha_port interface stats
HA Port
ha_port   Link encap:Ethernet  HWaddr 70:18:a7:c8:80:70
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Memory:e0900000-e0920000

Settings for ha_port:
        Supported ports:            [ TP ]
        Supported link modes:       10baseT/Half 10baseT/Full
                                    100baseT/Half 100baseT/Full
                                    1000baseT/Full
        Supported pause frame use:   Symmetric
        Supports auto-negotiation:   Yes
        Supported FEC modes:         Not reported
        Advertised link modes:       10baseT/Half 10baseT/Full
                                     100baseT/Half 100baseT/Full
                                     1000baseT/Full
        Advertised pause frame use:  Symmetric
        Advertised auto-negotiation: Yes
        Advertised FEC modes:        Not reported
        Speed:                       Unknown!
        Duplex:                      Unknown! (255)
        Port:                        Twisted Pair
        PHYAD:                       1
        Transceiver:                 internal
        Auto-negotiation:            on
        MDI-X:                       off (auto)
        Supports Wake-on:            pumbg
        Wake-on:                     g
        Current message level:       0x00000007 (7)
```

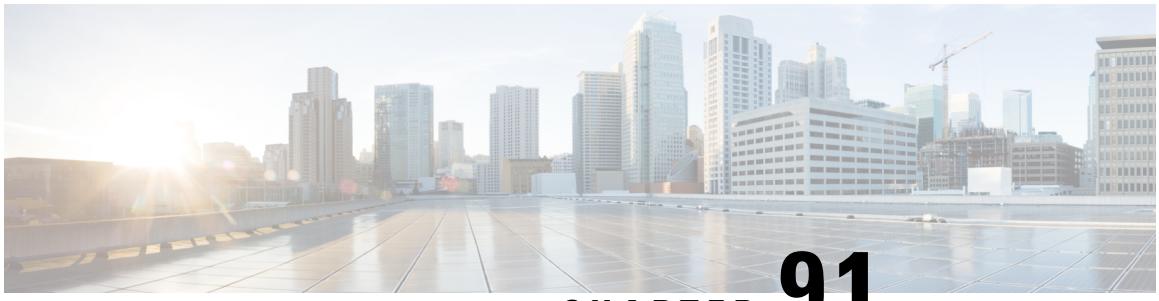
```
                                        drv probe link
        Link detected:                  no

NIC statistics:
     rx_packets:             0
     tx_packets:             0
     rx_bytes:               0
     tx_bytes:               0
     rx_broadcast:           0
     tx_broadcast:           0
     rx_multicast:           0
     tx_multicast:           0
     multicast:              0
     collisions:             0
     rx_crc_errors:          0
     rx_no_buffer_count:     0
     rx_missed_errors:       0
     tx_aborted_errors:      0
     tx_carrier_errors:      0
     tx_window_errors:       0
     tx_abort_late_coll:     0
     tx_deferred_ok:         0
     tx_single_coll_ok:      0
     tx_multi_coll_ok:       0
     tx_timeout_count:       0
     rx_long_length_errors:  0
     rx_short_length_errors: 0
     rx_align_errors:        0
     tx_tcp_seg_good:        0
     tx_tcp_seg_failed:      0
     rx_flow_control_xon:    0
     rx_flow_control_xoff:   0
     tx_flow_control_xon:    0
     tx_flow_control_xoff:   0
     rx_long_byte_count:     0
     tx_dma_out_of_sync:     0
     tx_smbus:               0
     rx_smbus:               0
     dropped_smbus:          0
     os2bmc_rx_by_bmc:       0
     os2bmc_tx_by_bmc:       0
     os2bmc_tx_by_host:      0
     os2bmc_rx_by_host:      0
     tx_hwtstamp_timeouts:   0
     rx_hwtstamp_cleared:    0
     rx_errors:              0
     tx_errors:              0
     tx_dropped:             0
     rx_length_errors:       0
     rx_over_errors:         0
     rx_frame_errors:        0
     rx_fifo_errors:         0
     tx_fifo_errors:         0
     tx_heartbeat_errors:    0
     tx_queue_0_packets:     0
     tx_queue_0_bytes:       0
     tx_queue_0_restart:     0
     tx_queue_1_packets:     0
     tx_queue_1_bytes:       0
     tx_queue_1_restart:     0
     rx_queue_0_packets:     0
     rx_queue_0_bytes:       0
     rx_queue_0_drops:       0
     rx_queue_0_csum_err:    0
```

```
rx_queue_0_alloc_failed:0
rx_queue_1_packets:     0
rx_queue_1_bytes:       0
rx_queue_1_drops:       0
rx_queue_1_csum_err:    0
rx_queue_1_alloc_failed:0
```

PART IX

Quality of Service

- Quality of Service, on page 837
- Wireless Auto-QoS, on page 871
- Native Profiling, on page 877
- Air Time Fairness, on page 889



CHAPTER 91

Quality of Service

- Wireless QoS Overview, on page 837
- Wireless QoS Targets, on page 837
- Wireless QoS Mobility, on page 839
- Precious Metal Policies for Wireless QoS, on page 839
- Prerequisites for Wireless QoS, on page 840
- Restrictions for QoS on Wireless Targets, on page 840
- Metal Policy Format, on page 841
- How to apply Bi-Directional Rate Limiting, on page 848
- How to apply Per Client Bi-Directional Rate Limiting, on page 855
- How to Configure Wireless QoS, on page 859
- SIP Call Admission Control (CAC), on page 864
- SIP Voice Call Snooping, on page 867

Wireless QoS Overview

Quality of Service (QoS), provides the ability to prioritize the traffic by giving preferential treatment to specific traffic over the other traffic types. Without QoS, the device offers best-effort service for each packet, regardless of the packet contents or size. The device sends the packets without any assurance of reliability, delay bounds, or throughput.

A target is the entity where the policy is applied. Wireless QoS policies for SSID and client are applied in the upstream and (or) downstream direction. The flow of traffic from a wired source to a wireless target is known as downstream traffic. The flow of traffic from a wireless source to a wired target is known as upstream traffic.

The following are some of the specific features provided by wireless QoS:

- SSID and client policies on wireless QoS targets
- Marking and Policing (also known as Rate Limiting) of wireless traffic
- Mobility support for QoS

Wireless QoS Targets

This section describes the various wireless QoS targets available on a device.

SSID Policies

You can create QoS policies on SSID in both the ingress and egress directions. If not configured, there is no SSID policy applied.

The policy is applicable per AP per SSID.

You can configure policing and marking policies on SSID.

Client Policies

Client policies are applicable in the ingress and egress direction. You can configure policing and marking policies on clients. AAA override is also supported.

Supported QoS Features on Wireless Targets

This table describes the various features available on wireless targets.

Table 33: QoS Features Available on Wireless Targets

Target	Features	Direction Where Policies Are Applicable
SSID	• Set • Police • Drop	Upstream and downstream
Client	• Set • Police • Drop	Upstream and downstream

This table describes the various features available on wireless targets.

Table 34: QoS Policy Actions

Policy Action Types	Wireless Target Support	
	Local Mode	Flex Mode
Police	Supported	Supported
Set	Supported	Supported

This table describes the various features available on wireless targets.

Table 35: QoS Policy Set Actions

Set Action Types	Supported	
	Local Mode	Flex Mode
set dscp	Supported	Supported
set qos-group	Supported	Not Supported
set wlan user-priority (downstream only)	Supported (BSSID only)	Supported (BSSID only)

Wireless QoS Mobility

Wireless QoS mobility enables you to configure QoS policies so that the network provides the same service anywhere in the network. A wireless client can roam from one location to another and as a result the client can get associated to different access points associated with a different device. Wireless client roaming can be classified into two types:

- Intra-device roaming
- Inter-device roaming

Note In a foreign WLC, client statistics are not displayed.

Note The client policies must be available on all of the devices in the mobility group. The same SSID policy must be applied to all devices in the mobility group so that the clients get consistent treatment.

Precious Metal Policies for Wireless QoS

The precious metal policies are system-defined policies that are available on the controller . They cannot be removed or changed.

The following policies are available:

- Platinum—Used for VoIP clients.
- Gold—Used for video clients.
- Silver— Used for traffic that can be considered best-effort.
- Bronze—Used for NRT traffic.

These policies are pre-configured. They cannot be modified.

For client metal policies, they can be pushed using AAA.

Based on the policies applied, the 802.11e (WMM), and DSCP fields in the packets are affected.

For more information about metal policies format see the Metal Policy Format, on page 841 section.

For more information about DSCP to UP mapping, see the Architecture for Voice, Video and Integrated Data (AVVID), on page 847 table.

Prerequisites for Wireless QoS

Before configuring wireless QoS, you must have a thorough understanding of these items:

- Wireless concepts and network topologies.
- Understanding of QoS implementation.
- Modular QoS CLI (MQC). For more information on Modular QoS, see the MQC guide
- The types of applications used and the traffic patterns on your network.
- Bandwidth requirements and speed of the network.

Restrictions for QoS on Wireless Targets

General Restrictions

A target is an entity where a policy is applied. A policy can be applied to a wireless target, which can be an SSID or client target, in the downstream and/or upstream direction. Downstream indicates that traffic is flowing from the controller to the wireless client. Upstream indicates that traffic is flowing from wireless client to the controller.

- Hierarchical (Parent policy and child policy) QoS is not supported.
- SSID and client targets can be configured only with marking and policing policies.
- One policy per target per direction is supported.
- Class maps in a policy map can have different types of filters. However, only one marking action (set dscp) is supported.
- Only one set action per class is supported.
- Access group matching is not supported.
- Access group (ACL) matching is not supported by access points in flex mode for local switching traffic.
- SIP Call Admission Control (CAC) is not supported on the central switching mode.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, SIP Call Admission Control (CAC) is not supported.
- Applying QoS on the WMI interface is not supported, as it may reboot the controller.

AP Side Restrictions

- In Cisco Embedded Wireless Controller, FlexConnect local switching, and SDA deployments, the QoS policies are enforced on the AP. Due to this AP-side restriction, police actions (e.g., rate limiting) are only enforced at a per flow (5-tuple) level and not per client.
- For FlexConnect local switching (local authentication) with AAA override enabled and external AAA server, only air space VLAN and ACL are supported as part of the AAA override and not the QoS override or other overrides.

Control Plane Rate Limiting and Policing

You need not explicitly configure control plane rate limiting or policing on the controller. The controller has embedded mechanisms (like policers) to protect the CPU by policing control plane traffic directed towards it. If you're migrating from AireOS to IOS-XE, this change is taken care of at the code level.

Metal Policy Format

Metal Policy Format

Metal Policies are system defined, and you cannot change it or delete it. There are four levels of metal policy - Platinum, Gold, Silver, and Bronze.

Note Each metal policy defines a DSCP ceiling so that the DSCP or the UP marking does not exceed a certain value.

For Platinum the value is 46, Gold is AF41, Silver is 22, and Bronze is CS1.

Policy Name	Policy-map Format	Class-map Format
platinum	policy-map platinum class cm-dscp-34 set dscp af41 class cm-dscp-45 set dscp 45 class cm-dscp-46 set dscp ef class cm-dscp-47 set dscp 47	class-map match-any cm-dscp-34 match dscp af41 class-map match-any cm-dscp-45 match dscp 45 class-map match-any cm-dscp-46 match dscp ef class-map match-any cm-dscp-47 match dscp 47 class-map match-any cm-dscp-0 match dscp default
gold	policy-map gold class cm-dscp-45 set dscp af41 class cm-dscp-46 set dscp af41 class cm-dscp-47 set dscp af41	
silver	policy-map silver class cm-dscp-34 set dscp default class cm-dscp-45 set dscp default class cm-dscp-46 set dscp default class cm-dscp-47 set dscp default	
bronze	policy-map bronze class cm-dscp-0 set dscp cs1 class cm-dscp-34 set dscp cs1 class cm-dscp-45 set dscp cs1 class cm-dscp-46 set dscp cs1 class cm-dscp-47 set dscp cs1	

Policy Name	Policy-map Format	Class-map Format

platinum-up	policy-map platinum-up
	 class cm-dscp-set1-for-up-4
	  set dscp af41
	 class cm-dscp-set2-for-up-4
	  set dscp af41
	 class cm-dscp-for-up-5
	  set dscp af41
	 class cm-dscp-for-up-6
	  set dscp ef
	 class cm-dscp-for-up-7
	  set dscp ef
		class-map match-any cm-dscp-for-up-0
		  match dscp default
		  match dscp cs2
		class-map match-any cm-dscp-for-up-1
		  match dscp cs1
		class-map match-any cm-dscp-set1-for-up-4
		  match dscp cs3
		  match dscp af31
		  match dscp af32
		  match dscp af33
		class-map match-any cm-dscp-set2-for-up-4
		  match dscp af41
		  match dscp af42
		  match dscp af43
		class-map match-any cm-dscp-for-up-5
		  match dscp cs4
		  match dscp cs5
		class-map match-any cm-dscp-for-up-6
		  match dscp 44
		  match dscp ef
		class-map match-any cm-dscp-for-up-7
		  match dscp cs6
		  match dscp cs7

gold-up	policy-map gold-up
	 class cm-dscp-for-up-6
	  set dscp af41
	 class cm-dscp-for-up-7
	  set dscp af41	

silver-up	policy-map silver-up
	 class cm-dscp-set1-for-up-4
	  set dscp default
	 class cm-dscp-set2-for-up-4
	  set dscp default
	 class cm-dscp-for-up-5
	  set dscp default
	 class cm-dscp-for-up-6
	  set dscp default
	 class cm-dscp-for-up-7
	  set dscp default	

bronze-up	policy-map bronze-up
	 class cm-dscp-for-up-0
	  set dscp cs1
	 class cm-dscp-for-up-1
	  set dscp cs1
	 class cm-dscp-set1-for-up-4
	  set dscp cs1
	 class cm-dscp-set2-for-up-4
	  set dscp cs1
	 class cm-dscp-for-up-5
	  set dscp cs1
	 class cm-dscp-for-up-6
	  set dscp cs1
	 class cm-dscp-for-up-7
	  set dscp cs1	

Policy Name	Policy-map Format	Class-map Format
clwmm-platinum	policy-map clwmm-platinum class voice-plat set dscp ef class video-plat set dscp af41 class class-default set dscp default	class-map match-any voice-plat match dscp ef class-map match-any video-plat match dscp af41 class-map match-any voice-gold match dscp ef class-map match-any video-gold match dscp af41
clwmm-gold	policy-map clwmm-gold class voice-gold set dscp af41 class video-gold set dscp af41 class class-default set dscp default	
clnon-wmm-platinum	policy-map clnon-wmm-platinum class class-default set dscp ef	
clnon-wmm-gold	policy-map clnon-wmm-gold class class-default set dscp af41	
clsilver	policy-map clsilver class class-default set dscp default	
clbronze	policy-map clbronze class class-default set dscp cs1	

Auto QoS Policy Format

Policy Name	Policy-map Format	Class-map Format
enterprise-avc	policy-map AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy class AutoQos-4.0-wlan-Voip-Data-Class set dscp ef class AutoQos-4.0-wlan-Voip-Signal-Class set dscp cs3 class AutoQos-4.0-wlan-Multimedia-Conf-Class set dscp af41 class AutoQos-4.0-wlan-Transaction-Class set dscp af21 class AutoQos-4.0-wlan-Bulk-Data-Class set dscp af11 class AutoQos-4.0-wlan-Scavanger-Class set dscp cs1 class class-default set dscp default policy-map AutoQos-4.0-wlan-ET-SSID-Output-Policy class AutoQos-4.0-RT1-Class set dscp ef class AutoQos-4.0-RT2-Class set dscp af31 class class-default	

Policy Name	Policy-map Format	Class-map Format
		class-map match-any AutoQos-4.0-wlan-Voip-Data-Class match dscp ef class-map match-any AutoQos-4.0-wlan-Voip-Signal-Class match protocol skinny match protocol cisco-jabber-control match protocol sip match protocol sip-tls class-map match-any AutoQos-4.0-wlan-Multimedia-Conf-Class match protocol cisco-phone-video match protocol cisco-jabber-video match protocol ms-lync-video match protocol webex-media class-map match-any AutoQos-4.0-wlan-Transaction-Class match protocol cisco-jabber-im match protocol ms-office-web-apps match protocol salesforce match protocol sap class-map match-any AutoQos-4.0-wlan-Bulk-Data-Class match protocol ftp match protocol ftp-data match protocol ftps-data match protocol cifs class-map match-any AutoQos-4.0-wlan-Scavanger-Class match protocol netflix match protocol youtube match protocol skype match protocol bittorrent class-map match-any AutoQos-4.0-RT1-Class match dscp ef

Policy Name	Policy-map Format	Class-map Format
		match dscp cs6 class-map match-any AutoQos-4.0-RT2-Class match dscp cs4 match dscp cs3 match dscp af41
voice	policy-map platinum-up class dscp-for-up-4 set dscp 34 class dscp-for-up-5 set dscp 34 class dscp-for-up-6 set dscp 46 class dscp-for-up-7 set dscp 46 policy-map platinum class cm-dscp-34 set dscp 34 class cm-dscp-46 set dscp 46	
guest	Policy Map AutoQos-4.0-wlan-GT-SSID-Output-Policy Class class-default set dscp default Policy Map AutoQos-4.0-wlan-GT-SSID-Input-Policy Class class-default set dscp default	
port (only applies to Local Mode)	policy-map AutoQos-4.0-wlan-Port-Output-Policy class AutoQos-4.0-Output-CAPWAP-C-Class priority level 1 class AutoQos-4.0-Output-Voice-Class priority level 2 class class-default ip access-list extended AutoQos-4.0-Output-Acl-CAPWAP-C permit udp any eq 5246 16666 any	class-map match-any AutoQos-4.0-Output-CAPWAP-C-Class match access-group name AutoQos-4.0-Output-Acl-CAPWAP-C class-map match-any AutoQos-4.0-Output-Voice-Class match dscp ef

Architecture for Voice, Video and Integrated Data (AVVID)

IETF DiffServ Service Class	DSCP	IEEE 802.11e	
		User Priority	Access Category
Network Control	(CS7) CS6	0	AC_BE
Telephony	EF	6	AC_VO
VOICE-ADMIT	44	6	AC_VO
Signaling	CS5	5	AC_VI

IETF DiffServ Service Class	DSCP	IEEE 802.11e	
		User Priority	Access Category
Multimedia Conferencing	AF41 AF42 AF43	4	AC_VI
Real-Time Interactive	CS4	5	AC_VI
Multimedia Streaming	AF31 AF32 AF33	4	AC_VI
Broadcast Video	CS3	4	AC_VI
Low-Latency Data	AF21 AF22 AF23	3	AC_BE
OAM	CS2	0	AC_BE
High-Throughput Data	AF11 AF12 AF13	2	AC_BK
Standard	DF	0	AC_BE
Low-Priority Data	CS1	1	AC_BK
Remaining	Remaining	0	

How to apply Bi-Directional Rate Limiting

Information about Bi-Directional Rate Limiting

Bi-Directional Rate Limiting (BDRL) feature defines rate limits on both upstream and downstream traffic. These rate limits are individually configured. The rate limits can be configured on WLAN directly instead of QoS profiles, which will override QoS profile values. The WLAN rate limiting will always supersede Global QoS setting for controller and clients.

BDRL feature defines throughput limits for clients on their wireless networks and allows setting a priority service to a particular set of clients.

The following four QoS profiles are available to configure the rate limits:

- Gold

- Platinum
- Silver
- Bronze

The QoS profile is applied to all clients on the associated SSID. Therefore all clients connected to the same SSID will have the same rate limits.

To configure BDRL, select the QoS profile and configure the various rate limiting parameters. When rate limiting parameters are set to *0*, the rate limiting feature is not functional. Each WLAN has a QoS profile associated with it in addition to the configuration in the QoS profile.

Note BDRL in a mobility Anchor-Foreign setup must be configured both on Anchor and Foreign controller. As a best practice, it is recommended to perform identical configuration on both the controllers to avoid breakage of any feature.

BDRL is is supported on Guest anchor scenarios. The feature is supported on IRCM guest scenarios with AireOS as Guest anchor or Guest Foreign. Cisco Catalyst 9800 Series Wireless Controller uses **Policing** option to rate limit the traffic.

To apply metal policy with BDRL, perform the following tasks:

- Configure Metal Policy on SSID
- Configure Metal Policy on Client
- Configure Bi-Directional Rate Limiting for All Traffic, on page 851
- Configure Bi-Directional Rate Limiting Based on Traffic Classification, on page 851
- Apply Bi-Directional Rate Limiting Policy Map to Policy Profile, on page 853
- Apply Metal Policy with Bi-Directional Rate Limiting, on page 854

Prerequisites for Bi-Directional Rate Limiting

- Client metal policy is applied through AAA-override.
- You must specify the metal policy on ISE server.
- AAA-override must be enabled on policy profile.

Configure Metal Policy on SSID

Procedure

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

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile1`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**description** *description* **Example:** `Device(config-wireless-policy)# description policy-profile1`	Adds a user defined description to the new wireless policy.
Step 4	**service-policy input** *input-policy* **Example:** `Device(config-wireless-policy)# service-policy input platinum-up`	Sets platinum policy for input.
Step 5	**service-policy output** *output-policy* **Example:** `Device(config-wireless-policy)# service-policy output platinum`	Sets platinum policy for output.

Configure Metal Policy on Client

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile1`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**description** *description* **Example:** `Device(config-wireless-policy)# description profile with aaa override`	Adds a user defined description to the new wireless policy.
Step 4	**aaa-override** **Example:**	Enables AAA override on the WLAN.

	Command or Action	Purpose
	`Device(config-wireless-policy)# aaa-override`	**Note** After AAA-override is enabled and ISE server starts sending policy, client policy defined in service-policy client will not take effect.

Configure Bi-Directional Rate Limiting for All Traffic

Use the police action in the policy-map to configure BDRL.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map** *policy-map* **Example:** `Device(config)# policy-map policy-sample 1`	Creates a named object representing a set of policies that are to be applied to a set of traffic classes. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**class** *class-map-name* **Example:** `Device(config-pmap)# class class-default`	Associates a class map with the policy map, and enters policy-map class configuration mode.
Step 4	**police** *rate* **Example:** `Device(config-pmap-c)# police 500000`	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.

Configure Bi-Directional Rate Limiting Based on Traffic Classification

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map** *policy-map* **Example:**	Creates a named object representing a set of policies that are to be applied to a set of traffic classes. Policy-map names can contain

	Command or Action	Purpose
	`Device(config)# policy-map policy-sample2`	alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**class** *class-map-name* **Example:** `Device(config-pmap)# class class-sample-youtube`	Associates a class map with the policy map, and enters policy-map class configuration mode.
Step 4	**police** *rate* **Example:** `Device(config-pmap-c)# police 1000000`	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.
Step 5	**conform-action drop** **Example:** `Device(config-pmap-c-police)# conform-action drop`	Specifies the drop action to take on packets that conform to the rate limit.
Step 6	**exceed-action drop** **Example:** `Device(config-pmap-c-police)# exceed-action drop`	Specifies the drop action to take on packets that exceeds the rate limit.
Step 7	**exit** **Example:** `Device(config-pmap-c-police)# exit`	Exits the policy-map class configuration mode.
Step 8	**set dscp default** **Example:** `Device(config-pmap-c)# set dscp default`	Sets the DSCP value to default.
Step 9	**police** *rate* **Example:** `Device(config-pmap-c)# police 500000`	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.
Step 10	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits the policy-map class configuration mode.
Step 11	**exit** **Example:** `Device(config-pmap)# exit`	Exits the policy-map configuration mode.
Step 12	**class-map match-any** *class-map-name* **Example:**	Selects a class map.

	Command or Action	Purpose
	`Device(config)# class-map match-any class-sample-youtube`	
Step 13	**match protocol** *protocol* **Example:** `Device(config-cmap)# match protocol youtube`	Configures the match criteria for a class map on the basis of the specified protocol.

Apply Bi-Directional Rate Limiting Policy Map to Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile3`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**description** *description* **Example:** `Device(config-wireless-policy)# description policy-profile3`	Adds a user defined description to the new wireless policy.
Step 4	**service-policy client input** *input-policy* **Example:** `Device(config-wireless-policy)# service-policy client input platinum-up`	Sets the input client service policy as platinum.
Step 5	**service-policy client output** *output-policy* **Example:** `Device(config-wireless-policy)# service-policy client output platinum`	Sets the output client service policy as platinum.
Step 6	**service-policy input** *input-policy* **Example:** `Device(config-wireless-policy)# service-policy input platinum-up`	Sets the input service policy as platinum.
Step 7	**service-policy output** *output-policy* **Example:** `Device(config-wireless-policy)# service-policy output platinum`	Sets the output service policy as platinum.

Apply Metal Policy with Bi-Directional Rate Limiting

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile3`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**description** *description* **Example:** `Device(config-wireless-policy)# description policy-profile3`	Adds a user defined description to the new wireless policy.
Step 4	**service-policy client input** *input-policy* **Example:** `Device(config-wireless-policy)# service-policy client input platinum-up`	Sets the input client service policy as platinum.
Step 5	**service-policy client output** *output-policy* **Example:** `Device(config-wireless-policy)# service-policy client output platinum`	Sets the output client service policy as platinum.
Step 6	**service-policy input** *input-policy* **Example:** `Device(config-wireless-policy)# service-policy input platinum-up`	Sets the input service policy as platinum.
Step 7	**service-policy output** *output-policy* **Example:** `Device(config-wireless-policy)# service-policy output platinum`	Sets the output service policy as platinum.
Step 8	**exit** **Example:** `Device(config-wireless-policy)# exit`	Exits the policy configuration mode.
Step 9	**policy-map** *policy-map* **Example:** `Device(config)# policy-map policy-sample 1`	Creates a named object representing a set of policies that are to be applied to a set of traffic classes. Policy map names can contain alphabetic, hyphen, or underscore characters,

	Command or Action	Purpose
		are case sensitive, and can be up to 40 characters.
Step 10	**class** *class-map-name* **Example:** `Device(config-pmap)# class class-default`	Associates a class map with the policy map, and enters configuration mode for the specified system class.
Step 11	**police** *rate* **Example:** `Device(config-pmap-c)# police 500000`	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.

How to apply Per Client Bi-Directional Rate Limiting

Information About Per Client Bi-Directional Rate Limiting

The Per Client Bi-Directional Rate Limiting feature adds bi-directional rate limiting for each wireless clients on 802.11ac Wave 2 APs in a Flex local switching configuration. Earlier, the Wave 2 APs supported only per-flow rate limiting for a wireless client. When wireless client starts multiple streams of traffic, the client-based rate limiting does not work as expected. This limitation is addressed by this feature.

For instance, if the controller is configured with QoS policy and you expect each client to have a rate limiting cap of 1000 kbps. Due to per-flow rate limiting on the AP, if the wireless client starts a Youtube stream and FTP stream, each of them will be rate limited at 1000 Kbps, therefore the client will be 2000 Kbps rates. This is not desirable.

Use Cases

The following are the use cases supported by the Per Client Bi-Directional Rate Limiting feature:

Use Case -1

Configuring only default class map

If policy map is configured only with default class map and mapped only to QoS client policy, AP does a per client rate limit to the client connected to AP.

Use Case-2

Changing from per client rate limit to per flow rate limit

If policy map is configured with another different class map along with a default class map and mapped to QoS client policy, AP performs per flow rate limit to client. As policy map has different class map along with the default class map. The per client rate limit values are cleared, if the AP has previously configured per client rate limit.

If the policy map has more than one class map, then additional class map is configured along with the default class map. So, the rate limit is applied from per client to per flow. The per client rate limit value is deleted from the rate info token bucket.

Use Case-3

Changing from per flow rate limit to per client limit

If different class map is removed from policy map and policy map has only one default class map, AP performs a per client rate limit to client.

The following covers the high-level steps for Per Client Bi-Directional Rate Limiting feature:

1. Configure a policy map to WLAN through policy profile.
2. Map the QoS related policy map to WLAN.
3. Configure policy map with the default class map.
4. Configure different police rate value for class Default map.

Note If policy map has class Default with valid police rate value, AP applies that rate limit to the overall client data traffic flow.

5. Apply the policy map with class Default to QoS client policy in WLAN policy profile.

Prerequisites for Per Client Bi-Directional Rate Limiting

- This feature is exclusive to QoS client policy, that is, the policy profile must have only QoS Policy or policy target as client.
- If policy map has class default with valid police rate value, AP applies that rate limit value to the overall client data traffic flow.

Restrictions on Per Client Bi-Directional Rate Limiting

- If policy map has class map other than the class Default map, the per client rate limit does not work in AP.

Configuring Per Client Bi-Directional Rate Limiting (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the Policy Profile Name.

The **Edit Policy Profile** window is displayed.

Note The **Edit Policy Profile** window is displayed and configured in default class map only.

Step 3 Choose the **QOS And AVC** tab.

Step 4 In the **QoS Client Policy** settings, choose the policies from the **Egress** and **Ingress** drop-down lists.

Note You need to apply the default policy map to the QoS Client Policy.

Step 5 Click **Update & Apply to Device**.

Verifying Per Client Bi-Directional Rate Limiting

To verify whether per client is applied in AP, use the following command:

```
Device# show rate-limit client
Config:
            mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in
 nrt_burst_out nrt_burst_in
A0:D3:7A:12:6C:5E   0           0          0             0            0             0
   0             0            0
Statistics:
            name     up down
        Unshaped      0    0
  Client RT pass 697610 8200
 Client NRT pass      0    0
 Client RT drops      0    0
Client NRT drops      0   16
              9    180    0
Per client rate limit:
             mac vap rate_out rate_in            policy
A0:D3:7A:12:6C:5E   0       88      23 per_client_rate_2
```

Configuring BDRL Using AAA Override

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device (config)# wireless profile policy default-policy-profile`	Configures the WLAN policy profile and enters wireless policy configuration mode.
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa`	Configures AAA override to apply policies coming from the AAA server or ISE the Cisco Identify Services Engine (ISE) server. The following attributes are available in the RADIUS server: • Airespace-Data-Bandwidth-Average-Contract: 8001 • Airespace-Real-Time-Bandwidth-Average-Contract: 8002

	Command or Action	Purpose
		• Airespace-Data-Bandwidth-Burst-Contract: 8003 • Airespace-Real-Time-Bandwidth-Burst-Contract: 8004 • Airespace-Data-Bandwidth-Average-Contract-Upstream: 8005 • Airespace-Real-Time-Bandwidth-Average-Contract-Upstream: 8006 • Airespace-Data-Bandwidth-Burst-Contract-Upstream: 8007 • Airespace-Real-Time-Bandwidth-Burst-Contract-Upstream: 8008 **Note** 8001, 8002, 8003, 8004, 8005, 8006, 8007, and 8008 are the desired rate-limit values configured as an example.

Verifying Bi-Directional Rate-Limit

To verify the bi-directional rate limit, use the following command:

```
Device# show wireless client mac-address E8-8E-00-00-00-71 detailClient MAC Address :
e88e.0000.0071
Client MAC Type     : Universally Administered Address
Client IPv4 Address : 100.0.7.94
Client Username     : e88e00000071
AP MAC Address      : 0a0b.0c00.0200
AP Name             : AP6B8B4567-0002
AP slot             : 0
Client State        : Associated
Policy Profile      : dnas_qos_profile_policy
Flex Profile        : N/A
Wireless LAN Id     : 10
WLAN Profile Name   : QoS_wlan
Wireless LAN Network Name (SSID): QoS_wlan
BSSID : 0a0b.0c00.0200
Connected For       : 28 seconds
Protocol            : 802.11n - 2.4 GHz
Channel             : 1
Client IIF-ID       : 0xa0000034
Association Id      : 10
Authentication Algorithm : Open System
Idle state timeout  : N/A
Session Timeout     : 1800 sec (Remaining time: 1777 sec)
Session Warning Time : Timer not running
Input Policy Name    : None
Input Policy State   : None
Input Policy Source  : None
Output Policy Name   : None
Output Policy State  : None
```

```
Output Policy Source : None
WMM Support          : Enabled
U-APSD Support       : Disabled
Fastlane Support     : Disabled
Client Active State  : In-Active
Power Save           : OFF
Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
  QoS Average Data Rate Upstream             : 8005 (kbps)
  QoS Realtime Average Data Rate Upstream    : 8006 (kbps)
  QoS Burst Data Rate Upstream               : 8007 (kbps)
  QoS Realtime Burst Data Rate Upstream      : 8008 (kbps)
  QoS Average Data Rate Downstream           : 8001 (kbps)
  QoS Realtime Average Data Rate Downstream  : 8002 (kbps)
  QoS Burst Data Rate Downstream             : 80300 (kbps)
  QoS Realtime Burst Data Rate Downstream    : 8004 (kbps)
```

To verify the rate-limit details from the AP terminal, use the following command

```
Device# show rate-limit client
Config:
mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in nrt_burst_out
 nrt_burst_in
00:1C:F1:09:85:E7 0 8001 8002 8003 8004 8005 8006 8007 8008
Statistics:
name up down
Unshaped 0 0
Client RT pass 0 0
Client NRT pass 0 0
Client RT drops 0 0
Client NRT drops 0 0
Per client rate limit:
mac vap rate_out rate_in policy
```

How to Configure Wireless QoS

Configuring a Policy Map with Class Map (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **QoS**.

Step 2 Click **Add** to view the **Add QoS** window.

Step 3 In the text box next to the **Policy Name**, enter the name of the new policy map that is being added.

Step 4 Click **Add Class-Maps**.

Step 5 Configure **AVC** based policies or **User Defined** policies. To enable **AVC** based policies, and configure the following:

a) Choose either **Match Any** or **Match All**.

b) Choose the required **Mark Type**. If you choose **DSCP** or **User Priority**, you must specify the appropriate **Mark Value**.

c) Check the **Drop** check box to drop traffic from specific sources.

Note When **Drop** is enabled, the **Mark Type** and **Police(kbps)** options are disabled.

d) Based on the chosen **Match Type**, select the required protocols from the **Available Protocol(s)** list and move them to the **Selected Protocol(s)** list. These selected protocols are the ones from which traffic is dropped.
e) Click **Save**.

Note To add more Class Maps, repeat steps 4 and 5.

Step 6 To enable **User-Defined** QoS policy, and the configure the following:

a) Choose either **Match Any** or **Match All**.
b) Choose either **ACL** or **DSCP** as the **Match Type** from the drop-down list, and then specify the appropriate **Match Value**.
c) Choose the required **Mark Type** to associate with the mark label. If you choose *DSCP*, you must specify an appropriate **Mark Value**.
d) Check the **Drop** check box to drop traffic from specific sources.

Note When **Drop** is enabled, the **Mark Type** and **Police(kbps)** options are disabled.

e) Click **Save**.

Note To define actions for all the remaining traffic, in the Class Default, choose **Mark** and/or **Police(kbps)** accordingly.

Step 7 Click **Save & Apply to Device**.

Configuring a Class Map (CLI)

Follow the procedure given below to configure class maps for voice and video traffic:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**class-map** *class-map-name* **Example:** `Device(config)# class-map test`	Creates a class map.
Step 3	**match dscp** *dscp-value* **Example:** `Device(config-cmap)# match dscp 46`	Matches the DSCP value in the IPv4 and IPv6 packets. **Note** By default for the class map the value is match-all.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config-cmap)# end`	Exits the class map configuration and returns to the privileged EXEC mode.
Step 5	**show class-map** *class-map-name* **Example:** `Device# show class-map class_map_name`	Verifies the class map details.

Configuring Policy Profile to Apply QoS Policy (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, click the name of the policy profile.

Step 3 In the **Edit Policy Profile** window, click the **QoS and AVC** tab.

Step 4 Under **QoS SSID Policy**, choose the appropriate **Ingress** and **Egress** policies for WLANs.

Note The ingress policies can be differentiated from the egress policies by the suffix *-up*. For example, the Platinum ingress policy is named *platinum-up*.

Step 5 Under **QoS Client Policy**, choose the appropriate **Ingress** and **Egress** policies for clients.

Step 6 Click **Update & Apply to Device**.

Note Only custom policies are displayed under **QoS Client Policy**. AutoQoS policies are auto generated and not displayed for user selection.

Configuring Policy Profile to Apply QoS Policy (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy qostest`	Configures WLAN policy profile and enters the wireless policy configuration mode.

	Command or Action	Purpose
Step 3	**service-policy client** {**input** | **output**} *policy-name* **Example:** `Device(config-wireless-policy)# service-policy client input policy-map-client`	Applies the policy. The following options are available. • **input**—Assigns the client policy for ingress direction on the policy profile. • **output**—Assigns the client policy for egress direction on the policy profile.
Step 4	**service-policy** {**input** | **output**} *policy-name* **Example:** `Device(config-wireless-policy)# service-policy input policy-map-ssid`	Applies the policy to the BSSID. The following options are available. • **input**—Assigns the policy-map to all clients in WLAN. • **output**—Assigns the policy-map to all clients in WLAN.
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.

Applying Policy Profile to Policy Tag (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 On the **Manage Tags** page in the **Policy** tab, click **Add**.

Step 3 In the **Add Policy Tag** window that is displayed, enter a name and description for the policy tag.

Step 4 Map the required WLAN IDs and WLAN profiles with appropriate policy profiles.

Step 5 Click **Update & Apply to Device**.

Applying Policy Profile to Policy Tag (CLI)

Procedure

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

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config-policy-tag)# wireless tag policy qostag`	Configures policy tag and enters the policy tag configuration mode.
Step 3	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan test policy qostest`	Maps a policy profile to a WLAN profile.
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Saves the configuration and exits the configuration mode and returns to privileged EXEC mode.
Step 5	**show wireless tag policy summary** **Example:** `Device# show wireless tag policy summary`	Displays the configured policy tags. **Note** To view the detailed information of a policy tag, use the **show wireless tag policy detailed** *policy-tag-name* command.

Attaching Policy Tag to an AP

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures Cisco APs and enters the ap profile configuration mode.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag qostag`	Maps a Policy tag to the AP.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config-ap-tag)# end`	Saves the configuration and exits the configuration mode and returns to privileged EXEC mode.
Step 5	**show ap tag summary** **Example:** `Device# show ap tag summary`	Displays the ap details and tags associated to it.

SIP Call Admission Control (CAC)

Call Admission Control (CAC) is a concept that applies to voice traffic only—not data traffic. The CAC implementation requires the traffic specification (TSPEC) to be sent by the client to reserve the bandwidth. The SIP CAC feature enables CAC in order to support SIP calls. Most of the available SIP phones do not have TSPEC implemented. TSPEC is needed to invoke CAC and reserve bandwidth.

CAC regulates voice quality by limiting the number of calls that can be active at the same time on a particular link. It allows you to regulate the bandwidth consumed by active calls on the link, but does not guarantee a particular level of audio quality on the link. This configuration is used to track the bandwidth used for voice calls on a per radio basis and to protect current active calls. After the maximum bandwidth is reached (configurable value), new calls are not accepted on this radio. Also, this feature does not guarantee bandwidth reservation for future calls.

Note In cases where the client supports both SIP and TSPEC, then the bandwidth reservation with the help of TSPEC takes priority.

Restrictions and Limitations

- SIP CAC can be enabled only if SIP Call Snoop is enabled globally and in the Policy Profile of the controller .

Configuring SIP CAC (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the Policy Profile Name. The **Edit Policy Profile** window is displayed.

Step 3 Choose the **QOS And AVC** tab.

Step 4 In the **QoS SSID Policy** settings, choose the policies from the **Egress** and **Ingress**drop-down lists.

Step 5 In the **QoS Client Policy** settings, choose the policies from the **Egress** and **Ingress**drop-down lists.

Step 6 In the **SIP-CAC** settings, check the **Call Snooping** check box. You can check or uncheck the **Send Disassociate** and **Send 486 Busy** check boxes.

Step 7 Click **Update & Apply to Device**.

Configuring SIP CAC

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** **<policy-name>** **Example:** `Device(config)# wireless profile policy policy1`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**shutdown** **Example:** `Device(config)# shutdown`	Disables the wireless policy profile.
Step 4	**service-policy input** *policy-name* **Example:** `Device(config-wireless-policy)# service-policy input platinum`	Configures the policy profile with the Platinum metal QoS Policy. The upstream policy is specified with the keyword platinum-up as shown in the example. **Note** Upstream policies differ from downstream policies. The upstream policies have a suffix of -up. **Note** SSID policies should be configured with Platinum when Call Snoop is enabled
Step 5	**service-policy output** *policy-name* **Example:** `Device(config-wireless-policy)# service-policy output platinum-up`	Configures the policy profile with the Platinum metal QoS Policy. The upstream policy is specified with the keyword platinum-up as shown in the example.
Step 6	**service-policy client input** *client-policy-name* **Example:** `Device(config-wireless-policy)#`	Assigns the ingress policy map to all the clients.

	Command or Action	Purpose
	`service-policy client input client-policy-name`	
Step 7	**service-policy client output** *client-policy-name* **Example:** `Device(config-wireless-policy)# service-policy client output client-policy-name`	Assigns the egress policy map to all the clients.
Step 8	**call-snoop** **Example:** `Device(config-wireless-policy)# call-snoop`	Enables call snooping for WLAN.
Step 9	**[no] shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.
Step 10	**ap dot11** {**5ghz** | **24ghz**} **cac** {**voice** | **video**} **acm** **Example:** `Device(config-wireless-policy)# ap dot11 5ghz cac voice acm`	Enables the ACM static on the radio. When enabling SIP snooping, use the static CAC, not the load-based CAC.
Step 11	**ap dot11** {**5ghz** | **24ghz**} **cac voice sip** **Example:** `Device(config)# ap dot11 5ghz cac voice sip`	Configures SIP-based CAC.
Step 12	**Example:** `Device(config)# ap dot11 24ghz cac voice sip bandwidth <8-64> sample-interval <10-80>`	(Optional) Configures the bandwidth and the interval value. For example, enter bandwidth as <8-64>. 8 kbps for G729 and 64 kbps for G711. Enter the interval value as <10-80>, which means the packetization interval 10-80 ms (10, 20, 30, 40, 80 ms for G711 or G729 codec; default is 20). **Note** This configuration step can be done only through the CLI, and not from the WebUI.

	Command or Action	Purpose
Step 13	**end** **Example:** `Device(config)#end`	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-z to exit global configuration mode.

Verifying SIP CAC

To verify the SIP CAC feature, use the following command:

show ap cac voice

The following is a sample output.

```
Device # show ap cac voice
AP Name: AP5897.bdd0.61d4
Slot#   Radio       Calls   BW-Max  BW-Alloc    BW-InUse
-----------------------------------------------------------
0       802.11b/g   1       23437         765         3


AP Name: AP70DF.2FA2.39E0
Slot#   Radio       Calls   BW-Max  BW-Alloc    BW-InUse
-----------------------------------------------------------


AP Name: APA023.9F11.C6DC
Slot#   Radio       Calls   BW-Max  BW-Alloc    BW-InUse
-----------------------------------------------------------
0       802.11b/g   1       23437   765         3
```

SIP Voice Call Snooping

This feature enables access points to detect the establishment, termination, and failure of Session Initiation Protocol (SIP) calls and then report them to the controller. You can enable or disable SIP 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.

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 of any major call events, such as call establishment, termination, and failure.

Note This feature is supported in the central switching mode, supported on Wave 1 and Wave 2 APs, supported in the mesh AP bridge mode; but not supported on Fabric.

Note When you run SIP call with L3 roaming, the controllers should be in sync with the NTP server, or, its time should be the same.

Configuring SIP Voice Call Snooping (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the Policy Profile Name. The **Edit Policy Profile** window is displayed.

Step 3 Choose **QOS And AVC** tab.

Step 4 In the **QoS SSID Policy** settings, choose the policies from the **Egress** and **Ingress**drop-down lists.

Step 5 In the **QoS Client Policy** settings, choose the policies from the **Egress** and **Ingress**drop-down lists.

Step 6 In the **SIP-CAC** settings, check the **Call Snooping** check box. You can check or uncheck the **Send Disassociate** and **Send 486 Busy** check boxes.

Step 7 Click **Update & Apply to Device**.

Configuring SIP Voice Call Snooping

Before you begin

- To enable call-snoop, the BSSID platinum policy should be configured first.

Procedure

	Command or Action	Purpose
Step 1	**Configure Terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** <*policy-name*> **Example:** `Device(config)# wireless profile policy policy-name`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**shutdown** **Example:** `Device(config)# Shutdown`	Disables the wireless policy profile.
Step 4	**service-policy** {**input** | **output**} *policy-name*	Configure the policy profile with the Platinum metal QoS Policy. The upstream policy is

	Command or Action	Purpose

	Example:
	`Device(config-wireless-policy)# service-policy input platinum-up`
	`Device(Config-wireless-policy)# service-policy output platinum`
		specified with the keyword **platinum-up** as shown in the example.
		Note Upstream policies differ from downstream policies. The upstream policies have a suffix of -up.
		Note SSID policies should be configured with Platinum when Call Snoop is enabled.

Step 5	**service-policy client** {**input** | **output**} *client-policy-name*
	Example:
	`Device(config-wireless-policy)# service-policy client input voice-client`
	`Device(Config-wireless-policy)# service-policy client output voice-client`
		Configure the client policy profile.

Step 6	**call-snoop** **Example:** `Device(config-wireless-policy)# call-snoop`	Enables call snooping for WLAN.
Step 7	**[no] shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.
Step 8	**end** **Example:** `Device(config)#end`	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-z to exit global configuration mode.

Verifying SIP Voice Call Snooping

Use the following command to verify if the call-snoop command is enabled:

```
Device# sh wireless profile policy detailed <policy-name>
Classmap name for Reanchoring
  Reanchoring Classmap Name   : Not Configured
QOS per SSID
  Ingress Service Name        : platinum-up
  Egress Service Name         : platinum
QOS per Client
  Ingress Service Name        : voice-client
  Egress Service Name         : voice-client
```

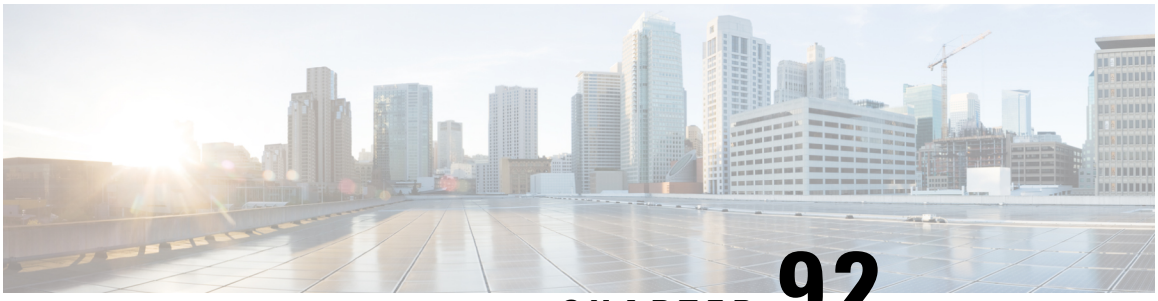
```
Umbrella information
  Ciso Umbrella Parameter Map : Not Configured
Autoqos Mode                  : None
Call Snooping                 : Enabled
Fabric Profile
  Profile Name                : Not Configured
Accounting list
```

To view the number of active calls, use the following command:

show wireless client calls active

The following is a sample output.

```
Device# show wireless client calls active
Number of Active TSPEC calls on 802.11a and 802.11b/g : 0
Number of Active SIP calls on 802.11a and 802.11b/g : 3
```



CHAPTER 92

Wireless Auto-QoS

•
• Information About Auto QoS, on page 871
• How to Configure Wireless AutoQoS, on page 872

Information About Auto QoS

Wireless Auto QoS automates deployment of wireless QoS features. It has a set of predefined profiles which can be further modified by the customer to prioritize different traffic flows. Auto-QoS matches traffic and assigns each matched packet to qos-groups. This allows the output policy map to put specific qos-groups into specific queues, including into the priority queue.

AutoQoS Policy Configuration

Table 36: AutoQoS Policy Configuration

Mode	Client Ingress	Client Egress	BSSID Ingress	BSSID Egress	Port Ingress	Port Egress	Radio
Voice	N/A	N/A	P3	P4	N/A	P7	ACM on
Guest	N/A	N/A	P5	P6	N/A	P7	
Fastlane	N/A	N/A	N/A	N/A	N/A	P7	edca-parameters fastlane
Enterprise-avc	N/A	N/A	P1	P2	N/A	P7	

P1	AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy
P2	AutoQos-4.0-wlan-ET-SSID-Output-Policy
P3	platinum-up
P4	platinum
P5	AutoQos-4.0-wlan-GT-SSID-Input-Policy

P6	AutoQos-4.0-wlan-GT-SSID-Output-Policy
P7	AutoQos-4.0-wlan-Port-Output-Policy

How to Configure Wireless AutoQoS

Configuring Wireless AutoQoS on Profile Policy

You can enable AutoQoS on a profile policy.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**wireless autoqos policy-profile** *policy-name* **mode { enterprise-avc | fastlane | guest | voice}** **Example:** `Device# wireless autoqos policy-profile test-profile mode voice`	Configures AutoQoS wireless policy. • **enterprise-avc**—Enables AutoQos Wireless Enterprise AVC Policy. • **fastlane**—Enable AutoQos Wireless Fastlane Policy. • **guest**—Enable AutoQos Wireless Guest Policy. • **voice**—Enable AutoQos Wireless Voice Policy. **Note** AutoQoS MIB attribute does not support full functionality with service policy. Service policy must be configured manually. Currently, there is only support for AutoQoS mode.

What to do next

Note After enabling AutoQoS, we recommend that you wait for a few seconds for the policy to install and then try and modify the AutoQoS policy maps if required; or retry if the modification is rejected.

Disabling Wireless AutoQoS

To globally disable Wireless AutoQoS:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**shutdown** **Example:** `Device# shutdown`	Shuts down the policy profile.
Step 3	**wireless autoqos disable** **Example:** `Device# wireless autoqos disable`	Globally disables wireless AutoQoS.
Step 4	**[no] shutdown** **Example:** `Device# no shutdown`	Enables the wireless policy profile. **Note** Disabling Auto QoS does not reset global radio configurations like CAC and EDCA parameters.

Rollback AutoQoS Configuration (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **QoS**.
Step 2 Click **Disable AutoQoS**.
Step 3 Click **Yes** to confirm.

Rollback AutoQoS Configuration

Before you begin

Note AutoQoS MIB attribute does not support the full functionality with service policy. Currently, there is only support for AutoQoS mode. Service policy must be configured manually.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device`**`enable`**	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**clear platform software autoqos config template { enterprise_avc | guest}** **Example:** `Device# clear platform software autoqos config template guest`	Resets AutoQoS configuration. • enterprise-avc—Resets AutoQoS Enterprise AVC Policy Template. • guest—Resets AutoQoS Guest Policy Template.

Clearing Wireless AutoQoS Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.
Step 2 Click on the **Policy Profile Name**.
Step 3 Go to **QOS and AVC** tab.
Step 4 From the **Auto Qos** drop-down list, choose **None**.
Step 5 Click **Update & Apply to Device**.

Clearing Wireless AutoQoS Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**shutdown** **Example:** `Device# shutdown`	Shuts down the policy profile.
Step 3	**wireless autoqos policy-profile** *policy-name* **mode clear** **Example:**	Clears the configured AutoQoS wireless policy.

	Command or Action	Purpose
	`Device# wireless autoqos policy-profile test-profile mode clear`	
Step 4	**[no] shutdown** **Example:** `no shutdown`	Enables the wireless policy profile.

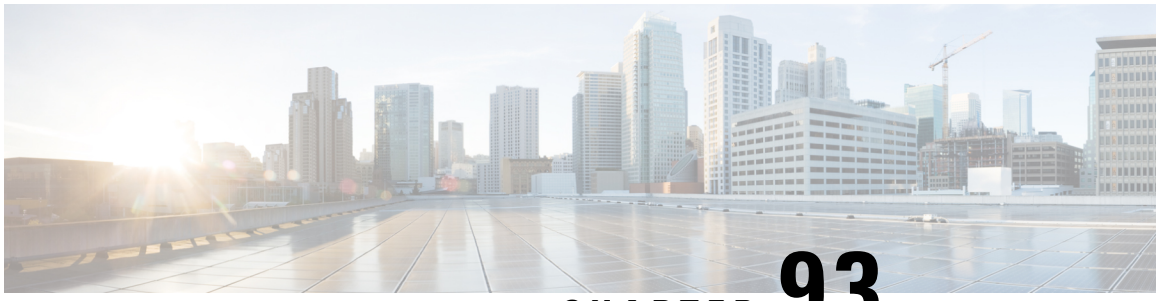
Viewing AutoQoS on policy profile

Before you begin

Autoqos is supported on the local mode and flex mode. Autoqos configures a set of policies and radio configurations depending on the template. It is possible to override the service-policy that is configured by autoqos. The latest configuration takes effect, with AAA override policy being of highest priority.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Deviceenable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**show wireless profile policy detailed** *policy-profile-name* **Example:** `Device# show wireless profile policy detailed testqos`	Shows policy-profile detailed parameters.



CHAPTER 93

Native Profiling

- Information About Native Profiling, on page 877
- Creating a Class Map (GUI), on page 878
- Creating a Class Map (CLI), on page 879
- Creating a Service Template (GUI), on page 881
- Creating a Service Template (CLI), on page 882
- Creating a Parameter Map, on page 883
- Creating a Policy Map (GUI), on page 883
- Creating a Policy Map (CLI), on page 884
- Configuring Native Profiling in Local Mode, on page 886
- Verifying Native Profile Configuration, on page 886

Information About Native Profiling

You can profile devices based on HTTP and DHCP to identify the end devices on the network. You can configure device-based policies and enforce these policies per user or per device policy on the network.

Policies allow profiling of mobile devices and basic onboarding of the profiled devices to a specific VLAN. They also assign ACL and QoS or configure session timeouts.

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 a wireless client joins an access point, certain QoS policies get enforced on the access point. One such feature is the native profiling for both upstream and downstream traffic at AP. The native profiling feature when clubbed with AAA override supports specific set of policies based on the time of day and day of week. The AAA override then applies these policies coming from a RADIUS server to the access point.

Let's consider a use case of time of the day in conjunction with user role. Usually, the user role is used as an extra matching criteria along with the time of day. You can club the time of day usage with any matching criteria to get the desired result. The matching will be performed when the client joins the controller .

You can configure policies as two separate components:

- Defining policy attributes as service templates that are specific to clients joining the network and applying policy match criteria
- Applying match criteria to the policy.

Note Before proceeding with the native profile configuration, ensure that HTTP Profiling and DHCP Profiling are enabled.

To configure Native Profiling, use one of the following procedures:

- Create a service template
- Create a class map

Note You can apply a service template using either a class map or parameter map.

- Create a parameter-map and associate the service template to parameter-map
  - Create a policy map
    1. If class-map has to be used: Associate the class-map to the policy-map and associate the service-template to the class-map.
    2. If parameter-map has to be used: Associate the parameter-map to the policy-map
  - Associate the policy-map to the policy profile.

Creating a Class Map (GUI)

Procedure

Step 1 Click **Configuration** > **Services** > **QoS**.
Step 2 In the **Qos – Policy** area, click **Add** to create a new QoS Policy or click the one you want to edit.
Step 3 Add **Add Class Map** and enter the details.
Step 4 Click **Save**.
Step 5 Click **Update and Apply to Device**.

Creating a Class Map (CLI)

Note Configuration of class maps via CLI offer more options and can be more granular than GUI.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**class-map type control subscriber match-any** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-any cls_user`	Specifies the class map type and name.
Step 3	**match username** *username* **Example:** `Device(config-filter-control-classmap)# match username ciscoise`	Specifies the class map attribute filter criteria.
Step 4	**class-map type control subscriber match-any** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-any cls_userrole`	Specifies the class map type and name.
Step 5	**match user-role** *user-role* **Example:** `Device(config-filter-control-classmap)# match user-role engineer`	Specifies the class map attribute filter criteria.
Step 6	**class-map type control subscriber match-any** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-any cls_oui`	Specifies the class map type and name.
Step 7	**match oui** *oui-address* **Example:** `Device(config-filter-control-classmap)# match oui 48.f8.b3`	Specifies the class map attribute filter criteria.

	Command or Action	Purpose
Step 8	**class-map type control subscriber match-any** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-any cls_mac`	Specifies the class map type and name.
Step 9	**match mac-address** *mac-address* **Example:** `Device(config-filter-control-classmap)# match mac-address 0040.96b9.4a0d`	Specifies the class map attribute filter criteria.
Step 10	**class-map type control subscriber match-any** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-any cls_devtype`	Specifies the class map type and name.
Step 11	**match device-type** *device-type* **Example:** `Device(config-filter-control-classmap)# match device-type windows`	Specifies the class map attribute filter criteria.
Step 12	**class-map type control subscriber match-all** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-all match_tod`	Specifies the class map type and name.
Step 13	**match join-time-of-day** *start-time end-time* **Example:** `Device(config-filter-control-classmap)# match join-time-of-day 10:30 12:30`	Specifies a match to the time of day. Here, join time is considered for matching. For example, if the match filter is set from 11:00 am to 2:00 pm, a device joining at 10:59 am is not considered, even if it acquires credentials after 11:00 am. Here, *start-time* and *end-time* specifies the 24-hour format. Use the **show class-map type control subscriber name** *name* command to verify the configuration. **Note** You should also disable AAA override for this command to work.
Step 14	**match day** *day-of-week*	Matches day of the week.

	Command or Action	Purpose
	Example: `Device(config-filter-control-classmap)# match day Monday`	Use the **show class-map type control subscriber name** *name* command to verify the configuration.
Step 15	**class-map type control subscriber match-all** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-all match_eap`	Specifies the class map type and filter as EAP.
Step 16	**match eap-type** *eap-type* **Example:** `Device(config-filter-control-classmap)# match eap-type peap`	Specifies the policy match with EAP type. Use the **show class-map type control subscriber name** *name* command to verify the configuration.
Step 17	**class-map type control subscriber match-all** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-all match_device`	Specifies the class map type and filter as device.
Step 18	**match device-type** *device-name* **Example:** `Device(config-filter-control-classmap)# match device-type android`	Matches name using the device type. Type a question mark (?) after the device type and select the device from the list. **Note** You should enable the device classifier for the device list to be populated.

Creating a Service Template (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Local Policy**.

Step 2 On the **Local Policy** page, **Service Template** tab, click **ADD**.

Step 3 In the **Create Service Template** window, enter the following parameters:

- **Service Template Name:** Enter a name for the template.
- **VLAN ID:** Enter the VLAN ID for the template. Valid range is between 1 and 4094.
- **Session Timeout (secs):** Sets the timeout duration for the template. Valid range is between 1 and 65535.
- **Access Control List:** Choose the Access Control List from the drop-down list.
- **Ingress QOS:** Choose the input QoS policy for the client from the drop-down list

- **Egress QOS:** Choose the output QoS policy for the client from the drop-down list.

Step 4 Click **Save & Apply to Device**.

Creating a Service Template (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**service-template** *service-template-name* **Example:** `Device(config)# service-template svc1`	Enters service template configuration mode.
Step 3	**vnid** *vnid* **Example:** `Device(config-service-template)# vnid test`	Specifies the VXLAN network identifier (VNID). Use the **show service-template** *service-template-name* command to verify the configuration.
Step 4	**access-group** *access-list-name* **Example:** `Device(config-service-template)# access-group acl-auto`	Specifies the access list to be applied.
Step 5	**vlan** *vlan-id* **Example:** `Device(config-service-template)# vlan 10`	Specifies VLAN ID. Valid range is from 1-4094.
Step 6	**absolute-timer** *timer* **Example:** `Device(config-service-template)# absolute-timer 1000`	Specifies session timeout value for a service template. Valid range is from 1-65535.
Step 7	**service-policy qos input** *qos-policy* **Example:** `Device(config-service-template)# service-policy qos input in_qos`	Configures an input QoS policy for the client.
Step 8	**service-policy qos output** *qos-policy* **Example:**	Configures an output QoS policy for the client.

	Command or Action	Purpose
	`Device(config-service-template)# service-policy qos output out_qos`	

Creating a Parameter Map

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type subscriber attribute-to-service** *parameter-map-name* **Example:** `Device(config)# parameter-map type subscriber attribute-to-service param`	Specifies the parameter map type and name.
Step 3	*map-index***map device-type eq***filter-name* **Example:** `Device(config-parameter-map-filter)# 1 map device-type eq "windows" mac-address eq 3c77.e602.2f91 username eq "cisco"`	Specifies the parameter map attribute filter criteria. Multiple filters are used in the example provided here.
Step 4	*map-index***service-template***service-template-name* **precedence** *precedence-num* **Example:** `Device(config-parameter-map-filter-submode)# 1 service-template svc1 precedence 150`	Specifies the service template and its precedence.

Creating a Policy Map (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Local Policy** > **Policy Map** tab..

Step 2 Enter a name for the Policy Map in the **Policy Map Name** text field.

Step 3 Click **Add**

Step 4 Choose the service template from the **Service Template** drop-down list.

Step 5 For the following parameters select the type of filter from the drop-down list and enter the required match criteria

- Device Type
- User Role
- User Name
- OUI
- MAC Address

Step 6 Click **Add Criteria**

Step 7 Click **Update & Apply to Device**.

Creating a Policy Map (CLI)

Before you begin

Before removing a policy map or parameter map, you should remove it from the target or shut down the WLAN profile or delete the session.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map type control subscriber** *policy-map-name* **Example:** `Device(config)# policy-map type control subscriber polmap5`	Specifies the policy map type.
Step 3	**event identity-update match-all** **Example:** `Device(config-event-control-policymap)# event identity-update match-all`	Specifies the match criteria to the policy map.
Step 4	You can apply a service template using either a class map or a parameter map, as shown here. • *class-num* **class** *class-map-name* **do-until-failure** • *action-index* **activate service-template** *service-template-name* • *action-index* **map attribute-to-service table** *parameter-map-name*	Configures the local profiling policy class map number and specifies how to perform the action or activates the service template or maps an identity-update attribute to an auto-configured template.

	Command or Action	Purpose

	Example:
	The following example shows how a class-map with a service-template has to be applied:
	`Device(config-class-control-policymap)# 10 class cls_mac do-until-failure`
	`Device(config-action-control-policymap)# 10 activate service-template svc1`
	Example:
	The following example shows how a parameter map has to be applied (service template is already associated with the parameter map 'param' while creating it):
	`Device(config-action-control-policymap)#1 map attribute-to-service table param`	

Step 5	**end** **Example:** `Device(config-action-control-policymap)# end`	Exits configuration mode.
Step 6	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 7	**wireless profile policy** *wlan-policy-profile-name* **Example:** `Device(config)# wireless profile policy wlan-policy-profilename`	Configures a wireless policy profile. **Caution** Do not configure aaa-override for native profiling under a named wireless profile policy. Native profiling is applied at a lower priority than AAA policy. If aaa-override is enabled, the AAA policies will override native profile policy.
Step 8	**description** *profile-policy-description* **Example:** `Device(config-wireless-policy)# description "default policy profile"`	Adds a description for the policy profile.
Step 9	**dhcp-tlv-caching** **Example:** `Device(config-wireless-policy)# dhcp-tlv-caching`	Configures DHCP TLV caching on a WLAN.
Step 10	**http-tlv-caching** **Example:**	Configures client HTTP TLV caching on a WLAN.

	Command or Action	Purpose
	`Device(config-wireless-policy)# http-tlv-caching`	
Step 11	**subscriber-policy-name** *policy-name* **Example:** `Device(config-wireless-policy)# subscriber-policy-name polmap5`	Configures the subscriber policy name.
Step 12	**vlan** *vlan-id* **Example:** `Device(config-wireless-policy)# vlan 1`	Configures a VLAN name or VLAN ID.
Step 13	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Saves the configuration.

Configuring Native Profiling in Local Mode

To configure native profiling in the local mode, you must follow the steps described in Creating a Policy Map (CLI), on page 884. In the policy profile, you must enable central switching as described in the step given below in order to configure native profiling.

Procedure

	Command or Action	Purpose
Step 1	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Enables central switching.

Verifying Native Profile Configuration

Use the following **show** commands to verify the native profile configuartion:

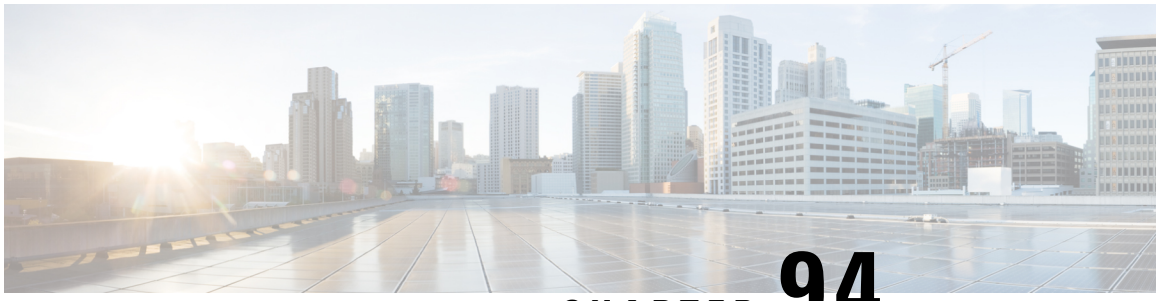
```
Device# show wireless client device summary

Active classified device summary
MAC Address       Device-type                      User-role
Protocol-map
-----------------------------------------------------------------------------------------------
1491.82b8.f94b    Microsoft-Workstation            sales
             9
1491.82bc.2fd5    Windows7-Workstation             sales
            41
```

```
Device# show wireless client device cache

Cached classified device info

MAC Address       Device-type                       User-role
Protocol-map
------------------------------------------------------------------------------------------------
2477.031b.aa18    Microsoft-Workstation
           9
30a8.db3b.a753    Un-Classified Device
           9
4400.1011.e8b5    Un-Classified Device
           9
980c.a569.7dd0    Un-Classified Device
```

```
Device# show wireless client mac-address 4c34.8845.e32c detail | s
Session Manager:
  Interface :
  IIF ID            : 0x90000002
  Device Type       : Microsoft-Workstation
  Protocol Map      : 0x000009
  Authorized        : TRUE
  Session timeout   : 1800
  Common Session ID: 783802090000000174BF2B5B9
  Acct Session ID   : 0
  Auth Method Status List
   Method : MAB
    SM State         : TERMINATE
    Authen Status    : Success
  Local Polices:
   Service Template : wlan_svc_C414.3CCA.0A51 (priority 254)
    Absolute-Timer   : 1800
  Server Polices:
  Resultant Policies:
  Filter-ID         : acl-auto
  Input QOS         : in_qos
  Output QOS        : out_qos
  Idle timeout      : 60 sec
  VLAN               : 10
  Absolute-Timer    : 1000
```

Use the following **show** command to verify the class map details for a class map name:

```
Device# show class-map type control subscriber name test
Class-map              Action                        Exec  Hit  Miss  Comp
---------               ------                       ----  ---  ----   ---
match-any test     match day Monday                    0     0    0     0
match-any test     match join-time-of-day 8:00 18:00   0     0    0     0
Key:
  "Exec" - The number of times this line was executed
  "Hit"  - The number of times this line evaluated to TRUE
  "Miss" - The number of times this line evaluated to FALSE
  "Comp" - The number of times this line completed the execution of its
       condition without a need to continue on to the end
```



CHAPTER 94

Air Time Fairness

- Information About Air Time Fairness, on page 889
- Restrictions on Cisco Air Time Fairness, on page 891
- Cisco Air Time Fairness (ATF) Use Cases, on page 892
- Configuring Cisco Air Time Fairness (ATF), on page 892
- Verifying Cisco ATF Configurations, on page 896
- Verifying Cisco ATF Statistics, on page 896

Information About Air Time Fairness

Cisco Air Time Fairness (ATF) allows network administrators to group devices of a defined category and enables some groups to receive traffic from the WLAN more frequently than the other groups. Therefore, some groups are entitled to more air time than the 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 in their environments with regards to the amount of air time per client group, the amount of traffic is also controlled.

To control air time on a percentage basis, the air time including both uplink and downlink transmissions of a client or 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 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 applies 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 can be applied to individual clients.

If the air time limit for an SSID (or client) is exceeded, the packets 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

Cisco Air Time Fairness can be enforced on clients that are associated with an SSID or WLAN. This ensures that all clients in an SSID or 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 or WLAN, thereby depriving Wi-Fi experience for other clients associated with the same SSID or 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 only to downstream traffic.
- Clients can be categorized into usage groups at the policy level.
- 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 APs:

- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points
- Cisco Aironet 1540 Series Access Points
- Cisco Aironet 1560 Series Access Points

Note Cisco ATF is supported on MESH, if APs support ATF. ATF is supported on FlexConnect mode and the Local mode.

Note Cisco Catalyst APs offer capabilities that are equivalent to ATF by leveraging the enhancements in the Wi-Fi 6 and 6E protocols. 802.11ax features such as OFDMA, bidirectional MU-MIMO, and BSS coloring, combined with the advanced QoS features in the Cisco Catalyst 9800 Series Wireless Controllers, help resolve scheduling and congestion problems, accommodate multiple users at the same time, and allocate bandwidth more efficiently.

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 or WLAN
    - per site group/tag
  - Report air time usage at periodic intervals
  - 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 the following:
    - A WLAN
    - All APs connected in a Cisco Catalyst 9800 Series Wireless Controller network
    - per site group/tag

Restrictions on Cisco Air Time Fairness

- Cisco ATF can be implemented only on data frames in the downstream direction.
- When ATF is configured in per-SSID mode, all the WLANs are disabled before you enter any ATF configuration commands. The WLANs are enabled after you enter all the ATF commands.

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 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 the service provider, for distribution of bandwidth privileges to the guests. 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 for 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.

Configuring Cisco Air Time Fairness (ATF)

Configuring Cisco Air Time Fairness

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 or per site group/tag.
4. Determine, if optimization must be enabled.
5. Periodically check the Cisco ATF statistics.

Creating a Cisco ATF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Air Time Fairness**.

Step 2 Click the **Profiles** tab and click the **Add** button, to create a new ATF policy.
The **Add ATF Policy** window is displayed.

Step 3 Specify a name, ID, and weight to the ATF policy. Weighted ratio is used instead of percentages so that the total can exceed 100. The minimum weight that you can set is 5. For example, if you configure the weight as 50, this means that the air time for this ATF profile is 50% when applied to an policy profile.

Step 4 Use the slider to enable or disable the **Client Sharing** feature. When you enable this option in the Web UI, the defaut ATF configuration is set to **Enforce** and not **Monitor**.

Step 5 Click **Apply to Device**.

Creating Cisco ATF Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile airtime-fairness** *atf-policy-name atf-profile-id* **Example:** `Device(config)# wireless profile airtime-fairness atf-policy-name 1`	Creates a new Cisco ATF policy. • *atf-policy-name*—Enters the ATF profile name. • *atf-profile-id*—Enters the ATF profile ID. Range is from 0 to 511.
Step 3	**weight** *policy-weight* **Example:** `Device(config-config-atf)# weight 5`	Adds a weight to the Cisco ATF policy. • *policy-weight*—Enters the policy weight. Range is from 5 to 100.
Step 4	**client-sharing** **Example:** `Device(config-config-atf)# client-sharing`	Enables or disables the client sharing for Cisco ATF policy.
Step 5	**end** **Example:** `Device(config-config-atf)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Attaching Cisco ATF Profile to a Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**. **Policy**.

Step 2 Click **Add**.
The **Add Policy Profile** window is displayed.

Step 3 Click the **Advanced** tab.

Step 4 Under the **Air Time Fairness Policies** section, select the required policy for 2.4 GHz and 5 GHz policies.

Step 5 Click **Apply to Device**.

Attaching Cisco ATF Profile to a Policy Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy profile-name`	Creates policy profile for the WLAN. • *profile-name* —Is the profile name of the policy profile.
Step 3	**dot11** {**24ghz** | **5ghz**} **airtime-fairness** *atf-policy-name* **Example:** `Device(config-wireless-policy)# dot11 24ghz airtime-fairness atf-policy-name`	Configures air time fairness policy for 2.4- or 5-GHz radio. • *atf-policy-name*—Is the name of the air time fairness policy. For more details on creating Cisco ATF policy, refer to the Creating Cisco ATF Profile (CLI). **Note** You can assign the same ATF policy to both 2.4-GHz and 5-GHz radios (or) have two different ATF policies as well.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Enabling ATF in the RF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF**.

Step 2 Click **Add**.
The **Add RF Profile** window is displayed.

Step 3 Click the **Advanced** tab.

Step 4 Under the **ATF Configuration** section, complete the following :

a) Use the slider to enable or disable the **Status**. The **Mode** field is displayed.

b) Click the **Monitor** mode or **Enforced** mode radio option. If you enable the **Enforced** mode, use the slider to enable or disable **Optimization**.

c) Use the slider to enable to disable **Bridge Client Access**. This is applicable for mesh mode APs. Bridge Client Access determines the percentage of the ATF policy weight that is allocated to clients connected to the mesh APs.

Step 5 Specify the **Airtime Allocation** value between 5 and 90.

Step 6 Click **Apply to Device**.

Enabling ATF in the RF Profile (CLI)

Cisco ATF must be enabled on 2.4 GHz or 5 GHz radios separately.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rf-profile** *rf-profile* **Example:** `Device(config)# ap dot11 24ghz rf-profile rfprof24_1`	Configures an RF profile for 2.4- or 5-GHz radio.
Step 3	**airtime-fairness mode** {**enforce-policy** | **monitor**} **Example:** `Device(config-rf-profile)# airtime-fairness mode enforce-policy`	Configures air time fairness in either of the modes: • Enforce-policy—This mode signifies that the ATF is operational. • Monitor—This mode gathers information about air time and reports air time usage.
Step 4	**airtime-fairness optimization**	Enables the air time fairness optimization.

	Command or Action	Purpose
	Example: `Device(config-rf-profile)# airtime-fairness optimization`	Optimization is effective when the current WLAN reaches the air time limit and the other available WLANs does not use air time to its full extent.
Step 5	**end** **Example:** `Device(config-rf-profile)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Cisco ATF Configurations

You can verify Cisco ATF configurations using the following commands:

Table 37: Commands for Verifying Cisco ATF Configurations

Commands	Description
show wireless profile airtime-fairness summary	Displays the summary of air time fairness profiles.
show wireless profile airtime-fairness mapping	Displays the ATF policy mapping with the wireless profiles.
show ap airtime-fairness summary	Displays the ATF configuration summary of all radios.
show ap dot11 24ghz airtime-fairness	Displays the ATF configuration for 2.4-GHz radio.
show ap dot11 5ghz airtime-fairness	Displays the ATF configuration for 5-GHz radio.
show ap name *ap-name* **airtime-fairness**	Displays the ATF configuration or statistics for an AP.
show ap name *ap-name* **dot11** {**24ghz** | **5ghz**} **airtime-fairness statistics summary**	Displays the ATF statistics of 2.4- or 5GHz radio.

Verifying Cisco ATF Statistics

Table 38: ATF Statistics per WLAN

Commands	Description
show ap name *ap-name* **dot11** {**24ghz** | **5ghz**} **airtime-fairness wlan** *wlan_name* **statistics**	Displays the ATF statistics related to a WLAN.

Table 39: ATF Statistics per ATF Policy

Commands	Description
show ap name *ap-name* **dot11** {**24ghz** | **5ghz**} **airtime-fairness policy** *policy-name* **statistics**	Displays the ATF statistics related to an ATF policy.

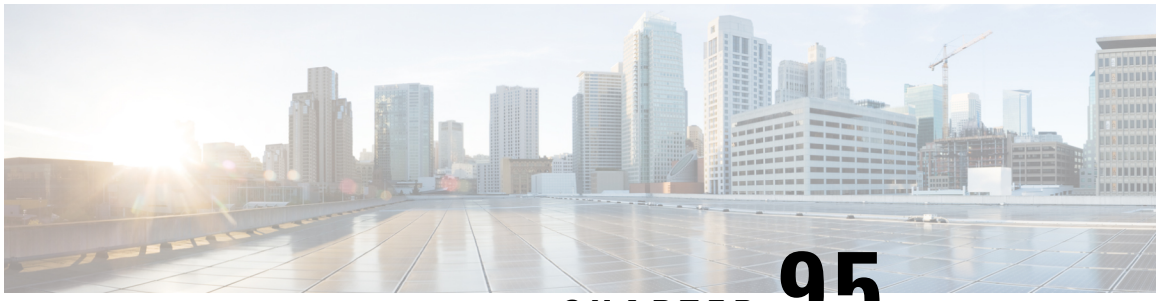
Table 40: ATF Statistics per Client

Commands	Description
show ap airtime-fairness statistics client *mac_address*	Displays the ATF statistics related to a client.

PART X

IPv6

- IPv6 Client IP Address Learning, on page 901
- IPv6 ACL, on page 919
- IPv6 Client Mobility, on page 931
- IPv6 Support on Flex and Mesh, on page 935



CHAPTER 95

IPv6 Client IP Address Learning

- Information About IPv6 Client Address Learning, on page 901
- Prerequisites for IPv6 Client Address Learning, on page 905
- Configuring RA Throttle Policy (CLI), on page 905
- Applying RA Throttle Policy on VLAN (GUI), on page 906
- Applying RA Throttle Policy on a VLAN (CLI), on page 907
- Configuring IPv6 Interface on a Switch (GUI), on page 907
- Configuring IPv6 on Interface (CLI), on page 908
- Configuring DHCP Pool on Switch (GUI), on page 909
- Configuring DHCP Pool on Switch (CLI), on page 909
- Configuring Stateless Auto Address Configuration Without DHCP on Switch (CLI), on page 910
- Configuring Stateless Auto Address Configuration With DHCP on Switch , on page 911
- Configuring Stateless Address Auto Configuration Without DHCP on Switch (CLI), on page 913
- Native IPv6, on page 914

Information About IPv6 Client Address Learning

Client Address Learning is configured on device to learn the IPv4 and IPv6 address of wireless client, and the client's transition state maintained by the device on association and timeout.

There are three ways for an IPv6 client to acquire IPv6 addresses:

- Stateless Address Auto-Configuration (SLAAC)
- Stateful DHCPv6
- Static Configuration

In all of these methods, the IPv6 client always sends a neighbor solicitation Duplicate Address Detection (DAD) request to ensure that there is no duplicate IP address on the network. The device snoops on the Neighbor Discovery Protocol (NDP) and DHCPv6 packets of the client to learn about its client IP addresses.

Address Assignment Using SLAAC

The most common method for IPv6 client address assignment is SLAAC, which provides simple plug-and-play connectivity, where clients self-assign an address based on the IPv6 prefix.

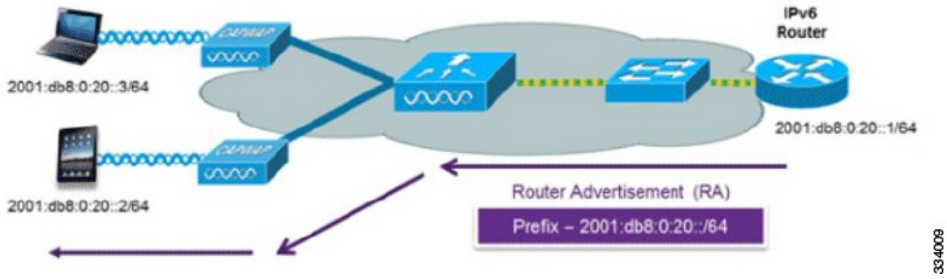
SLAAC is configured as follows:

- A host sends a Router Solicitation message.
- The host waits for a Router Advertisement message.
- The host take the first 64 bits of the IPv6 prefix from the Router Advertisement message and combines it with the 64 bit EUI-64 address (in the case of Ethernet, this is created from the MAC address) to create a global unicast message. The host also uses the source IP address, in the IP header, of the Router Advertisement message, as its default gateway.
- Duplicate Address Detection is performed by the IPv6 clients to ensure that random addresses that are picked do not collide with other clients.

Note The last 64 bits of the IPv6 address can be learned by using one of the following algorithms:

- EUI-64, which is based on the MAC address of the interface
- Private addresses that are randomly generated

Figure 21: Address Assignment Using SLAAC



The following Cisco IOS configuration commands from a Cisco-capable IPv6 router are used to enable SLAAC addressing and router advertisements:

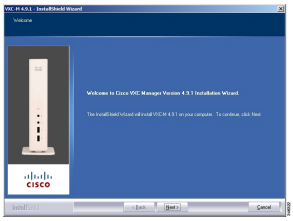
```
ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address FE80:DB8:0:20::1 linklocal
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end
```

Stateful DHCPv6 Address Assignment

The use of DHCPv6 is not required for IPv6 client connectivity if SLAAC is already deployed. There are two modes of operation for DHCPv6, that is, Stateless and Stateful.

The DHCPv6 Stateless mode is used to provide clients with additional network information that is not available in the router advertisement, but not an IPv6 address, becuase this is already provided by SLAAC. This information includes the DNS domain name, DNS servers, and other DHCP vendor-specific options.

Figure 22: Stateful DHCPv6 Address Assignment



The following interface configuration is for a Cisco IOS IPv6 router implementing stateless DHCPv6 with SLAAC enabled:

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
ipv6 address 2001:DB8:0:20::1/64
end
```

Router Solicitation

A Router Solicitation message is issued by a host controller to facilitate local routers to transmit a Router Advertisement from which the controller can obtain information about local routing, or perform stateless auto configuration. Router Advertisements are transmitted periodically and the host prompts with an immediate Router Advertisement using a Router Solicitation such as - when it boots or following a restart operation.

Router Advertisement

A Router Advertisement message is issued periodically by a router or in response to a Router Solicitation message from a host. The information contained in these messages is used by a host to perform stateless auto configuration and to modify its routing table.

Neighbor Discovery

IPv6 Neighbor Discovery is a set of messages and processes that determine relationships between neighboring nodes. Neighbor Discovery replaces the Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) Router Discovery, and ICMP Redirect used in IPv4.

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 tracks each IPv6 address and its associated MAC address. Clients are removed from the table according to neighbor-binding timers.

Neighbor Discovery Suppression

The IPv6 addresses of wireless clients are cached by a device once the wireless client is in RUN state. When the device receives an NS multicast, it looks into the IPv6 addresses cached. If the target address is known to the device and belongs to one of its wireless clients, the device converts the NS from multicast to unicast and forward it to the wireless client. If the target address is not present in the cache, then device interprets that the Multicast NS is for a wired entity and forward it towards the wired side and not to the wireless client.

The same behaviour is seen for ARP request in case of IPv4 address, where the device maintains IPv4 address of the wireless client in the cache.

When neither of the configuration is enabled, and when the device receives Non-DAD or DAD NS multicast looking for an IPv6 address, and if the target address is known to the device and belongs to one of its clients, the device will convert the multicast NS to unicast NS, with the destination MAC address, replaced with client's MAC and forward the unicast packet towards client.

When full-proxy is enabled, and when the device receives Non-DAD or DAD NS multicast, looking for an IPv6 address, and if the target address is known to the device and belongs to one of its clients, the device will reply with an NA message on behalf of the client.

You can use the **ipv6 nd proxy** command to enable or disable DAD or full proxy.

When the device receives an DAD-NS multicast looking for an IPv6 address, and if the target address is known to the device and belongs to one of its clients, the device will reply with an NA message on behalf of the client.

When the device receives Non-DAD NS multicast looking for an IPv6 address, and if the target address is known to the device and belongs to one of its clients, the device will convert the multicast NS to unicast NS, with the destination MAC address, replaced with client's MAC and forward the unicast packet towards client.

If the device does not have the IPv6 address of a wireless client, the device does not respond with NA; instead, it forwards the NS packet to the wired side. Reason for forwarding to Wired Side is due to the assumption that all wireless client IPv6 address and the its mapped MAC address should be available in the controller and if an IPv6 address required in the NS is not available, then that address is not a wireless client address, so forwarded to wired side.

Router Advertisement Guard

The RA Guard feature increases the security of the IPv6 network by dropping router advertisements coming from wireless clients. Without this feature, misconfigured or malicious IPv6 clients could announce themselves as a router for the network, often with a high priority, which could take precedence over legitimate IPv6 routers. By default, RA guard is always enabled on the controller.

- Port on which the frame is received
- IPv6 source address
- Prefix list
- Trusted or Untrusted ports for receiving the router advertisement guard messages
- Trusted/Untrusted IPv6 source addresses of the router advertisement sender
- Trusted/Untrusted Prefix list and Prefix ranges
- Router preference

Router Advertisement Throttling

RA throttling allows the controller to enforce limits to the RA packets headed toward the wireless network. By enabling RA throttling, routers that send multiple RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity. If a client sends an RS packet, an RA is sent back to the client. This RA is allowed through the controller and unicast to the client. This process ensures that the new clients or roaming clients are not affected by the RA throttling.

Prerequisites for IPv6 Client Address Learning

Before configuring IPv6 client address learning, configure the clients to support IPv6.

To enable wireless IPv6 client connectivity, the underlying wired network must support IPv6 routing and an address assignment mechanism, such as SLAAC or DHCPv6. The wireless LAN controller must have L2 adjacency to the IPv6 router.

Note The AP learns IPv6 client address based on source IP address even though Neighbor Advertisements can hold rest of the IPv6 addresses. AP won't look into the Neighbor Advertisements to learn the IPv6 address learnt by the client. This behavior is seen only on Apple clients and not on Microsoft Windows clients.

Configuring RA Throttle Policy (CLI)

Configure RA Throttle policy to allow the enforce the limits

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ipv6 nd ra-throttler policy ra-throttler1** **Example:** `Device(config)# ipv6 nd ra-throttler policy ra-throttler1`	Define the router advertisement (RA) throttler policy name and enter IPv6 RA throttle policy configuration mode.
Step 3	**throttleperiod 500** **Example:** `Device(config-nd-ra-throttle)# throttle-period 500`	Configures the throttle period in an IPv6 RA throttler policy. Throttle period is in seconds and it is the time while the controller will not forward RA to the wireless clients.

	Command or Action	Purpose
Step 4	**max-through** `10` **Example:** `Device(config-nd-ra-throttle)# max-through 15`	Limits multicast RAs per VLAN per throttle period.
Step 5	**allow-atleast** `5` **at-most** `10` **Example:** `Device(config-nd-ra-throttle)# allow at-least 5 at-most 10`	Limits the number of multicast RAs per device per throttle period in an RA throttler policy.

Applying RA Throttle Policy on VLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **RA Throttle Policy**.

Step 2 Click **Add**. The **Add RA Throttle Policy** dialog box appears.

Step 3 Enter a name for the policy in the **Name** field.

Step 4 Choose the desired option from the **Medium Type** drop-down list.

Step 5 Enter a value in the **Throttle Period** field. 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.

Step 6 Enter a value for the **Max Through** field, which is 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.

Step 7 Choose an **Interval Option**, which allows the device to act differently based on the RFC 3775 value set in IPv6 RA packets, from the following options:

- Ignore—Causes the RA throttle to treat packets with the interval option as a regular RA and subject to throttling if in effect.
- Passthrough—Allows any RA messages with the RFC 3775 interval option to go through without throttling.
- Throttle—Causes the RA packets with the interval option to always be subject to rate limiting.

Step 8 Enter the minimum number of RA packets per router that can be sent as multicast before throttling takes place in the **At Least Multicast RAs** field.

Step 9 Enter the maximum number of RA packets per router that can be sent as multicast before throttling takes place in the **At Most Multicast RAs** field. The **No Limit** option allows an unlimited number of RA packets through the router.

Step 10 Click the **Add & Apply to Device** button.

Applying RA Throttle Policy on a VLAN (CLI)

Applying the RA Throttle policy on a VLAN. 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.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**vlan configuration 1** **Example:** `Device(config)# vlan configuration 1`	Configures a VLAN or a collection of VLANs and enters VLAN configuration mode.
Step 3	**ipv6 nd ra throttler attach-policy ra-throttler1** **Example:** `Device(config-vlan)# ipv6 nd ra throttler attach-policy ra-throttler1`	Attaches an IPv6 RA throttler policy to a VLAN or a collection of VLANs.

Configuring IPv6 Interface on a Switch (GUI)

Procedure

Step 1 Choose **Configuration** > **Layer2** > **VLAN** > **SVI**.

Step 2 Click **Add**.

Step 3 Enter **VLAN Number**, **Description** and **MTU (Bytes)**.

Step 4 Enable or disable the **Admin Status** toggle button.

Step 5 In **IP Options**, check the **IPv6** check box.

Step 6 Choose the type of **Static** address from the drop-down list and enter the Static Address.

Step 7 Check or uncheck the **DHCP**, **Autoconfig** and **Act as an IPv6 DHCP client** check boxes.

If you check the **DHCP** check box, the **Rapid Commit** check box is displayed. Check or uncheck the **Rapid Commit** check box.

Step 8 Click **Apply to Device**.

Configuring IPv6 on Interface (CLI)

Follow the procedure given below to configure IPv6 on an interface:

Before you begin

Enable IPv6 on the client and IPv6 support on the wired infrastructure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 10`	Creates an interface and enters interface configuration mode.

Step 4	**ip address fe80::1 link-local**
	Example:
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		Configures IPv6 address on the GigabitEthernet interface using the link-local option.

Step 5	**ipv6 enable** **Example:** `Device(config)# ipv6 enable`	(Optional) Enables IPv6 on the GigabitEthernet interface.
Step 6	**end** **Example:** `Device(config)# end`	Exits interface mode.

Configuring DHCP Pool on Switch (GUI)

Procedure

Step 1 Choose **Administration** > **DHCP**.

Step 2 Click the **Add** button. The **Create DHCP Pool** dialog box appears.

Step 3 Enter a pool name in the **DHCP Pool Name** field. The name must not be greater than 236 characters in length.

Step 4 Choose either **IPv4** or **IPv6** from the **IP Type** drop-down list.

Step 5 Enter an IP address in the **Network** field.

Step 6 Choose any one of the available subnet masks from the **Subnet Mask** drop-down list.

Step 7 Enter an IP address in the **Starting ip** field.

Step 8 Enter an IP address in the **Ending ip** field.

Step 9 Optional, set the status of the **Reserved Only** field to **Enabled** if you wish to reserve the DHCP pool.

Step 10 Choose the desired option from the **Lease** drop-down list.

Step 11 Selecting the **User Defined** option from the **Lease** drop-down list enables the **(0-365 days)**, **(0-23 hours)**, and **(0-59 minutes)** fields. Enter appropriate values.

Step 12 Click the **Save & Apply to Device** button.

Step 13 For IPv6, Enter the **DNS Server, DNS Domain Name, and Ipv6 Address Allocation**.

Configuring DHCP Pool on Switch (CLI)

Follow the procedure given below to configure DHCP Pool on an interface:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *vlan-id* **Example:** `Device(config)# ipv6 dhcp pool 21`	Enters the configuration mode and configures the IPv6 DHCP pool on the Vlan.

	Command or Action	Purpose
Step 4	**address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10** **Example:** `Device(config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10`	Enters the configuration-dhcp mode and configures the address pool and its lifetime on a Vlan.
Step 5	**dns-server 2001:100:0:1::1** **Example:** `Device(config-dhcpv6)# dns-server 2001:20:21::1`	Configures the DNS servers for the DHCP pool.
Step 6	**domain-name example.com** **Example:** `Device(config-dhcpv6)# domain-name example.com`	Configures the domain name to complete unqualified host names.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Stateless Auto Address Configuration Without DHCP on Switch (CLI)

Follow the procedure given below to configure stateless auto address configuration without DHCP:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan 1** **Example:**	Creates an interface and enters interface configuration mode.

	Command or Action	Purpose
	`Device(config)# interface vlan 1`	

Step 4	**ip address fe80::1 link-local**
	Example:
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		Configures IPv6 address on the GigabitEthernet interface using the link-local option.

Step 5	**ipv6 enable** **Example:** `Device(config)# ipv6 enable`	(Optional) Enables IPv6 on the GigabitEthernet interface.

Step 6	**no ipv6 nd managed-config-flag**
	Example:
	`Device(config)# interface vlan 1`
	`Device(config-if)# no ipv6 nd managed-config-flag`
		Ensures the attached hosts do not use stateful autoconfiguration to obtain addresses.

Step 7	**no ipv6 nd other-config-flag** **Example:** `Device(config-if)# no ipv6 nd other-config-flag`	Ensures the attached hosts do not use stateful autoconfiguration to obtain non-address options from DHCP (domain etc).
Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Stateless Auto Address Configuration With DHCP on Switch

Follow the procedure given below to configure stateless auto address configuration with DHCP:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan 1** **Example:** `Device(config)# interface vlan 1`	Creates an interface and enters interface configuration mode.

Step 4	**ip address fe80::1 link-local**
	Example:
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		Configures IPv6 address on the GigabitEthernet interface using the link-local option.

Step 5	**ipv6 enable** **Example:** `Device(config)# ipv6 enable`	(Optional) Enables IPv6 on the GigabitEthernet interface.
Step 6	ipv6 nd prefix ipaddress **Example:** `ipv6 nd prefix 2001:9:3:54::/64 no-advertise`	Specifies a subnet prefix.

Step 7	**no ipv6 nd managed-config-flag**
	Example:
	`Device(config)# interface vlan 1`
	`Device(config-if)# no ipv6 nd managed-config-flag`
		Ensures the attached hosts do not use stateful autoconfiguration to obtain addresses.

Step 8	**ipv6 nd other-config-flag** **Example:** `Device(config-if)# no ipv6 nd other-config-flag`	Ensures the attached hosts do not use stateful autoconfiguration to obtain non-address options from DHCP (domain etc).
Step 9	ipv6 dhcp server servername **Example:** `ipv6 dhcp server VLAN54`	Displays the configuration parameters.
Step 10	**end** **Example:**	Exits interface mode.

	Command or Action	Purpose
	`Device(config)# end`	

Configuring Stateless Address Auto Configuration Without DHCP on Switch (CLI)

Follow the procedure given below to configure stateless auto address configuration without DHCP:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan 1** **Example:** `Device(config)# interface vlan 1`	Creates an interface and enters interface configuration mode.

Step 4	**ip address fe80::1 link-local**
	Example:
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		Configures IPv6 address on the GigabitEthernet interface using the link-local option.

Step 5	**ipv6 enable** **Example:** `Device(config)# ipv6 enable`	(Optional) Enables IPv6 on the GigabitEthernet interface.

Step 6	**no ipv6 nd managed-config-flag**
	Example:
	`Device(config)# interface vlan 1`
	`Device(config-if)# no ipv6 nd managed-config-flag`
		Ensures the attached hosts do not use stateful autoconfiguration to obtain addresses.

	Command or Action	Purpose
Step 7	**no ipv6 nd other-config-flag** **Example:** `Device(config-if)# no ipv6 nd other-config-flag`	Ensures the attached hosts do not use stateful autoconfiguration to obtain non-address options from DHCP (domain etc).
Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Native IPv6

Information About IPv6

IPv6 is a packet-based protocol used to exchange data, voice, and video traffic over digital networks. IPv6 is based on IP, but with a much larger address space, and improvements such as a simplified main header and extension headers. The architecture of IPv6 has been designed to allow existing IPv4 users to transition easily to IPv6 while continuing to use services such as end-to-end security, quality of service (QoS), and globally unique addresses. The larger IPv6 address space allows networks to scale and provide global reachability.

Note The features and functions that work on IPv4 networks with IPv4 addresses also work on IPv6 networks with IPv6 addresses.

General Guidelines

- The Wireless Management interface should have only one static IPv6 address.
- Router advertisement should be suppressed on the wireless management interface and client VLANs (if IPv6 is configured on the client VLAN).
- Preferred mode is part of an AP join profile. When you configure the preferred mode as IPv6, an AP attempts to join over IPv6 first. If it fails, the AP falls back to IPv4.
- You should use MAC addresses for RA tracing of APs and clients.
- APs can join IPv6 controllers only with an IPv6 static address. If you have a controller with auto configurations and multiple IPv6 addresses, APs cannot join the IPv6 controllers.

Unsupported Features

- UDP Lite is not supported.
- AP sniffer over IPv6 is not supported.
- IPv6 is not supported for the HA port interface.
- Auto RF grouping over IPv6 is not supported. Only static RF grouping is supported.

Configuring IPv6 Addressing

Follow the procedure given below to configure IPv6 addressing:

Note All the features and functions that work on IPv4 networks with IPv4 addresses will work on IPv6 networks with IPv6 addresses too.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ipv6 unicast-routing** **Example:** `Device(config)# ipv6 unicast-routing`	Configures IPv6 for unicasting.
Step 3	**interface vlan 1** **Example:** `Device(config)# interface vlan 1`	Creates an interface and enters interface configuration mode.
Step 4	**ipv6 address** *ipv6-address* **Example:** `Device(config-if)# ipv6 address FD09:9:2:49::53/64`	Specifies a global IPv6 address.
Step 5	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 on the interface.
Step 6	**ipv6 nd ra suppress all** **Example:** `Device(config-if)# ipv6 nd ra suppress all`	Suppresses IPv6 router advertisement transmissions on the interface.
Step 7	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 8	**wireless management interface gigabitEthernet** *gigabitEthernet-interface-vlan 64* **Example:**	Configures the ports that are connected to the supported APs with the wireless management interface.

	Command or Action	Purpose
	`Device(config)# wireless management interface gigabitEthernet vlan 64`	
Step 9	**ipv6 route** *ipv6-address* **Example:** `Device(config)# ipv6 route ::/0 FD09:9:2:49::1`	Specifies IPv6 static routes.

Creating an AP Join Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join Profile** window, click the **General** tab and click **Add**.

Step 3 In the **Name** field enter, a name for the AP join profile.

Step 4 (Optional) Enter a description for the AP join profile.

Step 5 Choose **CAPWAP** > **Advanced**.

Step 6 Under the **Advanced** tab, from the **Preferred Mode** drop-down list, choose **IPv6**. This sets the preferred mode of APs as IPv6.

Step 7 Click **Save & Apply to Device**.

Creating an AP Join Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**description** *ap-profile-name* **Example:** `Device(config-ap-profile)# description "xyz ap profile"`	Adds a description for the AP profile.

	Command or Action	Purpose
Step 4	**preferred-mode ipv6** **Example:** `Device(config-ap-profile)# preferred-mode ipv6`	Sets the preferred mode of APs as IPv6.

Configuring the Primary and Backup Controller (GUI)

Before you begin

Ensure that you have configured an AP join profile prior to configuring the primary and backup controller s.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join Profile** window, click the AP join profile name.

Step 3 In the **Edit AP Join Profile** window, click the **CAPWAP** tab.

Step 4 In the **High Availability** tab, under **Backup Controller Configuration**, check the **Enable Fallback** check box.

Step 5 Enter the primary and secondary controller names and IP addresses.

Step 6 Click **Update & Apply to Device**.

Configuring Primary and Backup Controller (CLI)

Follow the procedure given below to configure the primary and secondary controllers for a selected AP:

Procedure

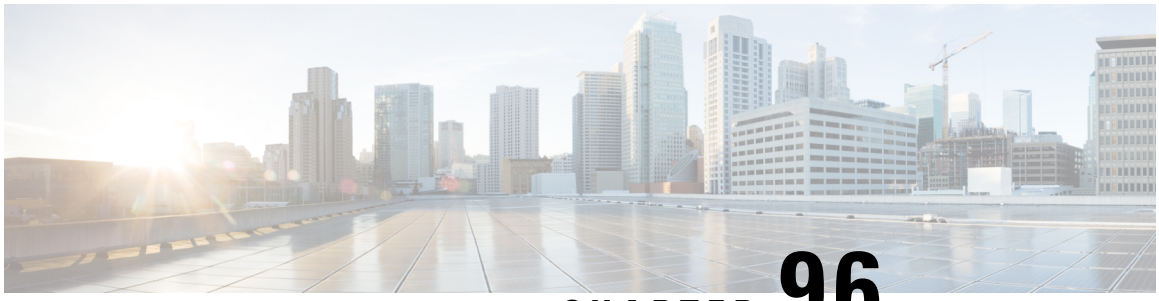
	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile yy-ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**capwap backup primary** *primary-controller-name primary-controller-ip* **Example:**	Configures AP CAPWAP parameters with the primary backup controller's name.

	Command or Action	Purpose
	`Device(config)# capwap backup primary WLAN-Controller-A 2001:DB8:1::1`	**Note** You need to enable fast heartbeat for **capwap backup primary** and **capwap backup secondary** to work. AP disconnection may occur if the link between the controller and AP is not reliable and fast heartbeat is enabled.
Step 4	**ap capwap backup secondary** *secondary-controller-name secondary-controller-ip* **Example:** `Device(config)# capwap backup secondary WLAN-Controller-B 2001:DB8:1::1`	Configures AP CAPWAP parameters with the secondary backup controller's name.
Step 5	**syslog host** *ipaddress* **Example:** `Device(config)# syslog host 2001:DB8:1::1`	Configures the system logging settings for the APs.
Step 6	**tftp-downgrade** *tftp-server-ip imagename* **Example:** `Device(config)# tftp-downgrade 2001:DB8:1::1 testimage`	Initiates AP image downgrade from a TFTP server for all the APs.

Verifying IPv6 Configuration

Use the following **show** command to verify the IPv6 configuration:

```
Device# show wireless interface summary

Wireless Interface Summary


Interface Name Interface Type VLAN ID IP Address      IP Netmask     MAC Address
-----------------------------------------------------------------------------------------
Vlan49         Management     49      0.0.0.0       255.255.255.0    001e.f64c.1eff
                                      fd09:9:2:49::54/64
```



CHAPTER 96

IPv6 ACL

- Information About IPv6 ACL, on page 919
- Prerequisites for Configuring IPv6 ACL, on page 920
- Restrictions for Configuring IPv6 ACL, on page 920
- Configuring IPv6 ACLs , on page 920
- How To Configure an IPv6 ACL, on page 921
- Verifying IPv6 ACL, on page 926
- Configuration Examples for IPv6 ACL, on page 927

Information About IPv6 ACL

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 are configured on the device and 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 can also create a preauthentication ACL for web authentication. Such an ACL is used to allow certain types of traffic before authentication is complete.

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.

Understanding IPv6 ACLs

Types of ACL

Per User IPv6 ACL

For the per-user ACL, the full access control entries (ACE) as the text strings are configured on the RADIUS server.

The ACE is not configured on the Cisco 9800 controller. The ACE is sent to the device in the `ACCESS-Accept` attribute and applies it directly for the client. When a wireless client roams into an foreign device, the ACEs are sent to the foreign device as an AAA attribute in the mobility Handoff message. Output direction, using per-user ACL is not supported.

Filter ID IPv6 ACL

For the filter-Id ACL, the full ACEs and the `acl name(filter-id)` is configured on the Cisco 9800 controller and only the `filter-id` is configured on the RADIUS Server.

The `filter-id` is sent to the device in the ACCESS-Accept attribute, and the device looks up the filter-id for the ACEs, and then applies the ACEs to the client. When the client L2 roams to the foreign device, only the filter-id is sent to the foreign device in the mobility Handoff message. Output filtered ACL, using per-user ACL is not supported. The foreign device has to configure the filter-id and ACEs beforehand.

Prerequisites for Configuring IPv6 ACL

You can filter IP Version 6 (IPv6) traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similarly to the way that you create and apply IP Version 4 (IPv4) named ACLs. You can also create and apply input router ACLs to filter Layer 3 management traffic when the switch is running the Network Essentials license.

Restrictions for Configuring IPv6 ACL

With IPv4, you can configure standard and extended numbered IP ACLs, named IP ACLs, and MAC ACLs. IPv6 supports only named ACLs. The IPv6 ACL does not support Flex connect mode.

The device supports most of the Cisco IOS-supported IPv6 ACLs with some exceptions:

- The device does not support matching on these keywords: **flowlabel**, **routing header**, and **undetermined-transport**.
- The device does not support reflexive ACLs (the **reflect** keyword).
- The device does not apply MAC-based ACLs on IPv6 frames.
- When configuring an ACL, there is no restriction on keywords entered in the ACL, regardless of whether or not they are supported on the platform. When you apply the ACL to an interface that requires hardware forwarding (physical ports or SVIs), the device checks to determine whether or not the ACL can be supported on the interface. If not, attaching the ACL is rejected.
- If an ACL is applied to an interface and you attempt to add an access control entry (ACE) with an unsupported keyword, the device does not allow the ACE to be added to the ACL that is currently attached to the interface

Configuring IPv6 ACLs

Follow the procedure given below to filter IPv6 traffic:

1. Create an IPv6 ACL, and enter IPv6 access list configuration mode.

2. Configure the IPv6 ACL to block (deny) or pass (permit) traffic.
3. Apply the IPv6 ACL to the interface where the traffic needs to be filtered.
4. Apply the IPv6 ACL to an interface. For router ACLs, you must also configure an IPv6 address on the Layer 3 interface to which the ACL is applied.

Default IPv6 ACL Configuration

There are no IPv6 ACLs configured or applied.

Interaction with Other Features and Switches

- If a bridged frame is to be dropped due to a port ACL, the frame is not bridged.
- You can create both IPv4 and IPv6 ACLs on a switch or switch stack, and you can apply both IPv4 and IPv6 ACLs to the same interface. Each ACL must have a unique name; an error message appears if you try to use a name that is already configured.

  You use different commands to create IPv4 and IPv6 ACLs and to attach IPv4 or IPv6 ACLs to the same Layer 2 or Layer 3 interface. If you use the wrong command to attach an ACL (for example, an IPv4 command to attach an IPv6 ACL), you receive an error message.

- You cannot use MAC ACLs to filter IPv6 frames. MAC ACLs can only filter non-IP frames.
- If the hardware memory is full, for any additional configured ACLs, packets are processed to the CPU, and the ACLs are applied in software. When the hardware is full a message is printed to the console indicating the ACL has been unloaded and the packets will be processed in software.

Note Only packets of the same type as the ACL that could not be added (ipv4, ipv6, MAC) will be processed in software.

- If the TCAM is full, for any additional configured ACLs, packets are forwarded to the CPU, and the ACLs are applied in software.

How To Configure an IPv6 ACL

Creating an IPv6 ACL (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **ACL**.

Step 2 Click **Add**.

Step 3 In the **Add ACL Setup** dialog box, enter the following parameters.

- **ACL Name:** Enter the name for the ACL
- **ACL Type:** IPv6
- **Sequence:** The valid range is between 100 and 199 or 2000 and 26991
- **Action:** Choose **Permit** or **Deny** the packet flow from the drop-down list.
- **Source Type:** Choose **any**, **Host** or **Network** from which the packet is sent.
- **Destination Type:** Choose **any**, **Host** or **Network** to which the packet is sent.
- **Protocol:** Choose a protocol from the drop-down list.
- **Log:** Enable or disable logging.
- **DSCP:** Enter to match packets with the DSCP value

Step 4 Click **Add**.

Step 5 Add the rest of the rules and click **Apply to Device**.

Creating an IPv6 ACL

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 access-list** *acl_name* **Example:** `Device# ipv6 access-list access-list-name`	Use a name to define an IPv6 access list and enter IPv6 access-list configuration mode.
Step 4	**{deny|permit} protocol** **Example:** `{deny | permit} protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length`	Enter deny or permit to specify whether to deny or permit the packet if conditions are matched. These are the conditions: • For protocol, enter the name or number of an Internet protocol: ahp, esp, icmp, ipv6, pcp, stcp, tcp, or udp, or an integer

	Command or Action	Purpose
	`| any |host destination-ipv6-address} [operator [port-number]][dscp value] [fragments][log] [log-input] [routing][sequence value] [time-range name]`	in the range 0 to 255 representing an IPv6 protocol number. • The source-ipv6-prefix/prefix-length or destination-ipv6-prefix/ prefix-length is the source or destination IPv6 network or class of networks for which to set deny or permit conditions, specified in hexadecimal and using 16-bit values between colons (see RFC 2373). • Enter any as an abbreviation for the IPv6 prefix ::/0. • For host source-ipv6-address or destination-ipv6-address, enter the source or destination IPv6 host address for which to set deny or permit conditions, specified in hexadecimal using 16-bit values between colons. • (Optional) For operator, specify an operand that compares the source or destination ports of the specified protocol. Operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range. If the operator follows the source-ipv6-prefix/prefix-length argument, it must match the source port. If the operator follows the destination-ipv6-prefix/prefix-length argument, it must match the destination port. • (Optional) The port-number is a decimal number from 0 to 65535 or the name of a TCP or UDP port. You can use TCP port names only when filtering TCP. You can use UDP port names only when filtering UDP. • (Optional) Enter dscp value to match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63. • (Optional) For packet fragmentation, enter fragments to check noninitial

	Command or Action	Purpose
		fragments. This keyword is visible only if the protocol is ipv6. • (Optional) Enter log to cause an logging message to be sent to the console about the packet that matches the entry. Enter log-input to include the input interface in the log entry. Logging is supported only for router ACLs. • (Optional) Enter routing to specify that IPv6 packets be routed. • (Optional) Enter sequence value to specify the sequence number for the access list statement. The acceptable range is from 1 to 4294967295 • (Optional) Enter time-range name to specify the time range that applies to the deny or permit statement.
Step 5	**{deny|permit} tcp** **Example:** `{deny | permit} tcp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |hostdestination-ipv6-address} [operator [port-number]][ack] [dscp value][established] [fin] [log][log-input] [neq {port |protocol}] [psh] [range{port | protocol}] [rst][routing] [sequence value] [syn] [time-range name][urg]`	(Optional) Define a TCP access list and the access conditions. Enter tcp for Transmission Control Protocol. The parameters are the same as those described in Step 3, with these additional optional parameters: • ack—Acknowledgment bit set. • established—An established connection. A match occurs if the TCP datagram has the ACK or RST bits set. • fin—Finished bit set; no more data from sender. • neq {port | protocol}—Matches only packets that are not on a given port number. • psh—Push function bit set. • range {port | protocol}—Matches only packets in the port number range. • rst—Reset bit set. • syn—Synchronize bit set. • urg—Urgent pointer bit set.

	Command or Action	Purpose
Step 6	**{deny|permit} udp** **Example:** `{deny | permit} udp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][dscp value] [log][log-input] [neq {port |protocol}] [range {port |protocol}] [routing][sequence value][time-range name]`	(Optional) Define a UDP access list and the access conditions. Enter udp for the User Datagram Protocol. The UDP parameters are the same as those described for TCP, except that the operator [port]] port number or name must be a UDP port number or name, and the established parameter is not valid for UDP.
Step 7	**{deny|permit} icmp** **Example:** `{deny | permit} icmp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][icmp-type [icmp-code] |icmp-message] [dscpvalue] [log] [log-input] [routing] [sequence value][time-range name]`	(Optional) Define an ICMP access list and the access conditions. Enter icmp for Internet Control Message Protocol. The ICMP parameters are the same as those described for most IP protocols in Step 3a, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings: • icmp-type—Enter to filter by ICMP message type, a number from 0 to 255. • icmp-code—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255. • icmp-message—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name. To see a list of ICMP message type names and code names, use the ? key or see command reference for this release.
Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 9	**show ipv6 access-list** **Example:** `show ipv6 access-list`	Verify the access list configuration.
Step 10	**copy running-config startup-config** **Example:** `copy running-config startup-config`	(Optional) Save your entries in the configuration file.

Creating WLAN IPv6 ACL (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**.

Step 4 Choose **Security** > **Layer3** tab, click **Show Advanced Settings** and under the **Preauthenticated ACL** settings, choose the ACL from the **IPv6** drop-down list.

Step 5 Click **Apply to Device**.

Creating WLAN IPv6 ACL

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `DeviceController # configure terminal`	Configures the terminal.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy test1`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**ipv6 acl** *acl_name* **Example:** `Device(config-wireless-policy)# ipv6 acl testacl`	Creates a named WLAN ACL.
Step 4	**ipv6 traffic-filter web** *acl_name-preauth* **Example:** `Device(config-wlan)# ipv6 traffic-filter web preauth1`	Creates a pre-authentication ACL for web authentication.

Verifying IPv6 ACL

Displaying IPv6 ACLs

To display IPv6 ACLs, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**show access-list** **Example:** `Device# show access-lists`	Displays all access lists configured on the device
Step 4	**show ipv6 access-list** *acl_name* **Example:** `Device# show ipv6 access-list [access-list-name]`	Displays all configured IPv6 access list or the access list specified by name.

Configuration Examples for IPv6 ACL

Example: Creating an IPv6 ACL

This example configures the IPv6 access list named CISCO. The first deny entry in the list denies all packets that have a destination TCP port number greater than 5000. The second deny entry denies packets that have a source UDP port number less than 5000. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets. The second permit entry in the list permits all other traffic. The second permit entry is necessary because an implicit deny -all condition is at the end of each IPv6 access list.

Note Logging is supported only on Layer 3 interfaces.

```
Device(config)# ipv6 access-list CISCO
Device(config-ipv6-acl)# deny tcp any any gt 5000
Device (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Device(config-ipv6-acl)# permit icmp any any
Device(config-ipv6-acl)# permit any any
```

Example: Applying an IPv6 ACL to a Policy Profile in a Wireless Environment

This example shows how to apply an IPv6 ACL to a Policy Profile in a Wireless environment.

Note All IPv6 ACLs must be associated to a policy profile.

1. Creating an IPv6 ACL.

```
Device(config)# ipv6 access-list <acl-name>
Device(config-ipv6-acl)# permit tcp 2001:DB8::/32 any
Device(config-ipv6-acl)# permit udp 2001:DB8::/32 any
```

2. Applying the IPv6 ACL to a policy profile.

```
Device(config)# wireless profile policy <policy-profile-name>
Device(config-wireless-policy)# shutdown
Device(config-wireless-policy)# ipv6 acl <acl-name>
Device(config-wireless-policy)# no shutdown
```

Displaying IPv6 ACLs

To display IPv6 ACLs, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**show access-list** **Example:** `Device# show access-lists`	Displays all access lists configured on the device
Step 2	**show ipv6 access-list** *acl_name* **Example:** `Device# show ipv6 access-list [access-list-name]`	Displays all configured IPv6 access list or the access list specified by name.

Example: Displaying IPv6 ACLs

This is an example of the output from the **show access-lists** privileged EXEC command. The output shows all access lists that are configured on the switch or switch stack.

```
Device #show access-lists
Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

This is an example of the output from the **show ipv6 access-lists** privileged EXEC command. The output shows only IPv6 access lists configured on the switch or switch stack.

```
Device# show ipv6 access-list
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30

IPv6 access list outbound
```

```
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```

Example: Configuring RA Throttling

This task describes how to create an RA throttle policy in order to help the power-saving wireless clients from being disturbed by frequent unsolicited periodic RA's. The unsolicited multicast RA is throttled by the controller.

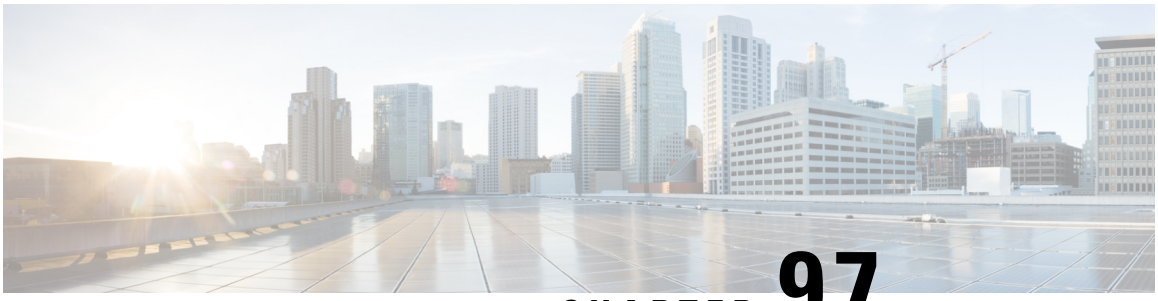
Before you begin

Enable IPv6 on the client machine.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ipv6 nd ra-throttler policy Mythrottle** **Example:** `Device (config)# ipv6 nd ra-throttler policy Mythrottle`	Creates a RA throttler policy called Mythrottle.
Step 3	**throttle-period 20** **Example:** `Device (config-nd-ra-throttle)# throttle-period 20`	Determines the time interval segment during which throttling applies.
Step 4	**max-through 5** **Example:** `Device (config-nd-ra-throttle)# max-through 5`	Determines how many initial RA's are allowed.
Step 5	**allow at-least 3 at-most 5** **Example:** `Device (config-nd-ra-throttle)# allow at-least 3 at-most 5`	Determines how many RA's are allowed after the initial RAs have been transmitted, until the end of the interval segment.
Step 6	**switch (config)# vlan configuration 100** **Example:** `Device (config)# vlan configuration 100`	Creates a per vlan configuration.
Step 7	**ipv6 nd ra-th attach-policy attach-policy_name** **Example:**	Enables the router advertisement throttling.

	Command or Action	Purpose
	`Device (config)# ipv6 nd ra-throttle attach-policy attach-policy_name`	
Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.



CHAPTER 97

IPv6 Client Mobility

- Information About IPv6 Client Mobility, on page 931
- Prerequisites for IPv6 Client Mobility, on page 933
- Monitoring IPv6 Client Mobility, on page 934

Information About IPv6 Client Mobility

Link layer mobility is not enough to make wireless client Layer 3 applications continue to work seamlessly while roaming. Cisco IOSd's wireless mobility module uses mobility tunneling to retain seamless connectivity for the client's Layer 3 PoP (point of presence) when the client roams across different subnets on different switches.

IPv6 is the next-generation network layer Internet protocol intended to replace 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 device keeps track of IPv6 clients by intercepting the ICMPv6 messages to provide seamless mobility and protect the network from network attacks. The NDP (neighbor discovery packets) packets are converted from multicast to unicast and delivered individually per client. This unique solution ensures that Neighbor Discovery and Router Advertisement packets are not leaked across VLANs. Clients can receive specific Neighbor Discovery and Router Advertisement packets ensuring correct IPv6 addressing to avoid 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 device must be part of the same mobility group. Both IPv4 and IPv6 client mobility are enabled by default.

IPv6 client mobility is used for the following:

- Retaining the client IPv6 multiple addresses in Layer-2 and Layer-3 roaming.
- IPv6 Neighbor Discovery Prootcol (NDP) packet management.
- Client IPv6 addresses learning.

Note The configuration for IPv6 mobility in SDA wireless and Local mode is the same as of IPv4 mobility and requires no different software configuration on the client side to achieve seamless roaming. Refer to IPv4 mobility section for configuration information.

Note If ipv6 address is configured on the SVI, you should configure **ipv6 nd ra suppress all** command on all client VLAN SVI interfaces on the controller. This prevents multiple devices from advertising themselves as the routers.

Using Router Advertisment

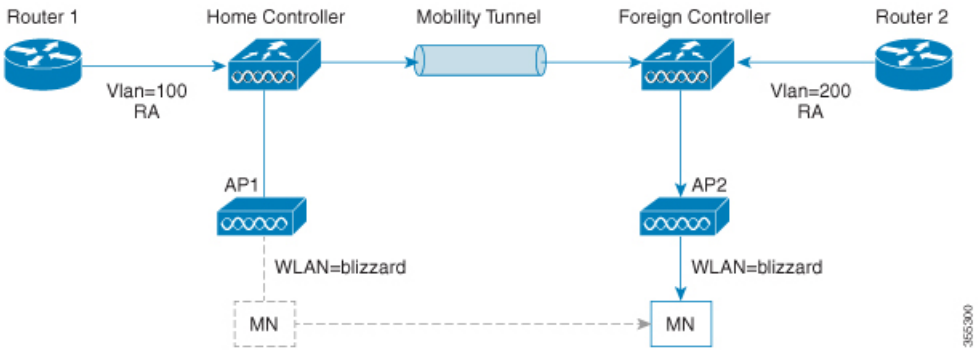
The Neighbor Discovery Protocol(NDP) operates in the link-layer and is responsible for the discovery of other nodes on the link. It determines the link-layer addresses of other nodes, finds the available routers, and maintains reachability information about the paths to other active neighbor nodes.

Router Advertisement (RA) is one of the IPv6 Neighbor Discovery Protocol (NDP) packets that is used by the hosts to discover available routers, acquire the network prefix to generate the IPv6 addresses, link MTU, and so on. The routers send RA on a regular basis, or in response to hosts Router Solicitation messages.

IPv6 wireless client mobility manages the IPv6 RA packet . The device forwards the link-local all-nodes multicast RA packets to the local and roaming wireless nodes mapped on same VLAN the RA was received on.

Figure 1 illustrates how a roaming client “MN” receives RA from VLAN 200 in a foreign controller and how it acquires an new IP address and breaks into L3 mobility's point of presence.

Figure 23: Roaming Client Receives Valid RA from Router 1



Router Advertisement Throttling

RA throttling allows the controller to enforce limits to the RA packets headed toward the wireless network. By enabling RA throttling, routers that send multiple RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity. If a client sends an RS packet, an RA is sent back to the client. This RA is allowed through the controller and unicast to the client. This process ensures that the new clients or roaming clients are not affected by the RA throttling.

IPv6 Address Learning

There are three ways for IPv6 client to acquire IPv6 addresses:

- Stateless Address Auto-Configuration (SLAAC)
- Stateful DHCPv6
- Static configuration

For these methods, the IPv6 client always sends NS DAD (duplicate address detection) to ensure that there is no duplicated IP address on the network. The device snoops the clients NDP and DHCPv6 packets to learn about its client IP addresses and then updates the controllers database. The database then informs the controller for the clients new IP address.

Handling Multiple IP Addresses

In the case when the new IP address is received after RUN state, whether an addition or removal, the controller updates the new IP addresses on its local database for display purposes. Essentially, the IPv6 uses the existing or same PEM state machine code flow as in IPv4. When the IP addresses are requested by external entities, for example, from Prime Infrastructure, the controller will include all the available IP addresses, IPv4 and IPv6, in the API/SPI interface to the external entities.

An IPv6 client can acquire multiple IP addresses from stack for different purposes. For example, a link-local address for link local traffic, and a routable unique local or global address.

When the client is in the DHCP request state and the controller receives the first IP address notification from the database for either an IPv4 or IPv6 address, the PEM moves the client into the RUN state.

When a new IP address is received after the RUN state, either for addition or removal, the controller updates the new IP addresses on its local database for display purposes.

When the IP addresses are requested by external entities, for example, from Prime Infrastructure, the controller provides the available IP addresses, both IPv4 and IPv6, to the external entities.

IPv6 Configuration

The device supports IPv6 client as seamlessly as the IPv4 clients. The administrator must manually configure the VLANs to enable the IPv6, IPv6's snooping and throttling functionality. This will enable the NDP packets to throttle between the device and its various clients.

Prerequisites for IPv6 Client Mobility

- To enable wireless IPv6 client connectivity, the underlying wired network must support IPv6 routing and an address assignment mechanism such as SLAAC or DHCPv6. The device must have L2 adjacency to the IPv6 router, and the VLAN needs to be tagged when the packets enter the device. APs do not require connectivity on an IPv6 network, as all traffic is encapsulated inside the IPv4 CAPWAP tunnel between the AP and device.
- When using the IPv6 Client Mobility, clients must support IPv6 with either static stateless auto configuration or stateful DHCPv6 IP addressing .

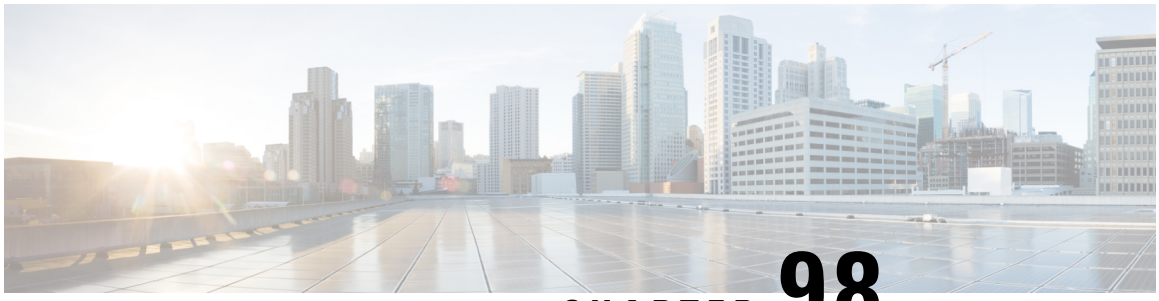
- To allow smooth operation of stateful DHCPv6 IP addressing, you must have a switch or router that supports the DHCP for IPv6 feature that is configured to act like a DHCPv6 server, or you need a dedicated server such as a Windows 2008 server with a built-in DHCPv6 server.

Monitoring IPv6 Client Mobility

The commands in Table 1 are used to monitor IPv6 Client mobility on the device.

Table 41: Monitoring IPv6 Client Mobility Commands

Commands	Description
show wireless client summary	Displays the wireless specific configuration of active clients.
show wireless client mac-address `(mac-addr-detail)`	Displays the wireless specific configuration of active clients based on their MAC address.



CHAPTER 98

IPv6 Support on Flex and Mesh

- IPv6 Support on Flex + Mesh Deployment, on page 935
- Configuring IPv6 Support for Flex + Mesh, on page 935
- Verifying IPv6 on Flex+Mesh , on page 937

IPv6 Support on Flex + Mesh Deployment

IPv6 is the backhaul transport of the Service Provider. The IPv6 support over flex + mesh feature is now supported on the Cisco Catalyst 9800 Series Wireless Controller . WLAN accepts IPv6 clients and forward the traffic.

Configuring IPv6 Support for Flex + Mesh

Follow the procedure given below to enable the IPv6 routing on the controller :

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface vlan** *vlan-interface-number* **Example:** `Device(config)#interface vlan 89`	Creates an interface and enters the interface configuration mode.
Step 3	**shutdown** **Example:** `Device(config-if)#shutdown`	Disables the interface configuration.
Step 4	**ipv6 enable** **Example:** `Device(config-if)#ipv6 enable`	Optional. Enables IPv6 on the interface.

	Command or Action	Purpose
Step 5	**ipv6 address** *X:X:X:X::X/<0-128>* **Example:** `Device(config-if)#ipv6 address 1:1:1:1::1/64`	Configures IPv6 address on the interface using the IPv6 prefix option.
Step 6	**no shutdown** **Example:** `Device(config-if)#no shutdown`	Enables the IPv6 address.
Step 7	**no shutdown** **Example:** `Device(config-if)#no shutdown`	Enables the PIM dense-mode operation.
Step 8	**end** **Example:** `Device(config-if)#end`	Returns to privileged EXEC mode.
Step 9	**show ipv6 interface brief** **Example:** `Device#show ipv6 interface brief`	Verifies your entries.
Step 10	**ping ipv6** *destination-address or hostname* **Example:** `Device#ping ipv6 1:1:1:1::10`	Checks the gateway connectivity.

Configuring Preferred IP Address as IPv6 (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 Click the AP Join Profile Name. The **Edit AP Join Profile** window is displayed.

Step 3 Choose **CAPWAP** > **Advanced**.

Step 4 From the **Preferred Mode** drop-down list, select **IPV6**.

Step 5 Click **Update & Apply to Device**.

Configuring Preferred IP Address as IPv6

Procedure

	Command or Action	Purpose
Step 1	**Configure Terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *default-ap-profile* **Example:** `Device(config)# ap profile default-ap-profile`	Enters AP profile configuration mode.
Step 3	**preferred-mode ipv6** **Example:** `Device(config-ap-profile)# preferred-mode ipv6`	Uses IPv6 to join the controller .
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Exits the configuration mode and returns to privileged EXEC mode.

Verifying IPv6 on Flex+Mesh

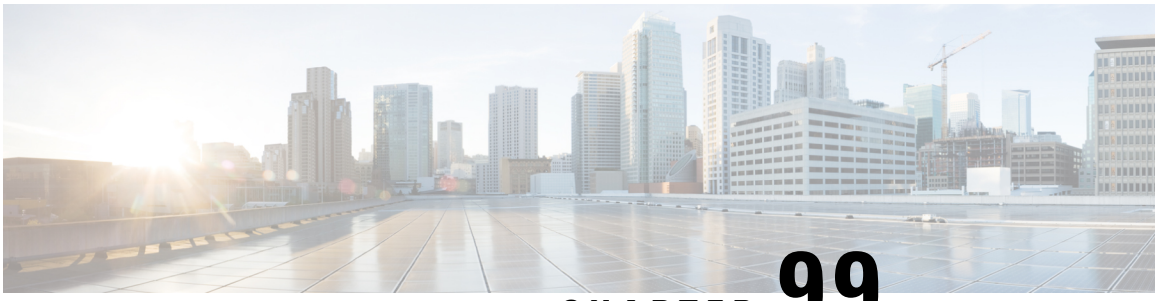
To verify the IPv6 configuration on the controller , use the following **show** command:

```
Device#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet2       unassigned      YES unset  up                    up
GigabitEthernet0       unassigned      YES NVRAM  administratively down down
Capwap1                unassigned      YES unset  up                    up
Capwap2                unassigned      YES unset  up                    up
Vlan1                  unassigned      YES NVRAM  administratively down down
Vlan89                 9.10.89.90      YES NVRAM  up                    up
Ewlc-9.10.89.90#show running-config interface vlan 89
Building configuration...

Current configuration : 120 bytes
!
interface Vlan89
 ip address 9.10.89.90 255.255.255.0
 ip helper-address 9.1.0.100
 no mop enabled
 no mop sysid
end
```

PART XI

CleanAir

- Cisco CleanAir, on page 941
- Bluetooth Low Energy, on page 957
- Spectrum Intelligence, on page 961



CHAPTER 99

Cisco CleanAir

- Information About Cisco CleanAir, on page 941
- Prerequisites for CleanAir, on page 944
- Restrictions for CleanAir, on page 945
- How to Configure CleanAir, on page 945
- Verifying CleanAir Parameters, on page 953
- Configuration Examples for CleanAir, on page 954
- CleanAir FAQs, on page 955

Information About Cisco CleanAir

Cisco CleanAir is a solution designed to proactively manage the challenges of a shared wireless spectrum. It allows you to see all the users of a shared spectrum (both native devices and foreign interferers). It also enables the network to act upon this information. For example, you can manually remove the interfering device, or the system can automatically change the channel away from the interference. CleanAir provides spectrum management and Radio Frequency (RF) visibility.

A Cisco CleanAir system consists of CleanAir-enabled access points and Cisco Catalyst 9800 Series Wireless Controller . These access points collect information about all the 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 and displays the interference devices.

For every device operating in the unlicensed band, Cisco CleanAir provides information about what 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-GHz 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 the Wi-Fi operations.

Some of the most advanced WLAN services, such as voice-over-wireless and IEEE 802.11 radio communications, might be significantly impaired by the interference caused by other legal users of the ISM bands. The integration of Cisco CleanAir functionality addresses this problem of RF interference.

Cisco CleanAir-Related Terms

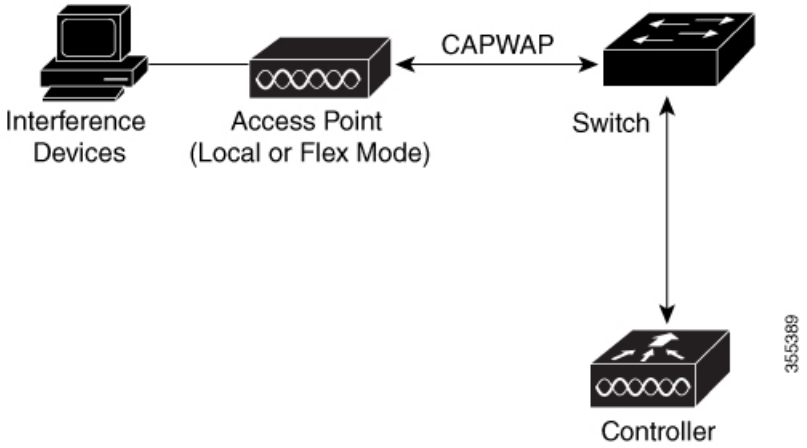
Table 42: CleanAir-Related Terms

Term	Decription
AQI	Air Quality Index. The AQI is an indicator of air quality, based on the air pollutants. An AQI of 0 is bad and an AQI > 85 is good.
AQR	Air Quality Report. AQRs contain information about total interference from all the identified sources represented by AQI and the summary of the most severe interference categories. AQRs are sent every 15 minutes to the Mobility Controller and every 30 seconds in the Rapid mode.
DC	Duty Cycle. Percentage of time that the channel is utilized by a device.
EDRRM	Event-Driven RRM. EDRRM allows an access point in distress to bypass normal RRM intervals and immediately change channels.
IDR	Interference Device Reports that an access point sends to the controller .
ISI	Interference Severity Index. The ISI is an indicator of the severity of the interference.
RSSI	Received Signal Strength Indicator. RSSI is a measurement of the power present in a received radio signal. It is the power at which an access point sees the interferer device.

Cisco CleanAir Components

The basic Cisco CleanAir architecture consists of Cisco CleanAir-enabled APs and device.

Figure 24: Cisco CleanAir Solution



An access point equipped with Cisco CleanAir technology collects information about Wi-Fi interference sources and processes it. The access point collects and sends the Air Quality Report (AQR) and Interference Device Report (IDR) to the controller .

The controller controls and configures CleanAir-capable access points, and collects and processes spectrum data. The controller provides local user interfaces (GUI and CLI) to configure basic CleanAir features and services and display current spectrum information. The controller also detects, merges, and mitigates interference devices using RRM TPC and DCA For details, see Interference Device Merging.

The device performs the following tasks in a Cisco CleanAir system:

- Configures Cisco CleanAir capabilities on the access point.
- Provides interfaces (GUI and CLI) for configuring Cisco CleanAir features and retrieving data.
- Displays spectrum data.
- Collects and processes AQRs from the access point and stores them in the air quality database. AQRs contain information about the total interference from all the identified sources represented by the Air Quality Index (AQI) and the summary for the most severe interference categories. The CleanAir system can also include unclassified interference information under per-interference type reports that enable you to take action in scenarios where interference because of unclassified interfering devices is more.
- Collects and processes IDRs from the access point and stores them in the interference device database.

Note When Cisco CleanAir is disabled and Spectrum Intelligence (SI) is enabled in the controller, both CleanAir and Air Quality reporting are disabled. In spite of this, Air Quality is still populated for SI APs and viewed as disabled when **show ap dot11 5ghz/24ghz cleanair config** command is executed. This is an expected behaviour as SI APs report Air Quality.

Here, Spectrum intelligence is a subset of CleanAir features. For more information on Spectrum Intelligence, see the *Spectrum Intelligence Deployment Guide*.

Interference Types that Cisco CleanAir can Detect

Cisco CleanAir access points can detect and report severity of the interference. Spectrum event-driven RRM is one such mitigation strategy.

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 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. Spontaneous interference event is commonly used for CleanAir.

Note Spectrum event-driven RRM can be triggered only by Cisco CleanAir-enabled access points in local mode.

Spontaneous interference is interference that appears suddenly on a network, perhaps jamming a channel or a range of channels completely. The Cisco CleanAir spectrum event-driven RRM feature allows you to set a threshold for air quality (AQ) which, 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.

Microwave Ovens, Outdoor Ethernet bridges are two classes of devices that qualify as persistent, since once detected, it is likely that these devices will continue to be a random problem and are not likely to move. For these types of devices we can tell RRM of the detection and Bias the affected channel so that RRM "remembers" that there is a high potential for client impacting interference for the Detecting AP on the detected channel. For more information, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/b_RRM_White_Paper_chapter_0100.html?bookSearch=true#id_15217.

CleanAir PDA devices include:

- Microwave Oven
- WiMax Fixed
- WiMax Mobile
- Motorola Canopy

In the case of Bluetooth devices, Cisco CleanAir-enabled access points can detect and report interference only if the devices are actively transmitting. Bluetooth devices have extensive power-save modes. For example, interference can be detected when data or voice is being streamed between the connected devices.

EDRRM and AQR Update Mode

EDRRM is a feature that allows an access point that is in distress to bypass normal RRM intervals and immediately change channels. A CleanAir access point always monitors AQ and reports the AQ every 15 minutes. AQ only reports classified interference devices. The key benefit of EDRRM is fast action time. If an interfering device is operating on an active channel and causes enough AQ degradation to trigger an EDRRM, then no clients will be able to use that channel or the access point. You must remove the access point from the channel. EDRRM is not enabled by default, you must first enable CleanAir and then enable EDRRM.

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

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 device's ability to detect neighboring in-network access points. Correlating interference device detections from multiple access points is limited between monitor-mode access points.
- 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.

How to Configure CleanAir

Enabling CleanAir for the 2.4-GHz Band (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **CleanAir**

Step 2 On the **CleanAir** page, click the me**2.4 GHz Band** > **General** tab.

Step 3 Check the **Enable CleanAir** checkbox.

Step 4 Click **Apply**.

Enabling CleanAir for the 2.4-GHz Band (CLI)

Procedure

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

Step 2	**ap dot11 24ghz cleanair**
	Example:
	`Device(config)#ap dot11 24ghz cleanair`
	`Device(config)#no ap dot11 24ghz cleanair`
		Enables the CleanAir feature on the 802.11b network. Run the **no** form of this command to disable CleanAir on the 802.11b network.

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

Configuring Interference Reporting for a 2.4-GHz Device (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **CleanAir**.

Step 2 Click the **2.4 GHz Band** tab.

Step 3 Choose the interference types and add them to the **Interference Types to detect** section.

The following interference types are available:

- BLE Beacon—Bluetooth low energy beacon
- Bluetooth Discovery
- Bluetooth Link
- Canopy
- Continuous Transmitter
- DECT-like Phone—Digital Enhanced Cordless Technology phone
- 802.11 FH—802.11 frequency hopping device
- WiFi Inverted—Device using spectrally inverted Wi-Fi signals
- Jammer
- Microwave Oven

- WiFi Invalid Channel—Device using nonstandard Wi-Fi channels
- TDD Transmitter
- Video Camera
- SuperAG—802.11 SuperAG device
- WiMax Mobile
- WiMax Fixed
- 802.15.4
- Microsoft Device
- SI_FHSS

Step 4 Click **Apply**.

Configuring Interference Reporting for a 2.4-GHz Device (CLI)

Procedure

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

Step 2	**ap dot11 24ghz cleanair device** {**ble-beacon** | **bt-discovery** | **bt-link** | **canopy** | **cont-tx** | **dect-like** | **fh** | **inv** | **jammer** | **mw-oven** | **nonstd** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile** | **xbox** | **zigbee** }
	Example:
	`Device(config)# ap dot11 24ghz cleanair device ble-beacon`
	`Device(config)# ap dot11 24ghz cleanair device bt-discovery`
	`Device(config)# ap dot11 24ghz cleanair device bt-link`
	`Device(config)# ap dot11 24ghz cleanair device canopy`
	`Device(config)# ap dot11 24ghz cleanair device cont-tx`
		Configures the 2.4-GHz interference devices to report to the device. Run the **no** form of this command to disable the configuration.
		The following is a list of the keyword descriptions:
		• **ble-beacon**—Bluetooth low energy beacon
		• **bt-discovery**—Bluetooth discovery
		• **bt-link**—Bluetooth link
		• **canopy**—Canopy device
		• **cont-tx**—Continuous transmitter
		• **dect-like**—Digital Enhanced Cordless Communication-like phone
		• **fh**—802.11-frequency hopping device
		• **inv**—Device using spectrally inverted Wi-Fi signals

	Command or Action	Purpose
	Device(config)# **ap dot11 24ghz cleanair device dect-like** Device(config)# **ap dot11 24ghz cleanair device fh** Device(config)# **ap dot11 24ghz cleanair device inv** Device(config)# **ap dot11 24ghz cleanair device jammer** Device(config)# **ap dot11 24ghz cleanair device mw-oven** Device(config)# **ap dot11 24ghz cleanair device nonstd** Device(config)# **ap dot11 24ghz cleanair device report** Device(config)# **ap dot11 24ghz cleanair device superag** Device(config)# **ap dot11 24ghz cleanair device tdd-tx** Device(config)# **ap dot11 24ghz cleanair device video** Device(config)# **ap dot11 24ghz cleanair device wimax-fixed** Device(config)# **ap dot11 24ghz cleanair device wimax-mobile** Device(config)# **ap dot11 24ghz cleanair device xbox** Device(config)# **ap dot11 24ghz cleanair device zigbee** Device(config)# **ap dot11 24ghz cleanair device alarm**	• **jammer**—Jammer • **mw-oven**—Microwave oven • **nonstd**—Device using nonstandard Wi-Fi channels • **report**—Interference device reporting • **superag**—802.11 SuperAG device • **tdd-tx**—TDD transmitter • **video**—Video camera • **wimax-fixed**—WiMax Fixed • **wimax-mobile**—WiMax Mobile • **microsoft xbox**—Microsoft Xbox device • **zigbee**—802.15.4 device
Step 3	**end** **Example:** Device(config)# **end**	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Enabling CleanAir for the 5-GHz Band (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **CleanAir**

Step 2 On the **CleanAir** page, click the me**5 GHz Band** > **General** tab.

Step 3 Check the **Enable CleanAir** checkbox.

Step 4 Click **Apply**.

Enabling CleanAir for the 5-GHz Band (CLI)

Procedure

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

Step 2	**ap dot11 5ghz cleanair**
	Example:
	`Device(config)#ap dot11 5ghz cleanair`
	`Device(config)#no ap dot11 5ghz cleanair`
		Enables the CleanAir feature on a 802.11a network. Run the **no** form of this command to disable CleanAir on the 802.11a network.

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

Configuring Interference Reporting for a 5-GHz Device (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **CleanAir**.

Step 2 Click the **5 GHz Band** tab.

Step 3 Choose the interference types and add them to the **Interference Types to detect** section.

The following interference types are available:

- Canopy
- Continuous Transmitter
- DECT-like Phone—Digital Enhanced Cordless Technology phone
- 802.11 FH—802.11 frequency hopping device
- WiFi Inverted—Device using spectrally inverted Wi-Fi signals
- Jammer
- WiFi Invalid Channel—Device using nonstandard Wi-Fi channels

- SuperAG—802.11 SuperAG device
- TDD Transmitter
- WiMax Mobile
- WiMax Fixed
- Video Camera

Step 4 Click **Apply**.

Configuring Interference Reporting for a 5-GHz Device (CLI)

Procedure

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

Step 2	**ap dot11 5ghz cleanair device** {**canopy** | **cont-tx** | **dect-like** | **inv** | **jammer** | **nonstd** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile**}
	Example:
	`Device(config)#ap dot11 5ghz cleanair device canopy`
	`Device(config)#ap dot11 5ghz cleanair device cont-tx`
	`Device(config)#ap dot11 5ghz cleanair device dect-like`
	`Device(config)#ap dot11 5ghz cleanair device inv`
	`Device(config)#ap dot11 5ghz cleanair device jammer`
	`Device(config)#ap dot11 5ghz cleanair device nonstd`
	`Device(config)#ap dot11 5ghz cleanair device report`
	`Device(config)#ap dot11 5ghz cleanair device superag`
		Configures a 5-GHz interference device to report to the device. Run the **no** form of this command to disable interference device reporting.
		The following is a list of the keyword descriptions:
		• **canopy**—Canopy device
		• **cont-tx**—Continuous transmitter
		• **dect-like**—Digital Enhanced Cordless Communication-like phone
		• **fh**—802.11-frequency hopping device
		• **inv**—Device using spectrally-inverted Wi-Fi signals
		• **jammer**—Jammer
		• **nonstd**—Device using nonstandard Wi-Fi channels
		• **superag**—802.11 SuperAG device
		• **tdd-tx**—TDD transmitter
		• **video**—Video camera
		• **wimax-fixed**—WiMax fixed

	Command or Action	Purpose

	`Device(config)#ap dot11 5ghz cleanair device tdd-tx`
	
	`Device(config)#ap dot11 5ghz cleanair device video`
	
	`Device(config)#ap dot11 5ghz cleanair device wimax-fixed`
	
	`Device(config)#ap dot11 5ghz cleanair device wimax-mobile`
	
	`Device(config)#ap dot11 5ghz cleanair device si_fhss`
	
	`Device(config)#ap dot11 5ghz cleanair device alarm`
		• **wimax-mobile**—WiMax mobile

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

Configuring Event Driven RRM for a CleanAir Event (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.
The **Radio Resource Management** page is displayed.

Step 2 Click the **DCA** tab.

Step 3 In the **Event Driven RRM** section, check the **EDRRM** check box to run RRM when CleanAir-enabled AP detects a significant level of interference.

Step 4 Configure the **Sensitivity Threshold** level at which RRM has to be invoked from the following options:

- **Low**: Represents a decreased sensitivity to changes in the environment and its value is set at 35.
- **Medium**: Represents medium sensitivity to changes in the environment at its value is set at 50.
- **High**: Represents increased sensitivity to changes in the environment at its value is set at 60.
- **Custom**: If you choose this option, you must specify a custom value in the **Custom Threshold** box.

Step 5 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 percent.

Note Rogue Contribution is a new component included in ED-RRM functionality. Rogue Contribution allows ED-RRM to trigger based on identified Rogue Channel Utilization, which is completely separate from CleanAir metrics. Rogue Duty Cycle comes from normal off channel RRM metrics, and invokes a channel change based on neighboring rogue interference. Because this comes from RRM metrics and not CleanAir, the timing - assuming normal 180 second off channel intervals - would be within 3 minutes or 180 seconds worst case. It is configured separately from CleanAir ED-RRM and is disabled by default. This allows the AP to become reactive to Wi-Fi interference that is not coming from own network and is measured at each individual AP.

Step 6 Save the configuration.

Configuring EDRRM for a CleanAir Event (CLI)

Procedure

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

Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event**
	Example:
	`Device(config)#ap dot11 24ghz rrm channel cleanair-event`
	`Device(config)#no ap dot11 24ghz rrm channel cleanair-event`
		Enables EDRRM CleanAir event. Run the **no** form of this command to disable EDRRM.

Step 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event** [**sensitivity** {**custom** | **high** | **low** | **medium**}] **Example:** `Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	Configures the EDRRM sensitivity of the CleanAir event. The following is a list of the keyword descriptions: • **Custom**—Specifies custom sensitivity to non-Wi–Fi interference as indicated by the AQ value. • **High**—Specifies the most sensitivity to non-Wi–Fi interference as indicated by the AQ value. • **Low**—Specifies the least sensitivity to non-Wi–Fi interference as indicated by the AQ value. • **Medium**—Specifies medium sensitivity to non-Wi–Fi interference as indicated by the AQ value.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying CleanAir Parameters

You can verify CleanAir parameters using the following commands:

Table 43: Commands for verifying CleanAir

Command Name	Description
show ap dot11 24ghz cleanair device type all	Displays all the CleanAir interferers for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type ble-beacon	Displays all the Bluetooth BLE beacons for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type bt-discovery	Displays CleanAir interferers of type BT Discovery for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type bt-link	Displays CleanAir interferers of type BT Link for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type canopy	Displays CleanAir interferers of type Canopy for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type cont-tx	Displays CleanAir interferers of type Continuous transmitter for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type dect-like	Displays CleanAir interferers of type DECT Like for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type fh	Displays CleanAir interferers of type 802.11FH for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type inv	Displays CleanAir interferers of type Wi-Fi Inverted for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type jammer	Displays CleanAir interferers of type Jammer for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type mw-oven	Displays CleanAir interferers of type MW Oven for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type nonstd	Displays CleanAir interferers of type Wi-Fi inverted channel for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type superag	Displays CleanAir interferers of type SuperAG for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type tdd-tx	Displays CleanAir interferers of type TDD Transmit for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type video	Displays CleanAir interferers of type Video Camera for the 2.4-GHz band.

Command Name	Description
show ap dot11 24ghz cleanair device type wimax-fixed	Displays CleanAir interferers of type WiMax Fixed for the 2.4-GHz band.

Monitoring Interference Devices

When a CleanAir-enabled access point detects interference devices, detections of the same device from multiple sensors are merged together to create clusters. Each cluster is given a unique ID. Some devices conserve power by limiting the transmit time until actually needed, which results in the spectrum sensor to stop detecting the device temporarily. This device is then correctly marked as down. Such a device is correctly removed from the spectrum database. In cases when all the interferer detections for a specific device 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 for longer and they are remerged into a single record upon detection. This process smoothens the user records and accurately represents the device history.

Note The following is a prerequisite for monitoring the interference devices:

You can configure Cisco CleanAir only on CleanAir-enabled access points.

Configuration Examples for CleanAir

This example shows how to enable CleanAir on the 2.4-GHz band and an access point operating in the channel:

```
Device#configure terminal
Device(config)#ap dot11 24ghz cleanair
Device(config)#exit
Device#ap name TAP1 dot11 24ghz cleanair
Device#end
```

This example shows how to enable an EDRRM CleanAir event in the 2.4-GHz band and configure high sensitivity to non-Wi–Fi interference:

```
Device#configure terminal
Device(config)#ap dot11 24ghz rrm channel cleanair-event
Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high
Device(config)#end
```

This example shows how to enable an access point in the monitor mode:

```
Device#ap name <ap-name> mode monitor
```

CleanAir FAQs

Q. Multiple access points detect the same interference device. However, the device shows them as separate clusters or different suspected devices clustered together. Why does this happen?

A. Access points must be RF neighbors for the device to consider merging the devices that are detected by these access points. An access point takes time to establish neighbor relationships. A few minutes after the device reboots or after there is a change in the RF group, and similar events, clustering will not be very accurate.

Q. How do I view neighbor access points?

A. To view neighbor access points, use the **show ap** *ap_name* **auto-rf dot11** {**24ghz** | **5ghz**} command.

This example shows how to display the neighbor access points:

```
Device#show ap name AS-5508-5-AP3 auto-rf dot11 24ghz

<snippet>
Nearby APs
  AP 0C85.259E.C350 slot 0                          :  -12 dBm on   1 (10.10.0.5)
  AP 0C85.25AB.CCA0 slot 0                          :  -24 dBm on   6 (10.10.0.5)
  AP 0C85.25C7.B7A0 slot 0                          :  -26 dBm on  11 (10.10.0.5)
  AP 0C85.25DE.2C10 slot 0                          :  -24 dBm on   6 (10.10.0.5)
  AP 0C85.25DE.C8E0 slot 0                          :  -14 dBm on  11 (10.10.0.5)
  AP 0C85.25DF.3280 slot 0                          :  -31 dBm on   6 (10.10.0.5)
  AP 0CD9.96BA.5600 slot 0                          :  -44 dBm on   6 (10.0.0.2)
  AP 24B6.5734.C570 slot 0                          :  -48 dBm on  11 (10.0.0.2)
<snippet>
```

Q. What are the AP debug commands available for CleanAir?

A. The AP debug commands for CleanAir are:

- **debug cleanair** {**bringup** | **event** | **logdebug** | **low** | **major** | **nsi** | **offchan**}
- **debug rrm** {**neighbor** | **off-channel** | **reports**}

CHAPTER 100

Bluetooth Low Energy

- Information About Bluetooth Low Energy, on page 957
- Enabling Bluetooth Low Energy Beacon (GUI), on page 958
- Enabling Bluetooth Low Energy Beacon, on page 958

Information About Bluetooth Low Energy

Note This feature is not related to the Indoor IoT Services feature set that is part of Cisco Spaces.

This feature describes how Access Points and Catalyst 9800 can detect BLE devices as wireless interferers using Clean Air - not the BLE radio that is available on some Access Point models. This feature is not meant to be used for BLE-based asset tracking, environmental monitoring, or tag management use cases, which are powered using Cisco Spaces.

For full feature functionality of how BLE-related use cases are delivered in the Cisco solution, refer to Cisco Spaces configuration guides for Indoor IoT services.

Bluetooth low energy (BLE) is a wireless personal area network technology aimed at enhancing location services for mobile devices. The small bluetooth tag devices placed at strategic locations transmit universally unique identifiers (UUIDs) and, Major and Minor fields as their identity. These details are picked up by bluetooth-enabled smartphones and devices. The location information of these devices are sent to the corresponding back-end server. Relevant advertisements and other important information are then pushed to the devices using this location-specific information.

By treating a tag device as an interferer and using the existing system capabilities, such as interference location, the tag device can be located on a map display in a wireless LAN deployment and its movement monitored. Besides this, information on missing tags can also be obtained. This feature can determine rogue and malicious tags using the unique identifier associated with each tag (or family of tags) against a predetermined allowed list from a customer. Using the management function, alerts can be displayed or emailed based on rogue tags, missing tags, or moved tags.

Limitations of BLE Feature

- The wireless infrastructure must support Cisco CleanAir.
- Supports a maximum of only 250 unique BLE beacons (cluster entries) and 1000 device entries.

- Cisco CleanAir feature is only supported on Cisco Aironet 3700 Series Access Points with Hyperlocation module RM3010. The BLE feature on Wave 2 and Wi-Fi 6 APs works in a different manner (through cloud beacon center) and is not covered by this feature.

Areas of Use

Since the BLE feature provides granular location details of devices (smart phones or bluetooth-enabled devices) that helps push context-sensitive advertising and other information to users. Possible areas of application include retail stores, museums, zoo, healthcare, fitness, security, advertising, and so on.

Enabling Bluetooth Low Energy Beacon (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **CleanAir** > **2.4 GHz Band** > **General**.

Step 2 Check the **Enable CleanAir** check box.

Step 3 From the **Available Interference Types** list, select and move **BLE Beacon** to the **Interference Types to Detect** list.

Step 4 Click **Apply**.

Enabling Bluetooth Low Energy Beacon

Bluetooth low energy (BLE) detection is enabled by default. Use the procedure given below to enable BLE when it is disabled.

Before you begin

- The wireless infrastructure must support Cisco CleanAir.
- Cisco CleanAir configuration and show commands are available only in Mobility Controller (MC) mode.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode.
Step 2	[**no**] **ap dot11 24ghz cleanair device** [**ble-beacon**] **Example:** `Controller(config)# ap dot11 24ghz cleanair device ble-beacon`	Enables the BLE feature on the 802.11b network. Use the **no** form of the command to disable BLE feature on the 802.11b network.

	Command or Action	Purpose
Step 3	**exit** **Example:** `Controller(config)# exit`	Returns to privileged EXEC mode.

Step 4	**show ap dot11 24ghz cleanair config**
	Example:
	`Controller# show ap dot11 24ghz cleanair config`
	
	`Interference Device Settings:`
	`Interference Device Reporting..... : Enabled`
	`Bluetooth Link..... : Enabled`
	
	`Microwave Oven..... : Enabled`
	
	`BLE Beacon..... : Enabled`
		(Optional) Displays the BLE beacon configuration.

Step 5	**show ap dot11 24ghz cleanair device type ble-beacon**
	Example:
	`Controller# show ap dot11 24ghz cleanair device type ble-beacon`
	
	`DC = Duty Cycle (%)`
	`ISI = Interference Severity Index (1-Low Interference, 100-High Interference)`
	`RSSI = Received Signal Strength Index (dBm)`
	`DevID = Device ID`
	
	`No ClusterID DevID Type AP Name ISI RSSI DC Channel`
	`1 2c:92:80:00:00:22 0xa001 BLE Beacon 5508_3_AP3600_f839 -- -74 0 unknown`
		(Optional) Displays the BLE beacon device-type information.

CHAPTER 101

Spectrum Intelligence

- Spectrum Intelligence, on page 961
- Configuring Spectrum Intelligence, on page 962
- Verifying Spectrum Intelligence Information, on page 962

Spectrum Intelligence

The Spectrum Intelligence feature scans for non-Wi-Fi radio interference on 2.4-GHz and 5-GHz bands. Spectrum intelligence provides basic functions to detect interferences of three types, namely microwave, continuous wave (like video bridge and baby monitor), wi-fi and frequency hopping (bluetooth and frequency-hopping spread spectrum (FHSS) cordless phone).

The following Cisco access points (APs) support Spectrum Intelligence feature:

- Cisco Catalyst 9115 Series Wi-Fi 6 APs
- Cisco Aironet 1852E/I APs
- Cisco Aironet 1832I APs
- Cisco Aironet 1815W/T/I/M APs
- Cisco Aironet 1810W/T APs
- Cisco Aironet 1800I/S APs
- Cisco Aironet 1542D/I APs

Note You must enable Spectrum Intelligence feature on the Cisco Aironet 1832 and 1852 series APs to get radio details, such as noise, air-quality, interference, and radio utilization on the Cisco Catalyst Center Assurance AP health.

Restrictions

- SI APs only report a single interference type in Local mode.

- SI does not support high availability for air quality or interference reports. High Availability is not supported because interference report/device reported will not be copied to standby after switchover. We expect AP to send it again, if at all interferer is still there.
- Spectrum Intelligence detects only three types of devices:
  - Microwave
  - Continuous wave—(video recorder, baby monitor)
  - SI-FHSS—(Bluetooth, Frequency hopping Digital European Cordless Telecommunications (DECT) phones)

Configuring Spectrum Intelligence

Follow the procedure given below to configure spectrum intelligence:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **SI** **Example:** `Device(config)# ap dot11 24ghz SI`	Configures the 2.4-GHz or 5-GHz Spectrum Intelligence feature on the 802.11a or 802.11b network. Add **no** form of the command to disable SI on the 802.11a or 802.11b network.

Verifying Spectrum Intelligence Information

Use the following commands to verify spectrum intelligence information:

To display the SI information for a 2.4-GHz or 5-GHz band, use the following command:

```
Device# show ap dot11 24ghz SI config

SI Solution..................................... : Enabled
Interference Device Settings:
        SI_FHSS............................... : Enabled
    Interference Device Types Triggering Alarms:
        SI_FHSS............................... : Disabled
```

To display SI interferers of type Continuous transmitter for a 2.4-GHz band, use the following command:

```
Device# show ap dot11 24ghz SI device type cont_tx

DC    = Duty Cycle (%)
ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
```

```
DevID = Device ID
AP type = CA, clean air, SI spectrum intelligence

No  ClusterID       DevID  Type     AP Type AP Name                 ISI  RSSI  DC   Channel
--- --------------- ------ -------- ------- ------------------ ---- ----- ----  ---  ------
   xx:xx:xx:xx  0014  BT     CA    myAP1              --   -69 00  133
   xx:xx:xx:xx  0014  BT     SI    myAP1              --   -69 00  133
```

To display 802.11a interference devices information for the given AP for 5-GHz, use the following command:

```
Device# show ap dot11 5ghz SI device type ap

DC    = Duty Cycle (%)
ISI   = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID
AP type = CA, clean air, SI spectrum intelligence

No  ClusterID/BSSID    DevID  Type    AP Type AP Name                 ISI  RSSI  DC   Channel
--- ------------------ ------ ------- ------  ------------------------ ---- ----- ----
----------
```

To display all Cisco CleanAir interferers for a 2.4-GHz band, use the following command:

```
Device# show ap dot11 24ghz cleanair device type all
```

PART XII

Mesh Access Points

- Mesh Access Points, on page 967

CHAPTER 102

Mesh Access Points

- Introduction to the Mesh Network, on page 968
- Restrictions for Mesh Access Points, on page 969
- MAC Authorization, on page 970
- Preshared Key Provisioning, on page 970
- EAP Authentication, on page 971
- Bridge Group Names, on page 971
- Background Scanning, on page 972
- Mesh Backhaul at 2.4 GHz and 5 GHz , on page 972
- Dynamic Frequency Selection, on page 973
- Country Codes, on page 973
- Intrusion Detection System, on page 973
- Mesh Interoperability Between Controllers, on page 973
- Information About DHCP and NAT Functionality on Root AP (RAP), on page 974
- Mesh Convergence, on page 974
- Ethernet Bridging, on page 975
- Multicast Over Mesh Ethernet Bridging Network, on page 976
- Radio Resource Management on Mesh, on page 976
- Air Time Fairness on Mesh, on page 977
- Spectrum Intelligence for Mesh, on page 977
- Indoor Mesh Interoperability with Outdoor Mesh, on page 978
- Workgroup Bridge, on page 978
- Link Test, on page 978
- Mesh Daisy Chaining, on page 979
- Mesh Leaf Node, on page 979
- Flex+Bridge Mode, on page 979
- Backhaul Client Access, on page 980
- Mesh CAC, on page 980
- Configuring MAC Authorization (GUI), on page 981
- Configuring MAC Authorization (CLI), on page 981
- Configuring MAP Authorization - EAP (GUI), on page 983
- Configuring MAP Authorization (CLI), on page 983
- Configuring PSK Provisioning (CLI), on page 984
- Configuring a Bridge Group Name (GUI), on page 985

- Configuring a Bridge Group Name (CLI), on page 985
- Configuring Background Scanning (GUI), on page 986
- Configuring Background Scanning, on page 986
- Configuring Backhaul Client Access (GUI), on page 987
- Configuring Backhaul Client Access (CLI), on page 987
- Configuring Wireless Backhaul Data Rate (CLI), on page 988
- Configuring Dynamic Frequency Selection (CLI), on page 988
- Configuring the Intrusion Detection System (CLI), on page 989
- Configuring Ethernet Bridging (GUI), on page 990
- Configuring Ethernet Bridging (CLI), on page 990
- Configuring Multicast Modes over Mesh, on page 991
- Configuring RRM on Mesh Backhaul (CLI), on page 992
- Selecting a Preferred Parent (GUI), on page 993
- Selecting a Preferred Parent (CLI), on page 993
- Changing the Role of an AP (GUI), on page 994
- Changing the Role of an AP (CLI), on page 995
- Configuring the Mesh Leaf Node (CLI), on page 995
- Configuring the Mesh Leaf Node (GUI), on page 995
- Configuring Subset Channel Synchronization , on page 996
- Provisioning LSC for Bridge-Mode and Mesh APs (GUI), on page 996
- Provisioning LSC for Bridge-Mode and Mesh APs, on page 997
- Specifying the Backhaul Slot for the Root AP (GUI), on page 998
- Specifying the Backhaul Slot for the Root AP (CLI), on page 998
- Using a Link Test on Mesh Backhaul (GUI), on page 999
- Using a Link Test on Mesh Backhaul, on page 999
- Configuring Battery State for Mesh AP (GUI), on page 1000
- Configuring Battery State for Mesh AP, on page 1000
- Configuring DHCP Server on Root Access Point (RAP), on page 1000
- Configuring Mesh CAC (CLI), on page 1001
- Configuring Fast Teardown for a Mesh AP Profile (CLI), on page 1001
- Verifying DHCP Server for Root AP Configuration, on page 1002
- Verifying Mesh Configuration, on page 1003

Introduction to the Mesh Network

Mesh networking employs Cisco Aironet outdoor mesh access points and indoor mesh access points along with Cisco Wireless Controller and Cisco Prime Infrastructure to provide scalability, central management, and mobility between indoor and outdoor deployments. Control and Provisioning of Wireless Access Points (CAPWAP) protocol manages the connection of mesh access points to the network.

End-to-end security within the mesh network is supported by employing Advanced Encryption Standard (AES) encryption between wireless mesh access points and Wi-Fi Protected Access 2 (WPA2) clients. For connections to a mesh access point (MAP) wireless client, such as MAP-to-MAP and MAP-to-root access point, WPA2 is applicable.

The wireless mesh terminates on two points on the wired network. The first location is where the root access point (RAP) is attached to the wired network, and where all bridged traffic connects to the wired network.

The second location is where the CAPWAP controller connect to the wired network; this location is where the WLAN client traffic from the mesh network is connected to the wired network. The WLAN client traffic from CAPWAP is tunneled to Layer 2. Matching WLANs should terminate on the same switch VLAN on which the wireless controllers are co-located. The security and network configuration for each of the WLANs on the mesh depend on the security capabilities of the network to which the wireless controller is connected.

In the new configuration model, the controller has a default mesh profile. This profile is mapped to the default AP-join profile, which is in turn is mapped to the default site tag. If you are creating a named mesh profile, ensure that these mappings are put in place, and the corresponding AP is added to the corresponding site-tag.

Restrictions for Mesh Access Points

The Mesh feature is supported only on the following AP platforms:

- Outdoor APs
  - Cisco Industrial Wireless 3702 Access Points (supported from Cisco IOS XE Gibraltar 16.11.1b).
  - Cisco Aironet 1542 Access Points
  - Cisco Aironet 1562 Access Points
  - Cisco Aironet 1572 Access Points
  - Cisco Catalyst IW6300 Heavy Duty Access Points
  - Cisco 6300 Series Embedded Services Access Points
- Indoor APs
  - Cisco Aironet 1700 Access Points
  - Cisco Aironet 1815m Access Points
  - Cisco Aironet 2700 Access Points
  - Cisco Aironet 3700 Access Points

The following mesh features are not supported:

- Serial backhaul AP support with separate backhaul radios for uplink and downlink.
- Public Safety channels (4.9-GHz band) support.
- Passive Beaconing (Anti-Stranding)

Note

- Only Root APs support SSO. MAPs will disconnect and rejoin after SSO.

  The AP Stateful Switch Over (SSO) feature allows the access point (AP) to establish a CAPWAP tunnel with the Active controller and share a mirror copy of the AP database with the Standby controller. The overall goal for the addition of AP SSO support to the controller is to reduce major downtime in wireless networks due to failure conditions that may occur due to box failover or network failover.

- In a mixed regulatory domain mesh AP deployment, ensure that the Dynamic Channel Assignment (DCA) allowed channel list is supported by MAPs.

MAC Authorization

You must enter the MAC address of an AP in the controller to make a MAP join the controller. The controller responds only to those CAPWAP requests from MAPs that are available in its authorization list. Remember to use the MAC address provided at the back of the AP.

MAC authorization for MAPs connected to the controller over Ethernet occurs during the CAPWAP join process. For MAPs that join the controller over radio, MAC authorization takes place when the corresponding AP tries to secure an adaptive wireless path protocol (AWPP) link with the parent MAP. The AWPP is the protocol used in Cisco mesh networks.

The Cisco Catalyst 9800 Series Wireless Controller supports MAC authorization internally as well as using an external AAA server.

Preshared Key Provisioning

Customers with mesh deployments can see their MAPs moving out of their network and joining another mesh network when both these mesh deployments use AAA with wild card MAC filtering to allow the association of MAPs. Since MAPs might use EAP-FAST, this cannot be controlled because a security combination of MAC address and type of AP is used for EAP, and no controlled configuration is available. The preshared key (PSK) option with a default passphrase also presents a security risk.

This issue is prominently seen in overlapping deployments of two service providers when the MAPs are used in a moving vehicle (public transportation, ferry, ship, and so on.). This way, there is no restriction on MAPs to remain with the service providers' mesh network, and MAPs can get hijacked or getting used by another service provider's network and cannot serve the intended customers of the original service providers in the deployment.

The PSK key provisioning feature enables a provisionable PSK functionality from the controller which helps make a controlled mesh deployment and enhance MAPs security beyond the default one. With this feature the MAPs that are configured with a custom PSK, will use the PSK key to do their authentication with their RAPs and controller.

EAP Authentication

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally on the controller. It is designed for use in remote offices that want to maintain connectivity with wireless clients when the backend system gets 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 in turn, removes dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users. Local EAP supports only the EAP-FAST authentication method for MAP authentication between the controller and wireless clients.

Local EAP uses an LDAP server as its backend database to retrieve user credentials for MAP authentication between the controller and wireless clients. 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.

Note If RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if RADIUS servers are not found, timed out, or were not configured.

EAP Authentication with LSC

Locally significant certificate-based (LSC-based) EAP authentication is also supported for MAPs. To use this feature, you should have a public key infrastructure (PKI) to control certification authority, define policies, validity periods, and restrictions and usages on the certificates that are generated, and get these certificates installed on the APs and controller.

After these customer-generated certificates or LSCs are available on the APs and controller, the devices can start using these LSCs, to join, authenticate, and derive a session key.

LSCs do not remove any preexisting certificates from an AP. An AP can have both LSC and manufacturing installed certificates (MIC). However, after an AP is provisioned with an LSC, the MIC certificate is not used during boot-up. A change from an LSC to MIC requires the corresponding AP to reboot.

The controller also supports mesh security with EAP authentication to a designated server in order to:

- Authenticate the mesh child AP
- Generate a master session key (MSK) for packet encryption.

Bridge Group Names

Bridge group names (BGNs) control the association of MAPs to the parent mesh AP. 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 comprising a maximum of 10 characters.

A BGN of *NULL VALUE* is assigned by default during manufacturing. Although not visible to you, it allows a MAP 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 a MAP, it will scan ten times to find a matching BGN parent. After ten scans, if the AP does not find the parent with matching BGN, it will connect to the nonmatched 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.

In Cisco Catalyst 9800 Series Wireless Controller, the BGN is configured on the mesh profile. Whenever a MAP joins the controller, the controller pushes the BGN that is configured on the mesh profile to the AP.

Preferred Parent Selection

The preferred parent for a MAP enables you to enforce a linear topology in a mesh environment. With this feature, you can override the Adaptive Wireless Path Protocol-defined (AWPP-defined) parent selection mechanism and force a MAP to go to a preferred parent.

For Cisco Wave 1 APs, when you configure a preferred parent, ensure that you specify the MAC address of the actual mesh neighbor for the desired parent. This MAC address is the base radio MAC address that has the letter "f" as the final character. For example, if the base radio MAC address is 00:24:13:0f:92:00, then you must specify 00:24:13:0f:92:0f as the preferred parent.

```
Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:0f
```

For Cisco Wave 2 APs, when you configure a preferred parent, the MAC address is the base radio MAC address that has "0x11" added to the last two characters. For example, if the base radio MAC address is 00:24:13:0f:92:00, then you must specify 00:24:13:0f:92:11 as the preferred parent.

```
Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:11
```

Background Scanning

Mesh background scanning improves convergence time, and reliability and stability of parent selection. With the help of the Background Scanning feature, a MAP can find and connect with a better potential parent across channels, and maintain its uplink with the appropriate parent all the time.

When background scanning is disabled, a MAP has to scan all the channels of the regulatory domain after detecting a parent loss in order to find a new parent and go through the authentication process. This delays the time taken for the mesh AP to connect back to the controller.

When background scanning is enabled, a MAP can avoid scanning across the channels to find a parent after detecting a parent loss, and select a parent from the neighbor list and establish the AWPP link.

Mesh Backhaul at 2.4 GHz and 5 GHz

A backhaul is used to create only the wireless connection between MAPs. The backhaul interface is 802.11a/n/ac/g depending upon the AP. The default backhaul interface is 5-GHz. The rate selection is important for effective use of the available radio frequency spectrum. The rate can also affect the throughput of client devices. (Throughput is an important metric used by industry publications to evaluate vendor devices.)

Mesh backhaul is supported at 2.4-GHz and 5-GHz. However, in certain countries it is not allowed to use mesh network with a 5-GHz backhaul network. The 2.4-GHz radio frequencies allow you to achieve much

larger mesh or bridge distances. When a RAP gets a slot-change configuration, it gets propagated from the RAP to all its child MAPs. All the MAPs get disconnected and join the new configured backhaul slot.

Dynamic Frequency Selection

To protect the existing radar services, the regulatory bodies require that devices that have to share the newly opened frequency sub-band behave in accordance with the Dynamic Frequency Selection (DFS) protocol. DFS dictates that in order to be compliant, a radio device must be capable of detecting the presence of radar signals. When a radio detects a radar signal, the radio should stop transmitting for at least 30 minutes to protect that service. The radio should then select a different channel to transmit on, but only after monitoring it. If no radar is detected on the projected channel for at least one minute, the new radio service device can begin transmissions on that channel. The DFS feature allows mesh APs to immediately switch channels when a radar event is detected in any of the mesh APs in a sector.

Country Codes

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

In certain countries, there is a difference in the following for indoor and outdoor APs:

- Regulatory domain code
- Set of channels supported
- Transmit power level

Intrusion Detection System

The Cisco Intrusion Detection System/Intrusion Prevention System (CIDS/CIPS) instructs controllers to block certain clients from accessing a wireless network when attacks involving these clients are detected in Layer 3 through Layer 7. This system offers significant network protection by helping to detect, classify, and stop threats, including worms, spyware or adware, network viruses, and application abuse.

Mesh Interoperability Between Controllers

Interoperability can be maintained between AireOS and the Cisco Catalyst 9800 Series Wireless Controller with the following support:

- MAPs can join an AireOS controller through a mesh network formed by APs connected to a Cisco Catalyst 9800 Series Wireless Controller.
- MAPs can join a Cisco Catalyst 9800 Series Wireless Controller through a mesh network formed by APs connected to as AireOS controller.

- MAP roaming is supported between parent mesh APs connected to AireOS and the Cisco Catalyst 9800 Series Wireless Controller by using PMK cache.

Note For seamless interoperability, AireOS controller and the Cisco Catalyst 9800 Series Wireless Controller should be in the same mobility group and use the image versions that support IRCM.

Information About DHCP and NAT Functionality on Root AP (RAP)

Note This feature is applicable for Cisco Aironet 1542 series outdoor access points only.

The access points associated to a mesh network can play one of the two roles:

- Root Access Point (RAP) - An access point can be a root access point for multiple mesh networks.
- Mesh Access Point (MAP) - An access point can be a mesh access point for only one single mesh network at a time.

DHCP and NAT Functionality on Root AP - IPv4 Scenario

This feature enables the controller to send a TLV to RAP when a new RAP joins the controller.

The following covers the workflow:

- Controller pushes TLV to RAP for enabling DHCP and NAT functionality.
- Client associates to an SSID.
- RAP executes DHCP funtionality to assign private IPv4 address to the client.
- RAP executes NAT functionality to get the private IPv4 address of the client and allow access to the network.

Mesh Convergence

Mesh convergence allows MAPs to reestablish connection with the controller, when it loses backhaul connection with the current parent. To improve the convergence time, each mesh AP maintains a subset of channels that is used for future scan-seek and to identify a parent in the neighbor list subset.

The following convergence methods are supported.

Table 44: Mesh Convergence

Mesh Convergence	Parent Loss Detection / Keepalive Timers
Standard	21 / 3 seconds
Fast	7 / 3 seconds
Very Fast	4 / 2 seconds
Noise-tolerant-fast	21 / 3 seconds

Noise-Tolerant Fast

Noise-tolerant fast detection is based on the failure to get a response for an AWPP neighbor request, which evaluates the current parent every 21 seconds in the standard method. Each neighbor is sent a unicast request every 3 seconds along with a request to the parent. Failure to get a response from the parent initiates either a roam if neighbors are available on the same channel or a full scan for a new parent.

Ethernet Bridging

For security reasons, the Ethernet port on all the MAPs are disabled by default. They can be enabled only by configuring Ethernet bridging on the root and its respective MAP.

Both tagged and untagged packets are supported on secondary Ethernet interfaces.

In a point-to-point bridging scenario, a Cisco Aironet 1500 Series MAP can be used to extend a remote network by using the backhaul radio to bridge multiple segments of a switched network. This is fundamentally a wireless mesh network with one MAP and no WLAN clients. Just as in point-to-multipoint networks, client access can still be provided with Ethernet bridging enabled, although if bridging between buildings, MAP coverage from a high rooftop might not be suitable for client access. To use an Ethernet-bridged application, enable the bridging feature on the RAP and on all the MAPs in that sector.

Ethernet bridging should be enabled for the following scenarios:

- Use mesh nodes as bridges.
- Connect Ethernet devices, such as a video camera on a MAP using its Ethernet port.

Note Ensure that Ethernet bridging is enabled for every parent mesh AP taking the path from the mesh AP to the controller.

In a mesh environment with VLAN support for Ethernet bridging, the secondary Ethernet interfaces on MAPs are assigned a VLAN individually from the controller. All the backhaul bridge links, both wired and wireless, are trunk links with all the VLANs enabled. Non-Ethernet bridged traffic, as well as untagged Ethernet bridged traffic travels along the mesh using the native VLAN of the APs in the mesh. It is similar for all the traffic to and from the wireless clients that the APs are servicing. The VLAN-tagged packets are tunneled through AWPP over wireless backhaul links.

VLAN Tagging for MAP Ethernet Clients

The backhaul interfaces of mesh APs are referred to as primary interfaces, and other interfaces are referred to as secondary interfaces.

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).

Multicast Over Mesh Ethernet Bridging Network

Mesh multicast modes determine how bridging-enabled APs such as MAP and RAP, send multicast packets among Ethernet LANs within a mesh network. Mesh multicast modes manage only non-CAPWAP multicast traffic. CAPWAP multicast traffic is governed by a different mechanism.

Three different mesh multicast modes are available to manage multicast and broadcast packets on all MAPs. When enabled, these modes reduce unnecessary multicast transmissions within the mesh network and conserve backhaul bandwidth.

The three mesh multicast modes are:

- 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 corresponding 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 such multicasts are filtered out.
- In-out mode: The RAP and MAP both multicast but in a different manner.
  - 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.

Radio Resource Management on Mesh

The Radio Resource Management (RRM) software embedded in the controller acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. RRM enables the controller to continually monitor the associated lightweight APs for information on traffic load, interference, noise, coverage, and other nearby APs:

The RRM measurement in the mesh AP backhaul is enabled based on the following conditions:

- Mesh AP has the Root AP role.
- Root AP has joined using Ethernet link.

- Root AP is not serving any child AP.

Air Time Fairness on Mesh

The Air Time Fairness (ATF) on Mesh feature is conceptually similar to the ATF feature for local access points (APs). ATF is a form of wireless quality of service (QoS) that regulates downlink airtime (as opposed to egress bandwidth). Before a frame is transmitted, the ATF budget for that SSID is checked to ensure that there is sufficient airtime budget to transmit the frame. Each SSID can be thought of as having a token bucket (1 token = 1 microsecond of airtime). If the token bucket contains enough airtime to transmit the frame, it is transmitted over air. Otherwise, the frame can either be dropped or deferred. Deferring a frame means that the frame is not admitted into the Access Category Queue (ACQ). Instead, it remains in the Client Priority Queue (CPQ) and transmitted at a later time when the corresponding token bucket contains a sufficient number of tokens (unless the CPQ reaches full capacity, at which point, the frame is dropped). The majority of the work involved in the context of ATF takes place on the APs. The wireless controller is used to configure the ATF on Mesh and display the results.

In a mesh architecture, the mesh APs (parent and child MAPs) in a mesh tree access the same channel on the backhaul radio for mesh connectivity between parent and child MAPs. The root AP is connected by wire to the controller, and MAPs are connected wirelessly to the controller. Hence, all the CAPWAP and Wi-Fi traffic are bridged to the controller through the wireless backhaul radio and through RAP. In terms of physical locations, normally, RAPs are placed at the roof top and MAPs in multiple hops are placed some distance apart from each other based on the mesh network segmentation guidelines. Hence, each MAP in a mesh tree can provide 100 percent of its own radio airtime downstream to its users though each MAP accessing the same medium. Compare this to a nonmesh scenario, where neighboring local-mode unified APs in the arena next to each other in different rooms, serving their respective clients on the same channel, and each AP providing 100% radio airtime downstream. ATF has no control over clients from two different neighboring APs accessing the same medium. Similarly, it is applicable for MAPs in a mesh tree.

For outdoor or indoor mesh APs, ATF must be supported on client access radios that serve regular clients similarly to how it is supported on ATF on nonmesh unified local mode APs to serve the clients. Additionally, it must also be supported on backhaul radios which bridge the traffic to/from the clients on client access radios to RAPs (one hop) or through MAPs to RAPs (multiple hops). It is a bit tricky to support ATF on the backhaul radios using the same SSID/Policy/Weight/Client fair-sharing model. Backhaul radios do not have SSIDs and it always bridge traffic through their hidden backhaul nodes. Therefore, on the backhaul radios in a RAP or a MAP, the radio airtime downstream is shared equally, based on the number of backhaul nodes. This approach provides fairness to users across a wireless mesh network, where clients associated to second-hop MAP can stall the clients associated to first-hop MAP where second-hop MAP is connected wireless to first-hop MAP through backhaul radio even though the Wi-Fi users in the MAPs are separated by a physical location. In a scenario where a backhaul radio has an option to serve normal clients through universal client access feature, ATF places the regular clients into a single node and groups them. It also enforces the airtime by equally sharing the radio airtime downstream, based on the number of nodes (backhaul nodes plus a single node for regular clients).

Spectrum Intelligence for Mesh

The Spectrum Intelligence feature scans for non-Wi-Fi radio interference on 2.4-GHz and 5-GHz bands. The feature supports client serving mode and monitor mode. The Cisco CleanAir technology in mesh backhaul and access radios provides an Interference Device Report (IDR) and Air Quality Index (AQI). Two key mitigation features (Event-Driven Radio Resource Management [EDRRM] and Persistence Device Avoidance

[PDA]) are present in CleanAir. Both rely directly on information that can only be gathered by CleanAir. In the client-access radio band, they work the same way in mesh networks as they do in nonmesh networks in the backhaul radio band, the CleanAir reports are only displayed on the controller. No action is taken through ED-RRM.

Note that no specific configuration options are available to enable or disable CleanAir for MAPs.

For more information about Spectrum Intelligence, see Configuring Spectrum Intelligence, on page 962 section.

Indoor Mesh Interoperability with Outdoor Mesh

Interoperability of indoor MAPs with outdoor APs are supported. This helps to bring coverage from outdoors to indoors. However, we recommend that you use indoor MAPs for indoor use only, and deploy them outdoors only under limited circumstances such as a simple short-haul extension from an indoor WLAN to a hop in a parking lot.

Mobility groups can be shared between outdoor mesh networks and indoor WLAN networks. It is also possible for a single controller to control indoor and outdoor MAPs simultaneously. Not that the same WLANs are broadcast out of both indoor and outdoor MAPs.

Workgroup Bridge

A workgroup bridge (WGB) is used to connect wired networks over a single wireless segment by informing the corresponding MAP 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 (four MAC headers, versus the normal three 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 a packet to and from the corresponding clients.

APs can be configured as workgroup bridges. Only one radio interface is used for controller connectivity, Ethernet interface for wired client connectivity, and other radio interface for wireless client connectivity.

In Cisco Catalyst 9800 Series Wireless Controller, WGB acts as a client association, with the wired clients behind WGB supported for data traffic over the mesh network. Wired clients with different VLANs behind WGB are also supported.

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.

Mesh Daisy Chaining

Mesh APs have the capability to *daisy chain* APs when they function as MAPs. The *daisy chained* MAPs can either operate the APs 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 Mesh AP to the Ethernet port of a MAP, thus extending the network to provide better client access.

Daisy chained APs must be cabled differently depending on how the APs are powered. If an AP is powered using DC power, an Ethernet cable must be connected directly from the LAN port of the Primary AP to the PoE in a port of the Subordinate AP.

The following are the guidelines for the daisy chaining mode:

- Primary MAP should be configured as mesh AP.
- Subordinate MAP should be configured as root AP.
- Daisy chaining should be enabled on both primary and subordinate MAP.
- Ethernet bridging should be enabled on all the APs in the Bridge mode. Enable Ethernet bridging in the mesh profile and map all the bridge mode APs in the sector to the same mesh profile.
- VLAN support should be enabled on the wired root AP, subordinate MAP, and primary MAP along with proper native VLAN configuration.

Mesh Leaf Node

You can configure a 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, thus ensuring that the wireless backhaul performance is not downgraded.

Flex+Bridge Mode

Flex+Bridge mode is used to enable FlexConnect capabilities on mesh (bridge mode) APs. Mesh APs inherit VLANs from the root AP that is connected to it.

Any EWC capable AP in Flex mode connected to a MAP, should be in CAPWAP mode (AP-type CAPWAP).

You can enable or disable VLAN trunking and configure a native VLAN ID on each AP for any of the following modes:

- FlexConnect

- Flex+Bridge (FlexConnect+Mesh)

Backhaul Client Access

When Backhaul Client Access is enabled, it allows wireless client association over the backhaul radio. The backhaul radio can be a 2.4-GHz or 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 performed only over the access radio.

Note Backhaul Client Access is disabled by default. After the Backhaul Client Access is enabled, all the MAPs, except subordinate AP and its child APs in daisy-chained deployment, reboot.

Mesh CAC

The Call Admission Control (CAC) enables a mesh access point to maintain controlled quality of service (QoS) on the controller to manage voice quality on the mesh network. Bandwidth-based, or 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.

- When client roams from one MAP to another in same site, bandwidth availability is checked again in the new tree for the active calls.
- When MAP roams to new parent, the active calls are not terminated and it continues to be active with other active calls in the sub tree.
- High Availability (HA) for MAPs is not supported; calls attached to MAP's access radio are terminated on HA switchover.
- HA for RAP is supported, hence calls attached to RAP's access radio continues to be active in new controller after switchover.
- Mesh CAC algorithm is applicable only for voice calls.
- For Mesh backhaul radio bandwidth calculation, static CAC is applied. Load-based CAC is not used as the APs do not support load-based CAC in Mesh backhaul.
- Calls are allowed based on available bandwidth on a radio. Airtime Fairness (ATF) is not accounted for call admission and the calls that fall under ATF policy are given bandwidth as per ATF weight.

Mesh CAC is not supported for the following scenarios.

- APs in a Mesh tree assigned with different site tags.
- APs in a Mesh tree assigned with the default site tag.

Configuring MAC Authorization (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **AAA Advanced** > **Device Authentication**.

Step 2 Click **Add**.
The **Quick Step: MAC Filtering** window is displayed.

Step 3 In the **Quick Step: MAC Filtering** window, complete the following:
a) Enter the **MAC Address**.
b) Choose the **Attribute List Name** from the drop-down list.
c) Choose the **WLAN Profile Name** from the drop-down list.
d) Click **Apply to Device**.

Step 4 Choose **Configuration** > **Security** > **AAA** > **AAA Method List** > **Authorization**.

Step 5 Click **Add**.
The **Quick Step: AAA Authorization** window is displayed.

Step 6 In the **Quick Step: AAA Authorization** window, complete the following:
a) Enter the **Method List Name**.
b) Choose the **Type** from the drop-down list.
c) Choose the **Group Type** from the drop-down list.
d) Check the **Fallback to Local** check box.
e) Check the **Authenticated** check box.
f) Move the required servers from the **Available Server Groups** to the **Assigned Server Groups.**
g) Click **Apply to Device**.

Step 7 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**.

Step 8 Click the mesh profile.
The **Edit Mesh Profile** window is displayed.

Step 9 Click the **Advanced** tab.

Step 10 In the **Security** settings, from the **Method** drop-down list, choose **EAP**.

Step 11 Choose the **Authentication Method** from the drop-down list.

Step 12 Choose the **Authorization Method** from the drop-down list.

Step 13 Click **Update & Apply to Device**.

Configuring MAC Authorization (CLI)

Follow the procedure given below to add the MAC address of a bridge mode AP to the controller.

Before you begin

- MAC filtering for bridge mode APs are enabled by default on the controller. Therefore, only the MAC address need to be configured. The MAC address that is to be used is the one that is provided at the back of the corresponding AP.
- MAC authorization is supported internally, as well as using an external AAA server.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**username** *user-name* **Example:** `Device(config)# username username1`	Configures user name authentication for MAC filtering where username is MAC address.
Step 3	**aaa authorization credential-download** *method-name* **local** **Example:** `Device(config)# aaa authorization credential-download list1 local`	Sets an authorization method list to use local credentials.
Step 4	**aaa authorization credential-download** *method-name* **radius group** *server-group-name* **Example:** `Device(config)# aaa authorization credential-download auth1 radius group radius-server-1`	Sets an authorization method list to use a RADIUS server group.
Step 5	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 6	**method authorization** *method-name* **Example:** `Device(config-wireless-mesh-profile)# method authorization auth1`	Configures the authorization method for mesh AP authorization.

Configuring MAP Authorization - EAP (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **AAA Method List** > **Device Authentication**.

Step 2 Click **Add**.

Step 3 Enter **Method List Name**.

Step 4 Choose **Type** as dot1x and **Group Type** from the the drop-down lists.

dot1x

Step 5 Check or uncheck the **Fallback to Local** check box.

Step 6 Move the required servers from the **Available Server Groups** to the **Assigned Server Groups.**

Step 7 Click **Apply to Device**.

Step 8 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**.

Step 9 Click the mesh profile. The **Edit Mesh Profile** window is displayed.

Step 10 Choose the **Advanced** tab.

Step 11 In the **Security** settings, from the **Method** drop-down list, choose **EAP**.

Step 12 Choose the options from the **Authentication Method** and **Authorization Method** drop-down lists.

Step 13 Click **Update & Apply to Device**.

Configuring MAP Authorization (CLI)

Select and configure authentication method of EAP/PSK for MAP authentication.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa authentication** *method-name* **radius group** *server-group-name* **Example:** `Device(config)# aaa authentication dot1x auth1 radius group radius-server-1`	For local authentication: `Device(config)# aaa authentication dot1x auth1 local` Sets an authentication method list to use a RADIUS server group. This is required for EAP authentication.
Step 3	**wireless profile mesh** *profile--name* **local** **Example:**	Sets an authorization method list to use local credentials.

	Command or Action	Purpose
	`Device(config)# wireless profile mesh mesh1`	
Step 4	**security eap** *server-group-name* **Example:** `Device(config-wireless-mesh-profile)# security eap / psk`	Configures the mesh security EAP/PSK for mesh AP.
Step 5	**method authentication** *method-name* **Example:** `Device(config-wireless-mesh-profile)# method authentication auth1`	Configures the authentication method for mesh AP authentication.

Configuring PSK Provisioning (CLI)

When PSK provisioning is enabled, the APs join with default PSK initially. After that PSK provisioning key is set, the configured key is pushed to the newly joined AP.

Follow the procedure given below to configure a PSK:

Before you begin

The provisioned PSK should have been pushed to all the APs that are configured with PSK as mesh security.

Note

- PSKs are saved across reboots in the controller as well as on the corresponding mesh AP.
- A controller can have total of five PSKs and one default PSK.
- A mesh AP deletes its provisioned PSK only on factory reset.
- A mesh AP never uses the default PSK after receiving the first provisioned PSK.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mesh security psk provisioning** **Example:** `Device(config)# wireless mesh security psk provisioning`	Configures the security method for wireless as PSK. **Note** The provisioned PSK is pushed only to those APs that are configured with PSK as the mesh security method.

	Command or Action	Purpose
Step 3	**wireless mesh security psk provisioning key** *index* {**0** | **8**} *pre-shared-key description* **Example:** `Device(config)# wireless mesh security psk provisioning key 1 0 secret secret-key`	Configures a new PSK for mesh APs.
Step 4	**wireless mesh security psk provisioning default-psk** **Example:** `Device(config)# wireless mesh security psk provisioning default-psk`	Enables default PSK-based authentication.
Step 5	**wireless mesh security psk provisioning inuse** *index* **Example:** `Device(config)# wireless mesh security psk provisioning inuse 1`	Specifies the PSK to be actively used. **Note** You should explicitly set the in-use key index in the global configuration pointing to the PSK index.

Configuring a Bridge Group Name (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Click **Add**.

Step 3 In the **Advanced** tab, under the **Bridge Group** settings, enter the **Bridge Group Name**.

Step 4 Click **Apply to Device**.

Configuring a Bridge Group Name (CLI)

- If a bridge group name (BGN) is configured on a mesh profile, whenever a MAP joins the controller, it pushes the BGN configured on the mesh profile to the AP.
- Whenever a mesh AP moves from AireOS controller to the Cisco Catalyst 9800 Series Wireless Controller, the BGN configured on the mesh profile is pushed to that AP and stored there.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**bridge-group name** *bridge-grp-name* **Example:** `Device(config-wireless-mesh-profile)# bridge-group name bgn1`	Configures a bridge group name.

Configuring Background Scanning (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Choose a profile.

Step 3 In **General** tab, check the **Background Scanning** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Background Scanning

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.

	Command or Action	Purpose
Step 3	**background-scanning** **Example:** `Device(config-wireless-mesh-profile)# background-scanning`	Configures background scanning in mesh deployments.

Configuring Backhaul Client Access (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Choose a profile.

Step 3 In **General** tab, check the **Backhaul Client Access** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Backhaul Client Access (CLI)

Note Backhaul client access is disabled by default. After it is enabled, all the MAPs, except subordinate AP and its child APs in daisy-chained deployment, reboot.

Follow the procedure given below to enable backhaul client access on a mesh profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**client-access** **Example:** `Device(config-wireless-mesh-profile)# client-access`	Configures backhaul with client access AP.

Configuring Wireless Backhaul Data Rate (CLI)

Backhaul is used to create a wireless connection between APs. A backhaul interface can be 802.11bg/a/n/ac depending on the AP. The rate selection provides for effective use of the available RF spectrum. Data rates can also affect the RF coverage and network performance. Lower data rates, for example, 6 Mbps, can extend farther from the AP than can have higher data rates, for example, 1300 Mbps. As a result, the data rate affects cell coverage, and consequently, the number of APs required.

Note You can configure backhaul data rate, preferably, through the mesh profile. In certain cases, where a specific data rate is needed, use the command to configure the data rate per AP.

Follow the procedure given below to configure wireless backhaul data rate in privileged EXEC mode or in mesh profile configuration mode.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **mesh backhaul rate** {**auto** | **dot11abg** | **dot11ac** |**dot11n**} **Example:** `Device# #ap name ap1 mesh backhaul rate auto`	Configures backhaul transmission rate.
Step 3	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 4	**backhaul rate dot11** {**24ghz** | **5ghz**}**dot11n RATE_6M** **Example:** `Device(config-wireless-mesh-profile)# backhaul rate dot11 5ghz dot11n mcs 31`	Configures backhaul transmission rate. **Note** Note that the rate configured on the AP (step 2) should match with the rate configured on the mesh profile (step4).

Configuring Dynamic Frequency Selection (CLI)

DFS specifies the types of radar waveforms that should be detected along with certain timers for an unlicensed operation in the DFS channel.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**full-sector-dfs** **Example:** `Device(config-wireless-mesh-profile)# full-sector-dfs`	Enables DFS. **Note** 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. The coordinated channel change is always enabled for Cisco Wave 2 and the later versions. The coordinated channel change can be disabled only for Cisco Wave 1 APs.

Configuring the Intrusion Detection System (CLI)

When enabled, the intrusion detection system generates reports for all the traffic on the client access. However, this is not applicable for the backhaul traffic.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**ids** **Example:**	Configures intrusion detection system reporting for mesh APs.

	Command or Action	Purpose
	`Device(config-wireless-mesh-profile)# ids`	

Configuring Ethernet Bridging (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Click **Add**.

Step 3 In **General** tab, enter the **Name** of the mesh profile.

Step 4 In **Advanced** tab, check the **Ethernet Bridging** check box.

Step 5 Click **Apply to Device**.

Configuring Ethernet Bridging (CLI)

The Ethernet port on the MAPs are disabled by default. It can be enabled only by configuring Ethernet bridging on the Root AP and the other respective MAPs.

Ethernet bridging can be enabled for the following scenarios:

- To use the mesh nodes as bridges.
- To connect Ethernet devices, such as a video camera, on a MAP using the MAP's Ethernet port.

Before you begin

- Ensure that you configure the following commands under the mesh profile configuration for Ethernet bridging to be enabled:
  - **ethernet-bridging**: Enables the Ethernet Bridging feature on an AP.
  - **no ethernet-vlan-transparent**: Makes the wireless mesh bridge VLAN aware. Allows VLAN filtering with the following AP command: **[no] mesh ethernet** {**0** | **1** | **2** | **3**} **mode trunk vlan allowed**.

Note If you wish to have all the VLANs bridged (where bridge acts like a piece of wire), then you must enable VLAN transparency, which allows all VLANS to pass. If you choose to use VLAN transparent mode, it is best to filter the VLANS on the wired side of the network to avoid unnecessary traffic from flooding the network.

- The switch port to which the Root AP is connected should be configured as the trunk port for Ethernet bridging to work.
- For Bridge mode APs, use the **ap name** *name-of-rap* **mesh vlan-trunking native** *vlan-id* command to configure a trunk VLAN on the corresponding RAP. The Ethernet Bridging feature will not be enabled on the AP without configuring this command.
- For Flex+Brigde APs, configure the native VLAN ID under the corresponding flex profile.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**ap name** *ap-name* **mesh ethernet** {**0** | **1** | **2** | **3**}**mode access** *vlan-id* **Example:** `Device# ap name ap1 mesh ethernet 1 mode access 21`	Configures the Ethernet port of the AP and sets the mode as trunk.
Step 3	**ap name** *ap-name* **mesh ethernet** {**0** | **1** | **2** | **3**}**mode trunk vlan** *vlan-id* **Example:** `Device# ap name ap1 mesh ethernet 1 mode trunk vlan native 21`	Sets the native VLAN for the trunk port.
Step 4	**ap name** *ap-name* **mesh ethernet** {**0** | **1** | **2** | **3**}**mode trunk vlan allowed** *vlan-id* **Example:** `Device# ap name ap1 mesh ethernet 1 mode trunk vlan allowed 21`	Configures the allowed VLANs for the trunk port. Permits VLAN filtering on an ethernet port of any Mesh or Root Access Point. Active only when VLAN transparency is disabled in the mesh profile.

Configuring Multicast Modes over Mesh

- If multicast packets are received at a MAP over Ethernet, they are sent to the RAP. However, they are not sent to other MAPs. 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.
- The *in-out* mode is the default mode. When this *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.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**multicast** {**in-only** | **in-out** | **regular**} **Example:** `Device(config-wireless-mesh-profile)# multicast regular`	Configures mesh multicast mode.

Configuring RRM on Mesh Backhaul (CLI)

The RRM measurement in the mesh AP backhaul is enabled based on the following conditions:

- Mesh AP has the Root AP role.
- Root AP has joined using an Ethernet link.
- Root AP is not serving any child AP.

Follow the procedure given below to enable RRM in the mesh backhaul:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mesh backhaul rrm** **Example:** `Device(config)# wireless mesh backhaul rrm`	Configures RRM on the mesh backhaul.

Selecting a Preferred Parent (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 Click the Access Point.

Step 3 In the **Mesh** tab, enter the **Preferred Parent MAC**.

Step 4 Click **Update & Apply to Device**.

Selecting a Preferred Parent (CLI)

Follow the procedure given below to configure a preferred parent for a MAP.

Using this mechanism, you can override the AWPP-defined parent selection mechanism and force a mesh AP to go to a preferred parent.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **mesh parent preferred** *mac-address* **Example:**	Configures mesh parameters for the AP and sets the mesh-preferred parent MAC address.

	Command or Action	Purpose

	`Device# ap name ap1 mesh parent preferred 00:0d:ed:dd:25:8F`	**Note** Ensure that you use the radio MAC address of the preferred parent.
		For Cisco Wave 1 APs, when you configure a preferred parent, ensure that you specify the MAC address of the actual mesh neighbor for the desired parent. This MAC address is the base radio MAC address that has the letter "f" as the final character. For example, if the base radio MAC address is 00:24:13:0f:92:00, then you must specify 00:24:13:0f:92:0f as the preferred parent.
		`Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:0f`
		For Cisco Wave 2 APs, when you configure a preferred parent, the MAC address is the base radio MAC address that has "0x11" added to the last two characters. For example, if the base radio MAC address is 00:24:13:0f:92:00, then you must specify 00:24:13:0f:92:11 as the preferred parent.
		`Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:11`

Changing the Role of an AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 Click the **Access Point**.

Step 3 In the **Mesh** tab, choose **Root** or **Mesh** from the **Role** drop-down list.

Step 4 Click **Update & Apply to Device**.

After the role change is triggered, the AP reboots.

Changing the Role of an AP (CLI)

Follow the procedure to change the AP from MAP to RAP or vice-versa.

By default, APs join the controller in a mesh AP role.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **role** {**mesh-ap** | **root-ap**} **Example:** `Device# #ap name ap1 root-ap`	Changes the role for the Cisco bridge mode APs. After the role change is triggered, the AP reboots.

Configuring the Mesh Leaf Node (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **mesh block-child** **Example:** `Device# #ap name ap1 mesh block-child`	Sets the AP to work only as a leaf node. This AP cannot be selected by other MAPs as a parent MAP. **Note** Use the **no** form of this command to change it to a regular AP.

Configuring the Mesh Leaf Node (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 Click the Access Point.

Step 3 In the **Mesh** tab, check the **Block Child** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Subset Channel Synchronization

All the channels used by all the RAPs in a controller are sent to all the MAPs for future seek and convergence. The controller keeps a list of the subset channels for each Bridge Group Name (BGN). The list of subset channels are also shared across all the controllers in a mobility group.

Subset channel list is list of channels where RAP of particular BGN are operating. This list is communicated to all the MAPs within and across the controllers. The idea of subset channel list is for faster convergence of the Mesh APs. Convergence method can be selected in mesh profile. If the convergence method is not standard then subset channel list is pushed to MAPs.

Follow the procedure given below to configure subset channel synchronization for mobility group.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mesh subset-channel-sync mac** **Example:** `Device(config)# wireless mesh subset-channel-sync`	Configures subset channel synchronization for a mobility group.

Provisioning LSC for Bridge-Mode and Mesh APs (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **LSC Provision**.

Step 2 In the **Add APs to LSC Provision List** settings, click the **Select File** option to upload a CSV file that contains AP details.

Step 3 Click **Upload File**.

Step 4 You can also use the **AP MAC Address** field to search for APs using the MAC address and add them. The APs added to the provision list are displayed in the **APs in Provision List** list.

Step 5 Click **Apply**.

Step 6 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 7 Click **Add**.

Step 8 In the **General** tab, enter the **Name** of the mesh profile and check the **LSC** check box.

Step 9 In the **Advanced** tab, under the **Security** settings, choose the authorization method from the **Authorization Method** drop-down list.

Step 10 Click **Apply to Device**.

Provisioning LSC for Bridge-Mode and Mesh APs

- Configuring Locally Significant Certificate (LSC) will not remove pre-existing certificates from an AP.
- An AP can have both LSC and Message Integrity Check (MIC) certificates. However, when an AP is provisioned with LSC, the MIC certificate is not used on boot-up. A change from LSC to MIC requires the AP to reboot.

Follow the procedure given below to configure LSC for bridge-mode and mesh APs:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision** **Example:** `Device(config)# ap lsc-provision`	Configures LSC provisioning on an AP. **Note** This step is applicable only for mesh APs.
Step 3	**ap lsc-provision provision-list** **Example:** `Device(config)# ap lsc-provision provision-list`	(Optional) Configures LSC provision for all the APs in the provision list.
Step 4	**aaa authentication dot1x** *auth-list* **radius group** *radius-server-grp* **Example:** `Device(config)# aaa authentication dot1x list1 radius group sg1`	Configures named authorization list for downloading EAP credential from radius group server.
Step 5	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 6	**lsc-only-auth** **Example:** `Device(config-wireless-mesh-profile)# lsc-only-auth`	Configures mesh security to LSC-only MAP authentication. After this command is run, all the mesh APs reboot.

	Command or Action	Purpose
Step 7	**method authorization** *local* **Example:** `Device(config-wireless-mesh-profile)# method authorization list1`	Configures an authorization method for mesh AP authorization.

Specifying the Backhaul Slot for the Root AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Click **Add**.

Step 3 In **General** tab, enter the **Name** of the mesh profile.

Step 4 In **Advanced** tab, choose the rate types from the **Rate Types** drop-down list for **5 GHz Band Backhaul** and **2.4 GHz Band Backhaul**.

Step 5 Click **Apply to Device**.

Specifying the Backhaul Slot for the Root AP (CLI)

Follow the procedure given below to set the mesh backhaul rate.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *rap-name* **mesh backhaul radio dot11**{**24ghz** | **5ghz**} [**slot** *slot-id*] **Example:** `Device# ap name rap1 mesh backhaul radio dot11 24ghz slot 2`	Sets the mesh backhaul radio slot.

Using a Link Test on Mesh Backhaul (GUI)

Procedure

Step 1 Choose **Monitoring** > **Wireless** > **AP Statistics** > **General**.

Step 2 Click the Access Point.

Step 3 Choose **Mesh** > **Neighbor** > **Linktest**.

Step 4 Choose the desired values from the **Date Rates**, **Packets to be sent (per second)**, **Packet Size (bytes)** and **Test Duration (seconds)** drop-down lists..

Step 5 Click **Start**.

Using a Link Test on Mesh Backhaul

Follow the procedure given below to trigger linktest between neighbor mesh APs.

Note Use the **test mesh linktest mac-address** *neighbor-ap-mac* **rate** *data-rate* **fps** *frames-per-second* **frame-size** *frame-size* command to perform link test from an AP.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **mesh linktest** *dest-ap-mac data-rate packet-per-sec packet-size test-duration* **Example:** `Device# #ap name ap1 mesh linktest F866.F267.7DFB 24 234 1200 200`	Sets link test parameters.

Configuring Battery State for Mesh AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Choose a profile.

Step 3 In **General** tab, check the **Battery State for an AP** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Battery State for Mesh AP

Some Cisco outdoor APs come with the option of battery backup. There is also a POE-out port that can power a video surveillance camera. The integrated battery can be used for temporary backup power during external power interruptions.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**battery-state** **Example:** `Device(config-wireless-mesh-profile)# battery-state`	Configures the battery state for an AP.

Configuring DHCP Server on Root Access Point (RAP)

Procedure

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

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures an AP Profile.
Step 3	**dhcp-server** **Example:** `Device(config-ap-profile)# dhcp-server`	Configures DHCP server on the root access point.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Saves the configuration and exits configuration mode and returns to privileged **EXEC** mode.

Configuring Mesh CAC (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mesh cac** **Example:** `Device(config)# wireless mesh cac`	Enables mesh CAC mode.

Configuring Fast Teardown for a Mesh AP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters the mesh profile configuration mode.

	Command or Action	Purpose
Step 3	**fast-teardown** **Example:** `Device(config-wireless-mesh-profile)# fast-teardown`	Enables the fast teardown of mesh network and configures the feature's parameter.
Step 4	**enabled** **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# enabled`	Enables the fast teardown feature.
Step 5	**interval** *duration* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# interval 5`	(Optional) Configures the retry interval. The valid values range between 1 and 10 seconds.
Step 6	**latency-exceeded-threshold** *duration* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# latency-exceeded-threshold 20`	(Optional) Specifies the latency interval at which at least one ping must succeed in less than threshold time. The valid values range between 1 and 30 seconds.
Step 7	**latency-threshold** *threshold range* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# latency-threshold 20`	(Optional) Speficies the latency threshold. The valid values range between 1 and 500 milliseconds.
Step 8	**retries** *retry limit* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# retries 1`	(Optional) Specifies the number of retries until the gateway is considered unreachable. The valid values range between 1 and 10.
Step 9	**uplink-recovery-intervals** *recovery interval* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# uplink-recovery-intervals 1`	(Optional) Specifies the time during which root access point uplink has to be stable to accept child connections. The valid values range between 1 and 3600 seconds.

Verifying DHCP Server for Root AP Configuration

To verify the DHCP server for root AP configuration, use the following command:

```
Device# show ap config general
Cisco AP Name   : AP4C77.6DF2.D588
================================================
<SNIP>
Dhcp Server                                     : Enabled
```

Verifying Mesh Configuration

Use the following **show** commands to verify the various aspects of mesh configuration.

- **show wireless mesh stats** *ap-name*
- **show wireless mesh security-stats** {*all* | *ap-name*}
- **show wireless mesh queue-stats** {*all* | *ap-name*}
- **show wireless mesh per-stats summary** {*all* | *ap-name*}
- **show wireless mesh neighbor summary** {*all* | *ap-name*}
- **show wireless mesh neighbor detail** *ap-name*
- **show wireless mesh ap summary**
- **show wireless mesh ap tree**
- **show wireless mesh ap backhaul**
- **show wireless mesh config**
- **show wireless mesh convergence detail** *bridge-group-name*
- **show wireless mesh convergence subset-channels**
- **show wireless mesh neighbor**
- **show wireless profile mesh detailed** *mesh-profile-name*
- **show wireless stats mesh security**
- **show wireless stats mesh queue**
- **show wireless stats mesh packet error**
- **show wireless mesh ap summary**
- **show ap name** *ap-name* **mesh backhaul**
- **show ap name** *ap-name* **mesh neighbor detail**
- **show ap name** *ap-name* **mesh path**
- **show ap name** *ap-name* **mesh stats packet error**
- **show ap name** *ap-name* **mesh stats queue**
- **show ap name** *ap-name* **mesh stats security**
- **show ap name** *ap-name* **mesh stats**
- **show ap name** *ap-name* **mesh bhrate**
- **show ap name** *ap-name* **config ethernet**
- **show ap name** *ap-name* **cablemodem**
- **show ap name** *ap-name* **environment**

- **show ap name** *ap-name* **gps location**
- **show ap name** *ap-name* **environment**
- **show ap name** *ap-name* **mesh linktest data** *dest-mac*
- **show ap environment**
- **show ap gps location**

For details about these commands, see the Cisco Catalyst 9800 Series Wireless Controller Command Reference document.

MAC Authorization

Use the following **show** command to verify the MAC authorization configuration:

```
Device# show run aaa
aaa authentication dot1x CENTRAL_LOCAL local
aaa authorization credential-download CENTRAL_AUTHOR local
username 002cc8de4f31 mac
username 00425a0a53b1 mac

ewlc_eft#sh wireless profile mesh detailed madhu-mesh-profile

Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abbc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
...
Battery State                 : ENABLED
Authorization Method          : CENTRAL_AUTHOR
Authentication Method         : CENTRAL_LOCAL
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

PSK Provisioning

Use the following **show** command to verify PSK provisioning configuration:

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                  : ENABLED
  Mesh CAC                                      : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)   : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed       : ENABLED
  Rap Channel Sync                              : ENABLED

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
  Parent Change Number                          :  3

Mesh PSK Config
  PSK Provisioning                              : ENABLED
  Default PSK                                   : ENABLED
```

```
PSK In-use key number                          : 1
Provisioned PSKs(Maximum 5)

Index    Description
------   ------------
1         key1
```

Bridge Group Name

Use the following **show** command to verify the bridge group name configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
Full Sector DFS               : ENABLED
IDS                           : ENABLED
Multicast Mode                : In-Out
Range in feet                 : 12000
Security Mode                 : EAP
Convergence Method            : Fast
LSC only Authentication       : DISABLED
Battery State                 : ENABLED
Authorization Method          : CENTRAL_AUTHOR
Authentication Method         : CENTRAL_LOCAL
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

Backhaul Client Access

Use the following **show** command to verify the backhaul client access configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
...
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

Wireless Backhaul Data Rate

Use the following **show** command to verify the wireless backhaul data rate configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
```

```
Description                     :
Bridge Group Name               : bgn-abc
Strict match BGN                : ENABLED
...
Authorization Method            : CENTRAL_AUTHOR
Authentication Method           : CENTRAL_LOCAL
Backhaul tx rate(802.11bg)      : auto
Backhaul tx rate(802.11a)       : 802.11n mcs15
```

Dynamic Frequency Selection

Use the following **show** command to verify the dynamic frequency selection configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name               : abc-mesh-profile
-------------------------------------------------
Description                     :
Bridge Group Name               : bgn-abc
Strict match BGN                : ENABLED
Amsdu                           : ENABLED
Background Scan                 : ENABLED
Channel Change Notification     : DISABLED
Backhaul client access          : ENABLED
Ethernet Bridging               : ENABLED
Ethernet Vlan Transparent       : DISABLED
Full Sector DFS                 : ENABLED
...
Backhaul tx rate(802.11a)       : 802.11n mcs15
```

Intrusion Detection System

Use the following **show** command to verify the wireless backhaul data rate configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name               : abc-mesh-profile
-------------------------------------------------
Description                     :
Bridge Group Name               : bgn-abc
Strict match BGN                : ENABLED
Amsdu                           : ENABLED
Background Scan                 : ENABLED
Channel Change Notification     : DISABLED
Backhaul client access          : ENABLED
Ethernet Bridging               : ENABLED
Ethernet Vlan Transparent       : DISABLED
Full Sector DFS                 : ENABLED
IDS                             : ENABLED
Multicast Mode                  : In-Out
...
Backhaul tx rate(802.11a)       : 802.11n mcs15
```

Ethernet Bridging

Use the following **show** command to verify ethernet bridging configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name               : abc-mesh-profile
-------------------------------------------------
Description                     :
Bridge Group Name               : bgn-abc
Strict match BGN                : ENABLED
Amsdu                           : ENABLED
Background Scan                 : ENABLED
```

```
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
Full Sector DFS               : ENABLED
IDS                           : ENABLED
Multicast Mode                : In-Out
...
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

Multicast over Mesh

Use the following **show** command to verify multicast over Mesh configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
Full Sector DFS               : ENABLED
IDS                           : ENABLED
Multicast Mode                : In-Out
...
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

RRM on Mesh Backhaul

Use the following **show** command to verify RRM on Mesh backhaul configuration:

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                  : ENABLED
  Mesh CAC                                      : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)   : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed       : ENABLED
  Rap Channel Sync                              : ENABLED

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
  Parent Change Number                          :  3

Mesh PSK Config
  PSK Provisioning                              : ENABLED
  Default PSK                                   : ENABLED
  PSK In-use key number                         : 1
  Provisioned PSKs(Maximum 5)

  Index    Description
  ------   ------------
  1         key1
```

Preferred Parent Selection

Use the following **show** command to verify preferred parent configuration:

```
Device# show wireless mesh ap tree
=========================================================================
AP Name [Hop Ctr,Link SNR,BG Name,Channel,Pref Parent,Chan Util,Clients]
=========================================================================

[Sector 1]
-----------
1542-RAP [0, 0, bgn-madhu, (165), 0000.0000.0000, 1%, 0]
   |-MAP-2700 [1, 67, bgn-madhu, (165), 7070.8b7a.6fb8, 0%, 0]

Number of Bridge APs : 2
Number of RAPs : 1
Number of MAPs : 1

(*)  Wait for 3 minutes to update or Ethernet Connected Mesh AP.
(**) Not in this Controller
```

AP Role Change

Use the following **show** command to verify AP role change configuration:

```
Device# show wireless mesh ap summary
AP Name                          AP Model BVI MAC        BGN        AP Role
-------                          -------- -------        ---        -------
1542-RAP                         1542D    002c.c8de.1338 bgn-abc  Root AP
MAP-2700                         2702I    500f.8095.01e4 bgn-abc  Mesh AP

Number of Bridge APs         :   2
Number of RAPs               :   1
Number of MAPs               :   1
Number of Flex+Bridge APs    :   0
Number of Flex+Bridge RAPs   :   0
Number of Flex+Bridge MAPs   :   0
```

Mesh Leaf Node

Use the following **show** command to verify mesh leaf node configuration:

```
Device# show ap name MAP-2700 config general
Cisco AP Name   : MAP-2700
=================================================

Cisco AP Identifier                             : 7070.8bbc.d3e0
Country Code                                    : Multiple Countries : IN,US,IO,J4
Regulatory Domain Allowed by Country            : 802.11bg:-AEJPQU   802.11a:-ABDJNPQU
AP Country Code                                 : IN  - India
AP Regulatory Domain
  Slot 0                                        : -A
  Slot 1                                        : -D
MAC Address                                     : 500f.8095.01e4
...
AP Mode                                         : Bridge
Mesh profile name                               : abc-mesh-profile
AP Role                                         : Mesh AP
Backhaul radio type                             : 802.11a
Backhaul slot id                                : 1
Backhaul tx rate                                : auto
Ethernet Bridging                               : Enabled
Daisy Chaining                                  : Disabled
```

```
Strict Daisy Rap                                  : Disabled
Bridge Group Name                                 : bgn-abc
Strict-Matching BGN                               : Enabled
Preferred Parent Address                          : 7070.8b7a.6fb8
Block child state                                 : Disabled
PSK Key Timestamp                                 : Not Configured
...
FIPS status                                       : Disabled
WLANCC status                                     : Disabled
GAS rate limit Admin status                       : Disabled
WPA3 Capability                                   : Disabled
EWC-AP Capability                                  : Disabled
AWIPS Capability                                  : Disabled
Proxy Hostname                                    : Not Configured
Proxy Port                                        : Not Configured
Proxy NO_PROXY list                               : Not Configured
GRPC server status                                : Disabled
```

Subset Channel Synchronization

Use the following **show** command to verify the subset channel synchronization configuration:

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                    : ENABLED
  Mesh CAC                                        : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)     : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed         : ENABLED
  Rap Channel Sync                                : ENABLED

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
  Parent Change Number                            :  3

Mesh PSK Config
  PSK Provisioning                                : ENABLED
  Default PSK                                     : ENABLED
  PSK In-use key number                           : 1
  Provisioned PSKs(Maximum 5)

  Index    Description
  ------   ------------
  1         key1
```

Provisioning LSC for Bridge-Mode and Mesh APs

Use the following **show** command to verify the provisioning LSC for Bridge-Mode and Mesh AP configuration:

```
Device# show wireless profile mesh detailed default-mesh-profile
Mesh Profile Name             : default-mesh-profile
-------------------------------------------------
Description                   : default mesh profile
Bridge Group Name             : bgn-abc
Strict match BGN              : DISABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : ENABLED
Backhaul client access        : ENABLED
```

```
Ethernet Bridging             : DISABLED
Ethernet Vlan Transparent     : ENABLED
Full Sector DFS               : ENABLED
IDS                           : DISABLED
Multicast Mode                : In-Out
Range in feet                 : 12000
Security Mode                 : EAP
Convergence Method            : Fast
LSC only Authentication       : DISABLED
Battery State                 : ENABLED
Authorization Method          : default
Authentication Method         : default
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : auto
```

Specify the Backhaul Slot for the Root AP

Use the following **show** command to verify the backhaul slot for the Root AP configuration:

```
Device# show ap name 1542-RAP mesh backhaul
MAC Address : 380e.4d85.5e60
  Current Backhaul Slot: 1
  Radio Type: 0
  Radio Subband: All
  Mesh Radio Role: DOWNLINK
  Administrative State: Enabled
  Operation State: Up
  Current Tx Power Level:
  Current Channel: (165)
  Antenna Type: N/A
  Internal Antenna Gain (in .5 dBm units): 18
```

Using a Link Test on Mesh Backhaul

Use the following **show** command to verify the use of link test on mesh backhaul configuration:

```
Device# show ap name 1542-RAP mesh linktest data 7070.8bbc.d3ef
380e.4d85.5e60 ==> 7070.8bbc.d3ef

Started at : 05/11/2020 20:56:28
Status: In progress

Configuration:
==============
Data rate:  Mbps
Packets per sec: : 234
Packet Size: : 1200
Duration: : 200
```

Mesh CAC

Use the following **show** command to verify mesh CAC configuration:

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                  : ENABLED
  Mesh CAC                                      : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)   : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed       : ENABLED
  Rap Channel Sync                              : ENABLED

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
  Parent Change Number                          :  3

Mesh PSK Config
  PSK Provisioning                              : ENABLED
  Default PSK                                   : ENABLED
  PSK In-use key number                         : 1
  Provisioned PSKs(Maximum 5)

  Index    Description
  ------   ------------
  1         key1
```

PART XIII

VideoStream

- VideoStream, on page 1015

CHAPTER 103

VideoStream

- Information about Media Stream, on page 1015
- Prerequisites for Media Stream, on page 1015
- How to Configure Media Stream, on page 1016
- Monitoring Media Streams, on page 1021
- Configuring the General Parameters for a Media Stream (GUI), on page 1021
- Adding Media Stream (CLI), on page 1022
- Enabling a Media Stream per WLAN (GUI), on page 1023
- Enabling a Media Stream per WLAN (CLI), on page 1023
- Configuring the General Parameters for a Media Stream (GUI), on page 1024
- Configuring the General Parameters for a Media Stream (CLI), on page 1024
- Configuring Multicast Direct Admission Control (GUI), on page 1025
- Configuring Multicast Direct Admission Control (CLI), on page 1025
- Create and Attach Policy-based QoS Profile, on page 1027
- Viewing Media Stream Information, on page 1032

Information about Media Stream

The IEEE 802.11 wireless multicast delivery mechanism does not provide a reliable way to acknowledge lost or corrupted packets. As a result, if any multicast packet is lost in the air, it is not sent again which may cause an IP multicast stream unviewable.

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

Prerequisites for Media Stream

- Make sure that the Multicast feature is enabled. We recommend that you configure IP multicast on the controller in multicast-multicast mode.
- Check for the IP address on the client machine. The machine should have an IP address from the respective VLAN.
- Verify that the access points have joined the controllers .

How to Configure Media Stream

Configuring Multicast-Direct Globally for Media Stream (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless multicast** **Example:** `Device(config)# wireless multicast`	Enables multicast for wireless forwarding.
Step 3	**ip igmp snooping** **Example:** `Device(config)# ip igmp snooping`	Enables IGMP snooping on a per-VLAN basis. If the global setting is disabled, then all the VLANs are treated as disabled, whether they are enabled or not.
Step 4	**ip igmp snooping querier** **Example:** `Device(config)# ip igmp snooping querier`	Enables a snooping querier on an interface when there is no multicast router in the VLAN to generate queries.
Step 5	**wireless media-stream multicast-direct** **Example:** `(config)#wireless media-stream multicast-direct`	Configures the global multicast-direct on the controller.

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

Step 7	**wireless media-stream group** *name startIp endIp* **Example:**	Configures each media stream and its parameters such as expected multicast destination addresses, stream bandwidth consumption, and stream-priority parameters.

	Command or Action	Purpose
	(config)#**wireless media-stream group grp1 231.1.1.1 239.1.1.3** avg-packet-size Configure average packet size default Set a command to its defaults exit Exit sub-mode max-bandwidth Configure maximum expected stream bandwidth in Kbps no Negate a command or set its defaults policy Configure media stream admission policy priority Configure media stream priority, <1:Lowest - 8:Highest> qos Configure over the air QoS class, <'video'> ONLY rrc-evaluation Configure RRC re-evaluation admission violation Configure stream violation policy on periodic re-evaluation	
Step 8	**end** **Example:** Device(config)# **end**	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Media Stream for 802.11 Bands (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** } **media-stream multicast-direct** **Example:** Device(config)#**ap dot11 24ghz media-stream multicast-direct**	Configures whether media stream (multicast to unicast) is allowed for the 802.11 band. You must disable to 802.11 network to enable the mediastream.
Step 3	**ap dot11** {**24ghz** | **5ghz** } **media-stream video-redirect** **Example:** Device(config)#**ap dot11 24ghz media-stream video-redirect**	Optional. Configures the redirection of unicast video traffic to the best-effort queue.

	Command or Action	Purpose
Step 4	**ap dot11** {**24ghz** | **5ghz** } **media-stream multicast-direct admission-besteffort** **Example:** `Device(config)#ap dot11 24ghz media-stream multicast-direct admission-besteffort`	Configures the media stream to be sent through the best-effort queue if that media stream cannot be prioritized due to bandwidth-availability limitations. Run the **no** form of the command to drop the stream, if the media stream cannot be prioritized due to bandwidth-availability limitations.
Step 5	**ap dot11** {**24ghz** | **5ghz** } **media-stream multicast-direct client-maximum** *value* **Example:** `Device(config)#ap dot11 24ghz media-stream multicast-direct client-max 15`	Configures the maximum number of allowed media streams per individual client. The maximum is 15 and the default is 0. The value of 0 denotes unlimited streams.
Step 6	**ap dot11** {**24ghz** | **5ghz** } **media-stream multicast-direct radio-maximum** *value* **Example:** `Device(config)#ap dot11 24ghz media-stream multicast-direct radio-maximum 20`	Configures maximum number of radio streams. The valid range is from 1 to 20. Default is 0. The value of 0 denotes unlimited streams.
Step 7	**ap dot11** {**24ghz** | **5ghz** } **cac multimedia max-bandwidth** *bandwidth* **Example:** `Device(config)#ap dot11 24ghz cac multimedia max-bandwidth 60`	Configures maximum media (voice + video) bandwidth, in percent. The range is between 5-85%.
Step 8	**ap dot11** {**24ghz** | **5ghz** } **cac media-stream multicast-direct min-client-rate** *dot11_rate* **Example:** `Device(config)#ap dot11 24ghz cac media-stream multicast-direct min_client_rate`	Configures the minimum PHY rate needed for a client to send a media stream as unicast. Clients communicating below this rate will not receive the media stream as a unicast flow. Typically, this PHY rate is equal to or higher than the rate at which multicast frames are sent.
Step 9	**ap dot11** {**24ghz** | **5ghz** } **cac media-stream** **Example:** `Device(config)#ap dot11 5ghz cac media-stream`	Configures Call Admission Control (CAC) parameters for media stream access category.
Step 10	**ap dot11** {**24ghz** | **5ghz** } **cac multimedia** **Example:** `Device(config)#ap dot11 5ghz cac multimedia`	Configures CAC parameters for media access category: used for voice and video.
Step 11	**ap dot11** {**24ghz** | **5ghz** } **cac voice** **Example:** `Device(config)#ap dot11 5ghz cac voice`	Configures CAC parameters for voice access category.

	Command or Action	Purpose
Step 12	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a WLAN to Stream Video(GUI)

Procedure

Step 1 Choose **Configuration > Wireless > WLANs > Wireless Networks**.
Step 2 Select a **WLAN** to view the **Edit WLAN** window.
Step 3 Click **Advanced** tab.
Step 4 Check the **Media Stream Multicast-Direct** check box to enable the feature.
Step 5 Click **Update & Apply to Device**.

Configuring a WLAN to Stream Video (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan_name* **Example:** `(config)#wlan wlan50`	Enters WLAN configuration mode.
Step 3	**shutdown** **Example:** `(config-wlan)#shutdown`	Disables the WLAN for configuring its parameters.
Step 4	**media-stream multicast-direct** **Example:** `(config)#media-stream multicast-direct`	Configures the multicast-direct on media stream for the WLAN.
Step 5	**no shutdown** **Example:** `(config-wlan)#no shutdown`	Enables the WLAN.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Deleting a Media Stream (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Media Stream**.

Step 2 Click the **Streams** tab.

Step 3 Check the checkbox adjecent to the Stream Name you want to delete.

To delete multiple streams, select multiple stream name checkboxes.

Step 4 Click **Delete**.

Step 5 Click **Yes** on the confirmation window to delete the VLAN.

Deleting a Media Stream (CLI)

Before you begin

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

Procedure

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

Monitoring Media Streams

Table 45: Commands for monitoring media streams

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

Configuring the General Parameters for a Media Stream (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Media Stream**.

Step 2 In the **General** tab, check the **Multicast Direct Enable** check box.

Step 3 In the **Session Message Config** section, check the **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.

Step 4 In the **Session Announcement URL** field, enter the URL where the client can find more information when an error occurs during the multicast media stream transmission.

Step 5 In the **Session Announcement Email** field, enter the e-mail address of the person who can be contacted.

Step 6 In the **Session Announcement Phone** field, enter the phone number of the person who can be contacted.

Step 7 In the **Session Announcement Note** field, enter a reason as to why a particular client cannot be served with a multicast media.

Step 8 Click **Apply**.

Adding Media Stream (CLI)

Procedure

	Command or Action	Purpose
Step 1	**wireless media-stream group** *groupName startIpAddr endIpAddr* **Example:** `Device(config)# wireless media-stream group group1 224.0.0.0 224.0.0.223`	Configures each media stream and its parameters, such as expected multicast destination addresses, stream bandwidth consumption , and stream priority parameters.
Step 2	**avg-packet-size** *packetsize* **Example:** `Device(media-stream)# avg-packet-size 100`	Configures the average packet size.
Step 3	**max-bandwidth** *bandwidth* **Example:** `Device(media-stream)# max-bandwidth 80`	Configures the maximum expected stream bandwidth, in Kbps.
Step 4	**policy** { **admit** | **deny** } **Example:** `Device(media-stream)# policy admit`	Configure the media stream admission policy.
Step 5	**qos video** **Example:** `Device(media-stream)# qos video`	Configures over-the-air QoS class, as 'video'.
Step 6	**violation** { **drop** | **fallback** } **Example:** `Device(media-stream)# violation drop`	Configures the violation mode.
Step 7	**rrc-evaluation** { **initial** | **periodic** } **Example:** `Device(media-stream)# rrc-evaluation initial`	Configure Resource Reservation Control (RRC) re-evaluation admission, which provides initial or periodic admission evaluation. The re-evaluation admission occurs at 2, 4,8, and so on seconds.
Step 8	**priority** *priority-value* **Example:** `Device(media-stream)# priority 6`	Sets the priority value. The valid range is from 1-8, with 1 being the lowest.

Enabling a Media Stream per WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **WLANs** page, click the name of the **WLAN** or click **Add** to create a new one.

Step 3 In the **Add/Edit WLAN** window that is displayed, click the **Advanced** tab.

Step 4 Check the **Enabling a Media Stream for each WLAN** check box to enable Media Stream on the WLAN.

Step 5 Save the configuration.

Enabling a Media Stream per WLAN (CLI)

Follow the procedure given below to enable a media stream for each WLAN:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan_name* **Example:** `Device(config)# wlan wlan5`	Enters WLAN configuration mode.
Step 3	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Disables the WLAN for configuring its parameters.
Step 4	**media-stream multicast-direct** **Example:** `Device(config-wlan)# media-stream multicast-direct`	Configures multicast-direct for the WLAN.
Step 5	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring the General Parameters for a Media Stream (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Media Stream**.

Step 2 Check the **Multicast Direct Enable** check box to enable multicast direct globally on the local mode.

Step 3 In the **Session Message Config** section, enter the values for the following parameters

- Session Announcement URL
- Session Announcement Email
- Session Announcement Phone
- Session Announcement Note

Step 4 Save the configuration.

Configuring the General Parameters for a Media Stream (CLI)

Follow the procedure given below to configure the general parameters for a media stream:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless media-stream message** { **URL** *url* | **email** *email-address* | **phone** *phone-no* | **notes** *notes* } **Example:** `Device(config)# wireless media-stream message url www.xyz.com`	Configures various message configuration parameters, such as phone, URL, email, and notes.
Step 3	**wireless media-stream multicast-direct** **Example:** `Device(config)# wireless media-stream multicast-direct`	Enables multicast direct globally for local mode. **Note** This configuration will not impact flex and fabric media-stream configurations.
Step 4	**exit** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config)# exit`	

Configuring Multicast Direct Admission Control (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Media Stream**.

Step 2 Check the **Media Stream Admission Control (ACM)** check box to enable multicast direct admission control.

Step 3 In the **Maximum Media Stream RF bandwidth (%)** field, enter the percentage of the maximum bandwidth to be allocated for media applications on this radio band. Valid range is from 5 to 85. When the client reaches a specified value, the AP rejects new calls on this radio band.

Step 4 In the **Maximum Media Bandwidth (%)** field, enter the bandwidth. Valid range is from 5 to 85%.

Step 5 From the **Client Minimum Phy Rate** drop-down list, select the minimum transmission data rate or the rate in kilobits per second at which the client can operate. If the transmission data rate is below the physical 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.

Step 6 In the **Maximum Retry Percent (%)** field, 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.

Step 7 Click **Apply**.

Configuring Multicast Direct Admission Control (CLI)

Follow the procedure given below to configure multicast direct admission control:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** } **shutdown** **Example:** `Device(config)# ap dot11 24ghz shutdown`	Disables the 802.11 network.
Step 3	**ap dot11** {**24ghz** | **5ghz** } **media-stream video-redirect** **Example:**	Configures the redirection of the unicast video traffic to best-effort queue.

	Command or Action	Purpose
	`Device(config)# ap dot11 24ghz media-stream video-redirect`	
Step 4	**ap dot11** {**24ghz** | **5ghz** } **cac media-stream acm** **Example:** `Device(config)# ap dot11 24ghz cac media-stream acm`	Enables admission control on the media-stream access category.
Step 5	**ap dot11** {**24ghz** | **5ghz** } **cac media-stream max-bandwidth** *bandwidth* **Example:** `Device(config)# ap dot11 24ghz cac media-stream max-bandwidth 65`	Configures the maximum media bandwidth, in percent. The range is between 5-85%.
Step 6	**ap dot11** {**24ghz** | **5ghz** } **cac multimedia max-bandwidth** *bandwidth* **Example:** `Device(config)# ap dot11 24ghz cac multimedia max-bandwidth 65`	Configures the maximum bandwidth allocated to Wi-Fi Multimedia (WMM) clients for media. The range is between 5-85%.
Step 7	**ap dot11** {**24ghz** | **5ghz** } **cac media-stream multicast-direct min-client-rate** *dot11Rate* **Example:** `Device(config)# ap dot11 24ghz cac media-stream multicast-direct min-client-rate 800`	Configures the minimum PHY rate needed for a client to receive media stream as unicast. Clients communicating below this rate will not receive the media stream as a unicast flow. Typically, this PHY rate is equal to or higher than the rate at which multicast frames are sent.
Step 8	**ap dot11** {**24ghz** | **5ghz** } **cac media-stream multicast-direct max-retry-percent** *retryPercent* **Example:** `Device(config)# ap dot11 24ghz cac media-stream multicast-direct max-retry-percent 50`	Configures CAC parameter maximum retry percent for multicast-direct streams.
Step 9	**ap dot11** {**24ghz** | **5ghz** } **media-stream multicast-direct radio-maximum** *value* **Example:** `Device(config)# ap dot11 24ghz media-stream multicast-direct radio-maximum 10`	Configures the maximum number of radio streams. The range is from 1 to 20. Default is 0. Value 0 denotes unlimited streams.
Step 10	**ap dot11** {**24ghz** | **5ghz** } **media-stream multicast-direct client-maximum** *value* **Example:** `Device(config)# ap dot11 24ghz media-stream multicast-direct client-maximum 12`	Configures the maximum number of allowed media streams per individual client. The maximum is 15 and the default is 0. Value 0 denotes unlimited streams.

	Command or Action	Purpose
Step 11	**ap dot11** {**24ghz** | **5ghz** } **media-stream multicast-direct admission-besteffort** **Example:** `Device(config)# ap dot11 24ghz media-stream multicast-direct admission-besteffort`	Configures the media stream to still be sent through the best effort queue if a media stream cannot be prioritized due to bandwidth availability limitations. Add **no** in the command to drop the stream if the media stream cannot be prioritized due to bandwidth availability limitations.
Step 12	**no ap dot11** {**24ghz** | **5ghz** } **shutdown** **Example:** `Device(config)# no ap dot11 24ghz shutdown`	Enables the 802.11 network.

Create and Attach Policy-based QoS Profile

The high-level steps to create and attach policy-based QoS profile are as follows:

1. Create a QoS Profile
2. Create a Service Template
3. Map the Service Template to the Policy Map
4. Map the Policy Map to the Policy Profile

Create a QoS Profile (GUI)

Procedure

Step 1 Click **Configuration** > **Services** > **QoS**.
Step 2 Click **Add** to create a new QoS Policy.
Step 3 Enter a **Policy Name**.
Step 4 Enter a **Description** for the policy.
Step 5 In the **Class Default** section, choose a value in the **Mark** drop-down list.
Step 6 Enter the **Police(kbps)** value.
Step 7 Click **Apply to Device**.

Create a QoS Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map** *policy-map-name* **Example:** `Device(config)# policy-map QoS_Drop_Youtube`	Creates a policy map.
Step 3	**description** *description* **Example:** `Device(config-pmap)# description QoS_Drop_Youtube`	Adds a description to the policy map.
Step 4	**class** *class-map-name* **Example:** `Device(config-pmap)# class QoS_Drop_Youtube1_AVC_UI_CLASS`	Creates a policy criteria.
Step 5	**police cir** *committ-information-rate* **Example:** `Device(config-pmap-c)# police cir 8000`	Polices the provided committed information rate.
Step 6	**conform-action drop** **Example:** `Device(config-pmap-c-police)# conform-action drop`	Configures the action when the rate is less than the conform burst.
Step 7	**exceed-action drop** **Example:** `Device(config-pmap-c-police)# exceed-action drop`	Configures the action when the rate is within the conform and conform plus exceed burst.
Step 8	**end** **Example:** `Device(config-pmap-c-police)# end`	Returns to privileged EXEC mode.

Create a Service Template (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Local Policy**.

Step 2 On the **Local Policy** page, **Service Template** tab, click **Add**.

Step 3 In the **Create Service Template** window, enter the following parameters:

- **Service Template Name:** Enter a name for the template.
- **VLAN ID:** Enter the VLAN ID for the template. Valid range is between 1 and 4094.
- **Session Timeout (secs):** Sets the timeout duration for the template. Valid range is between 1 and 65535.
- **Access Control List:** Choose the Access Control List from the drop-down list.
- **Ingress QOS:** Choose the input QoS policy for the client from the drop-down list
- **Egress QOS:** Choose the output QoS policy for the client from the drop-down list.

Step 4 Click **Apply to Device**.

Create a Service Template (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**service-template** *template-name* **Example:** `Device(config)# service-template qos-template`	Configures the service-template or identity policy.
Step 3	**vlan** *vlan-id* **Example:** `Device(config-service-template)# vlan 87`	Specifies VLAN ID.
Step 4	**absolute-timer** *timer* **Example:** `Device(config-service-template)# absolute-timer 3600`	Specifies session timeout value for a service template.

	Command or Action	Purpose
Step 5	**service-policy qos input** *qos-policy* **Example:** `Device(config-service-template)# service-policy qos input QoS_Drop_Youtube`	Configures an input QoS policy for the client.
Step 6	**service-policy qos output** *qos-policy* **Example:** `Device(config-service-template)# service-policy qos output QoS_Drop_Youtube`	Configures an output QoS policy for the client.
Step 7	**end** **Example:** `Device(config-service-template)# end`	Returns to privileged EXEC mode.

Map the Service Template to the Policy Map (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, select the **Policy Profile** to be mapped.

Step 3 In the **Edit Policy Profile** window, click **Access Policies** tab.

Step 4 Use the **Local Subscriber Policy Name** drop-down list to select the policy name.

Step 5 Click **Update & Apply to Device**.

Map the Service Template to the Policy Map (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type subscriber attribute-to-service** *parameter-map-name* **Example:** `Device(config)# parameter-map type subscriber attribute-to-service QoS-Policy_Map-param`	Specifies the parameter map type and name.

	Command or Action	Purpose
Step 3	*map-index* **map device-type eq** *filter-name* **user-role eq** *user-name* **Example:** `Device(config-parameter-map-filter)# 1 map device-type eq "Android" user-role eq "student"`	Specifies the parameter map attribute filter criteria. Multiple filters are used in the example provided here.
Step 4	*map-index* **service-template** *service-template-name* **precedence** *precedence-num* **Example:** `Device(config-parameter-map-filter-submode)# 1 service-template Qos_template`	Specifies the service template.
Step 5	**end** **Example:** `Device(config-parameter-map-filter-submode)# end`	Returns to privileged EXEC mode.
Step 6	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 7	**policy-map type control subscriber** *policy-map-name* **Example:** `Device(config)# policy-map type control subscriber QoS-Policy_Map`	Specifies the policy map type.
Step 8	**event identity-update match-all** **Example:** `Device(config-event-control-policymap)# event identity-update match-all`	Specifies the match criteria to the policy map.
Step 9	*class-num* **class always do-until-failure** **Example:** `Device(config-event-control-policymap)# 1 class always do-until-failure`	Applies a class-map with a service-template.
Step 10	*action-index* **map attribute-to-service table** *parameter-map-name* **Example:** `Device(config-event-control-policymap)# 1 map attribute-to-service table QoS-Policy_Map-param`	Applies a parameter map.

Map the Policy Map (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Local Policy** > **Policy Map** tab.
Step 2 Click **Add**.
Step 3 Enter a name in the **Policy Map Name** text field.
Step 4 Click **Add** to add the matching criteria information.
Step 5 Choose the service template from the **Service Template** drop-down list.
Step 6 Choose the filters from **Device Type**, **User Role**, **User Name**, **OUI** and **MAC Address** drop-down lists.
Step 7 Click **Add Criteria**
Step 8 Click **Apply to Device**.

Map the Policy Map (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan-policy-profile-name* **Example:** `Device(config)# wireless profile policy test-policy-profile`	Configures a wireless policy profile.
Step 3	**description** *profile-policy-description* **Example:** `Device(config-wireless-policy)# description "test policy profile"`	Adds a description for the policy profile.
Step 4	**subscriber-policy-name** *policy-name* **Example:** `Device(config-wireless-policy)# subscriber-policy-name QoS-Policy_Map`	Configures the subscriber policy name.

Viewing Media Stream Information

Use the following **show** commands to view the media stream information.

To view media stream general information and status, use the following commands:

```
Device# show wireless media-stream multicast-direct state

Multicast-direct State..... : enabled
Allowed WLANs:
WLAN-Name                                              WLAN-ID
-------------------------------------------------------------
zsetup_mc                                              1
vwlc-mc_mo                                             3
mcuc_test1                                             4
mcuc_test2                                             5


Device# show wireless media-stream group summary


Number of Groups:: 4

Stream Name          Start IP                End IP            Status
------------------------------------------------------------------------------
new2                 231.2.2.3               231.2.4.4         Enabled
my234                234.0.0.0               234.10.10.10      Enabled
uttest2              235.1.1.20              235.1.1.25        Enabled
uttest3              235.1.1.40              235.1.1.200       Enabled
```

To view the details of a particular media stream, use the **show wireless media-stream client detail** *media_stream_name* command:

```
Device# show wireless media-stream group detail uttest2


Media Stream Name         : uttest2
Start IP Address          : 235.1.1.20
End IP Address            : 235.1.1.25
RRC Parameters:
 Avg Packet Size(Bytes)   : 1200
 Expected Bandwidth(Kbps) : 1000
 Policy                   : Admitted
 RRC re-evaluation        : Initial
 QoS                      : video
 Status                   : Multicast-direct
 Usage Priority           : 4
 Violation                : Drop
```

To view RRC information for a dot11 band, use the **show ap dot11** {**24ghz** | **5ghz** } **mediastream rrc**command:

```
Device# show  ap dot11 5ghz media-stream rrc

Multicast-direct                : Enabled
Best Effort                     : Disabled
Video Re-Direct                 : Disabled
Max Allowed Streams Per Radio   : Auto
Max Allowed Streams Per Client  : 5
Max Media-Stream Bandwidth      : 5
Max Voice Bandwidth             : 50
Max Media Bandwidth             : 43
Min PHY Rate (Kbps)             : 6000
Max Retry Percentage            : 5
```

To view session announcement message details, use the **show wireless media-stream message details** command:

```
Device# show wireless media-stream message details
URL          :
Email        : abc@cisc
Phone        :
Note         :
State        : Disabled
```

To view the list of clients in the blocked list database, use the **show ip igmp snooping igmpv2-tracking** command:

```
Device# show ip igmp snooping igmpv2-tracking

Client to SGV mappings
----------------------
Client: 10.10.10.215 Port: Ca1
 Group: 239.255.255.250 Vlan: 10 Source: 0.0.0.0 blacklisted: no
 Group: 234.5.6.7 Vlan: 10 Source: 0.0.0.0 blacklisted: no
 Group: 234.5.6.8 Vlan: 10 Source: 0.0.0.0 blacklisted: no
 Group: 234.5.6.9 Vlan: 10 Source: 0.0.0.0 blacklisted: no

Client: 10.10.101.177 Port: Ca2
 Group: 235.1.1.14 Vlan: 10 Source: 0.0.0.0 blacklisted: no
 Group: 235.1.1.16 Vlan: 10 Source: 0.0.0.0 blacklisted: no
 Group: 235.1.1.18 Vlan: 10 Source: 0.0.0.0 blacklisted: no

SGV to Client mappings
----------------------
Group: 234.5.6.7 Source: 0.0.0.0 Vlan: 10
 Client: 10.10.10.215 Port: Ca1 Blacklisted: no
```

To view wireless client summary, use the **show wireless media-stream client summary** command:

```
Device# show wireless media-stream client summary
```

To view details of a specific wireless media stream, use the **show wireless media-stream client detail**command:

```
Device# show wireless media-stream client detail uttest2

Media Stream Name         : uttest2
Start IP Address          : 235.1.1.20
End IP Address            : 235.1.1.25
RRC Parameters:
 Avg Packet Size(Bytes)   : 1200
 Expected Bandwidth(Kbps) : 1000
 Policy                   : Admitted
 RRC re-evaluation        : Initial
 QoS                      : video
 Status                   : Multicast-direct
 Usage Priority           : 4
 Violation                : Drop
```

PART XIV

Software-Defined Access Wireless

- Software-Defined Access Wireless, on page 1037
- Passive Client, on page 1045
- Encrypted Traffic Analytics, on page 1053

CHAPTER 104

Software-Defined Access Wireless

- Information to Software-Defined Access Wireless, on page 1037
- Configuring SD-Access Wireless, on page 1040
- Verifying SD-Access Wireless, on page 1044

Information 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.

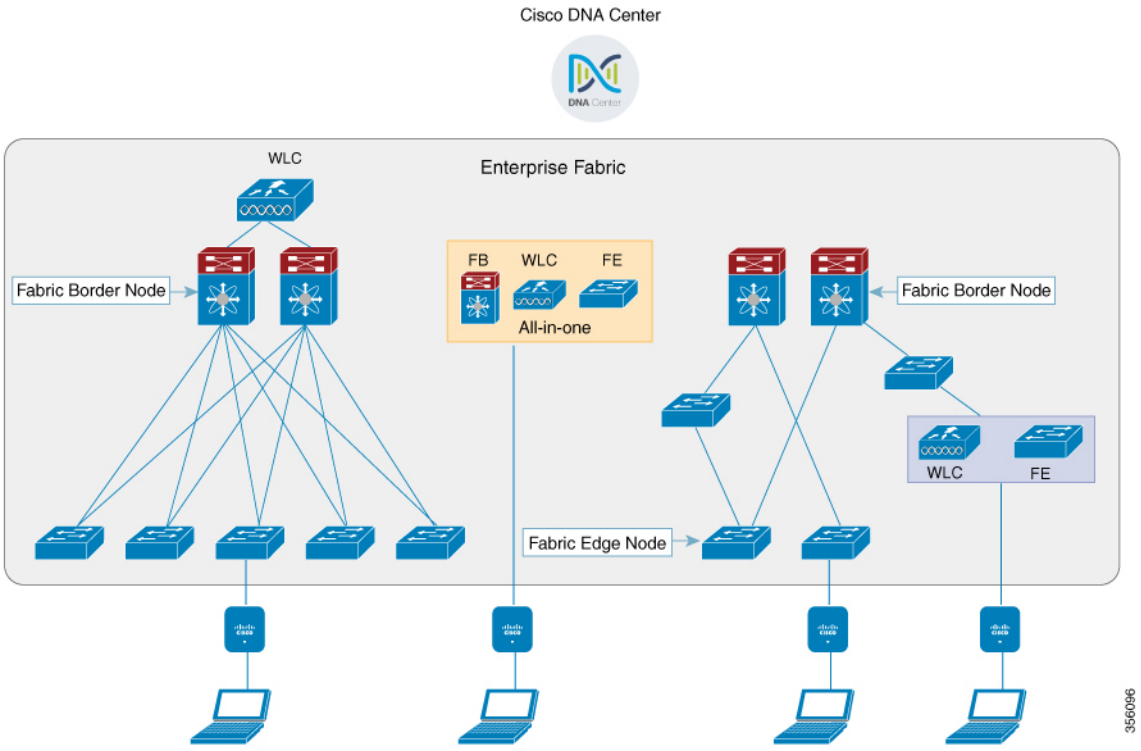
Enterprise fabric is a network topology where traffic is passed through inter-connected switches, while providing the abstraction of a single Layer 2 or Layer 3 device. This provides seamless connectivity, with policy application and enforcement at the edge of the fabric. Fabric uses IP overlay, which 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 Catalyst Center, and Host Tracking Database (HDB).

Figure 25: 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 Cat 9K 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 Cat 9K 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 Cat 9K switch. This toplogy is depicted in the right-most part of the figure.

Cisco Catalyst Center: Is an open, software-driven architecture built on a set of design principles with the objective of configuring and managing Cisco Catalyst 9800 Series Wireless Controllers.

Control Plane: 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

Note Role co-location between wireless controller and fabric edge is supported.

Platform Support

Table 46: Supported Platforms for Software-Defined Access Wireless

Platforms	Support
Catalyst 9300	Yes
Catalyst 9400	Yes
Catalyst 9500H	Yes
Cisco Catalyst 9800 Series Wireless Controller for Cloud	Yes
Cisco Catalyst 9800-40 Series Wireless Controller	Yes
Cisco Catalyst 9800-80 Series Wireless Controller	Yes

Table 47: Multi-Instance Support

Multi-instance	Support
Multiple LISP sessions	Yes

Multi-instance	Support
Emulated database support	Yes
Client roaming between WNCd instances	Yes

Table 48: Feature Support

Feature	Support
Inter-WLC roam for IRCM	Only L2 mobility is supported as VLAN is stretched across the fabric.
DNS-IPv4-ACL	• ACLs are enforced at AP. • Controller needs to push the DNS-ACL information to AP.
IPv6 ACL for clients	Yes. Open, 802.11x, WebbAuth, PSK WLANs, IPv6 address visibility are also supported.
Location tracking/Hyperlocation	Yes
Multicast Video-Stream (IPv4)	Yes
Smart Licensing	Yes

Table 49: Outdoor Access Points Support

AP	Support
1542	Yes
1560	Yes

Configuring SD-Access Wireless

- To enable SD-Access wireless globally, you need to run the **wireless fabric** configuration command.
- During SD-Access Wireless provisioning, ensure that L2-VNID value is unique.

Configuring Default Map Server (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless Plus** > **Fabric** > **Fabric Configuration**.

Step 2 In the **Map Server** section, specify the IP address and preshared key details for Server 1.

Step 3 Optionally, you can specify the IP address and preshared key details for Server 2.

Step 4 Click **Apply**.

Configuring Default Map Server (CLI)

Follow the procedure given below to configure default map server:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless fabric control-plane** *map-server-name* **Example:** `Device(config)# wireless fabric control-plane map-server-name`	Configures the default map server. Here, *map-server-name* defines a pair of map servers.
Step 3	**ip address** *ip-address* **key** *user_password reenter_password* **Example:** `Device(config-wireless-cp)# ip address 200.0.0.0 key user-password user-password`	Configures IP address for the default map server.
Step 4	**end** **Example:** `Device(config-wireless-cp)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring SD-Access Wireless Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Fabric**.

Step 2 On the **Fabric** page, click the **Profiles** tab and click **Add**.

Step 3 In the **Add New Profile** window that is displayed, specify the following parameters:

- Profile name
- Description
- L2 VNID; valid range is between 0 and 16777215
- SGT tag; valid range is between 2 and 65519

Step 4 Click **Save & Apply to Device**.

Configuring SD-Access Wireless Profile (CLI)

Follow the procedure given below to configure SD-Access wireless profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless profile fabric** *fabric-profile-name* **Example:** `Device(config)# wireless profile fabric fabric-profile-name`	Configures the SD-Access wireless profile parameters.
Step 3	**sgt-tag** *sgt* **Example:** `Device(config-wireless-fabric)# sgt-tag 2`	Configures SGT tag. Here, *sgt* refers to the sgt tag value. The valid range is from 2-65519. The default value is 0.
Step 4	**client-l2-vnid** *client-l2-vnid* **Example:** `Device(config-wireless-fabric)# client-l2-vnid client-l2-vnid`	Configures client L2-VNID. Here, *client-l2-vnid* refers to the client L2-VNID value. The valid range is from 0-16777215.
Step 5	**end** **Example:** `Device(config-wireless-fabric)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Map Server in Site Tag (GUI)

Before you begin

Ensure that you have configured a control plane at the time of configuring Wireless Fabric.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 On the **Manage Tags** page, click the **Site** tab.

Step 3 Click the name of the site tag.

Step 4 In the **Edit Site Tag** window, choose the Fabric control plane name from the **Control Plane Name** drop-down list.

Step 5 Save the configuration.

Configuring Map Server in Site Tag (CLI)

Follow the procedure given below to configure map server in site tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless tag site** *site-tag* **Example:** `Device(config)# wireless tag site default-site-tag`	Configures site tag. Here, *site-tag* refers to the site tag name.
Step 3	**fabric control-plane** *map-server-name* **Example:** `Device(config-site-tag)# fabric control-plane map-server-name`	Configures fabric control plane details. Here, *map-server-name* refers to the fabric control plane name associated with the site tag.
Step 4	**end** **Example:** `Device(config-site-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Map Server per L2-VNID (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Fabric**.

Step 2 On the **Fabric Configuration** page in the **Fabric VNID Mapping** section, click **Add**.

Step 3 In the **Add Client and AP VNID** window, specify a name for the Fabric, L2 VNID value (valid range is from 0 to 4294967295), control plane name.

Step 4 Save the configuration.

Configuring Map Server per L2-VNID (CLI)

Follow the procedure given below to configure map server in site tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless fabric name** *name* **l2-vnid** *l2-vnid-value* **l3-vnid** *l3-vnid-value* **ip** *network-ip subnet-mask* **control-plane-name** *control-plane-name* **Example:** `Device(config)# wireless fabric name fabric_name l2-vnid 2 l3-vnid 2 ip 122.220.234.0 255.255.0.0 control-plane-name sample-control-plane`	Configures the map server to the VNID map table. • *name* refers to the fabric name. • *l2-vnid-value* refers to the L2 VNID value. The valid range is from 0 to 16777215. • *L3-vnid-value* refers to the L3 VNID value. The valid range is from 0 to 16777215. • *control-plane-name* refers to the control plane name.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying SD-Access Wireless

You can verify the SD-Access wireless configurations using the following commands:

Table 50: Commands for Verifying SD-Access Wireless

Commands	Description
show wireless fabric summary	Displays the fabric status.
show wireless fabric vnid mapping	Displays all the VNID mapping details.
show wireless profile fabric detailed *fabric_profile_name*	Displays the details of a given fabric profile name.
show ap name *AP_name* **config general**	Displays the general details of the Cisco AP.
show wireless client mac *MAC_addr* **detail**	Displays the detailed information for a client by MAC address.
show wireless tag site detailed *site_tag*	Displays the detailed parameters for a site tag.

CHAPTER 105

Passive Client

- Information About Passive Clients, on page 1045
- Enabling Passive Client on WLAN Policy Profile (GUI), on page 1046
- Enabling Passive Client on WLAN Policy Profile (CLI), on page 1046
- Enabling ARP Broadcast on VLAN (GUI), on page 1046
- Enabling ARP Broadcast on VLAN (CLI), on page 1047
- Configuring Passive Client in Fabric Deployment, on page 1047
- Verifying Passive Client Configuration, on page 1051

Information About Passive Clients

Passive Clients are wireless devices, such as printers and devices configured using a static IP address. Such clients do no transmit any IP information after associating to an AP. That is why, the controller does not learn their IP address unless they perform the DHCP process.

In the controller, the clients just show up in the **Learn IP** state and get timed out because of the DHCP policy-timeout.

The Passive Client feature can be enabled on a per WLAN basis. Enabling this feature will change a few default behaviors in order to better accommodate passive clients. These changes include :

- No client will ever timeout in the IP_LEARN phase. The controller will keep on waiting to learn their IP address. Note that the idle timeout remains active and will delete the client entry after the timeout period expiry, if the client remains silent all along.
- ARP coming from the wired side is broadcasted to all the APs, if the controller does not know the client IP address, to ensure that it reaches the passive client. After this, the controller learns the client IP from the ARP response.

Note Passive client feature is not supported on FlexConnect local switching mode.

Enabling Passive Client on WLAN Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy** page, click **Add** to open the **Add Policy Profile** page.

Step 2 In the **General** tab, use the slider to enable **Passive Client**.

Step 3 Click **Save & Apply to Device**.

Enabling Passive Client on WLAN Policy Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**[no] passive-client** **Example:** `Device(config-wireless-policy)# [no] passive-client`	Enables Passive Client.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.

Enabling ARP Broadcast on VLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Layer2** > **VLAN** page, click **VLAN** tab.

Step 2 Click **Add** to view the **Create VLAN** window.

Step 3 Use the slider to enable **ARP Broadcast**.

Step 4 Click **Save & Apply to Device**.

Enabling ARP Broadcast on VLAN (CLI)

Note ARP Broadcast feature is not supported on VLAN groups.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**vlan configuration** *vlan-id* **Example:** `Device(config)# vlan configuration 1`	Configures a VLAN or a collection of VLANs and enters VLAN configuration mode.
Step 3	**[no] arp broadcast** **Example:** `Device(config-vlan)# [no] arp broadcast`	Enables ARP broadcast on VLAN.
Step 4	**end** **Example:** `Device(config-vlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Passive Client in Fabric Deployment

You need to enable the following for passive client feature to work:

- ARP broadcast on VLANs
- LISP multicast. For information on LISP multicast, see:

  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-lisp-multicast.html

For information on LISP (Locator ID Separation Protocol), see:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-cfg-lisp.html

Enabling Broadcast Underlay on VLAN

Note You can perform the following configuration tasks from Fabric Edge Node only and not from your controller.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `FabricEdge# configure terminal`	Enters global configuration mode.
Step 2	**router lisp** **Example:** `FabricEdge(config)# router lisp`	Enters LISP configuration mode.
Step 3	**instance-id** *instance* **Example:** `FabricEdge(config-router-lisp)# instance-id 3`	Creates a LISP EID instance to group multiple services. Configurations under this instance-id are applicable to all services underneath it.
Step 4	**service ipv4** **Example:** `FabricEdge(config-router-lisp-instance)# service ipv4`	Enables Layer 3 network services for the IPv4 address family and enters the service submode.
Step 5	**database-mapping** *eid* **locator-set** *RLOC name* **Example:** `FabricEdge(config-router-lisp-instance-dynamic-eid)# database-mapping 66.66.66.64/32 locator-set rloc1`	Configures EID to RLOC mapping relationship.
Step 6	**map-cache** *destination-eid* **map-request** **Example:** `FabricEdge(config-router-lisp-instance-service)# map-cache 0.0.0.0/0 map-request`	Generates a static map request for the destination EID.
Step 7	**exit-service-ipv4** **Example:** `FabricEdge(config-router-lisp-instance-service)# exit-service-ipv4`	Exits service submode.
Step 8	**exit-instance-id** **Example:**	Exits instance submode.

	Command or Action	Purpose
	`FabricEdge(config-router-lisp-instance)# exit-instance-id`	
Step 9	**instance-id** *instance* **Example:** `FabricEdge(config-router-lisp)# instance-id 101`	Creates a LISP EID instance to group multiple services.
Step 10	**service ethernet** **Example:** `FabricEdge(config-router-lisp-instance)# service ethernet`	Enables Layer 2 network services and enters service submode.
Step 11	**eid-table vlan** *vlan-number* **Example:** `FabricEdge(config-router-lisp-instance-service)# eid-table vlan 101`	Associates the LISP instance-id configured earlier with a VLAN through which the endpoint identifier address space is reachable.
Step 12	**broadcast-underlay** *multicast-group* **Example:** `FabricEdge(config-router-lisp-instance-service)# broadcast-underlay 239.0.0.1`	Specifies the multicast group used by the underlay to carry the overlay Layer 2 broadcast traffic.
Step 13	**exit-service-ethernet** **Example:** `FabricEdge(config-router-lisp-instance-service)# exit-service-ethernet`	Exits service sub mode.
Step 14	**exit-instance-id** **Example:** `FabricEdge(config-router-lisp-instance)# exit-instance-id`	Exits instance sub mode.

Enabling ARP Flooding

Note You can perform the following configuration tasks from Fabric Edge Node only and not from your controller.

Procedure

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

	Command or Action	Purpose
Step 2	**router lisp** **Example:** `FabricEdge(config)# router lisp`	Enters LISP configuration mode.
Step 3	**instance-id** *instance* **Example:** `FabricEdge(config-router-lisp)# instance-id 3`	Creates a LISP EID instance to group multiple services. Configurations under this instance-id are applicable to all services underneath it.
Step 4	**service ipv4** **Example:** `FabricEdge(config-router-lisp-instance)# service ipv4`	Enables Layer 3 network services for the IPv4 address family and enters the service submode.
Step 5	**database-mapping** *eid* **locator-set** *RLOC name* **Example:** `FabricEdge(config-router-lisp-instance-dynamic-eid)# database-mapping 66.66.66.64/32 locator-set rloc1`	Configures EID to RLOC mapping relationship.
Step 6	**map-cache** *destination-eid* **map-request** **Example:** `FabricEdge(config-router-lisp-instance-service)# map-cache 0.0.0.0/0 map-request`	Generates a static map request for the destination EID.
Step 7	**exit-service-ipv4** **Example:** `FabricEdge(config-router-lisp-instance-service)# exit-service-ipv4`	Exits service submode.
Step 8	**exit-instance-id** **Example:** `FabricEdge(config-router-lisp-instance)# exit-instance-id`	Exits instance submode.
Step 9	**instance-id** *instance* **Example:** `FabricEdge(config-router-lisp)# instance-id 101`	Creates a LISP EID instance to group multiple services.
Step 10	**service ethernet** **Example:** `FabricEdge(config-router-lisp-instance)# service ethernet`	Enables Layer 2 network services and enters service submode.

	Command or Action	Purpose
Step 11	**eid-table vlan** *vlan-number* **Example:** `FabricEdge(config-router-lisp-instance-service)# eid-table vlan 101`	Associates the LISP instance-id configured earlier with a VLAN through which the endpoint identifier address space is reachable.
Step 12	**flood arp-nd** **Example:** `FabricEdge(config-router-lisp-instance-service)# flood arp-nd`	Enables ARP flooding.
Step 13	**database-mapping** *mac* **locator-set** *RLOC name* **Example:** `FabricEdge(config-router-lisp-instance-service)# database-mapping mac locator-set rloc1`	Configures EID to RLOC mapping relationship.
Step 14	**exit-service-ethernet** **Example:** `FabricEdge(config-router-lisp-instance-service)# exit-service-ethernet`	Exits service sub mode.
Step 15	**exit-instance-id** **Example:** `FabricEdge(config-router-lisp-instance)# exit-instance-id`	Exits instance sub mode.

Verifying Passive Client Configuration

To verify the status of the Passive Client, use the following command:

```
Device# show wireless profile policy detailed sample-profile-policy

Policy Profile Name           : sample-profile-policy
Description                   : sample-policy
Status                        : ENABLED
VLAN                          : 20
Client count                  : 0
Passive Client                : ENABLED    <--------------------
WLAN Switching Policy
  Central Switching           : ENABLED
  Central Authentication      : ENABLED
  Central DHCP                : DISABLED
  Override DNS                : DISABLED
  Override NAT PAT            : DISABLED
  Central Assoc               : DISABLED
.
.
.
```

To verify VLANs that have ARP broadcast enabled, use the following command:

```
Device# show platform software arp broadcast

Arp broadcast is enabled on vlans:
20
```

CHAPTER 106

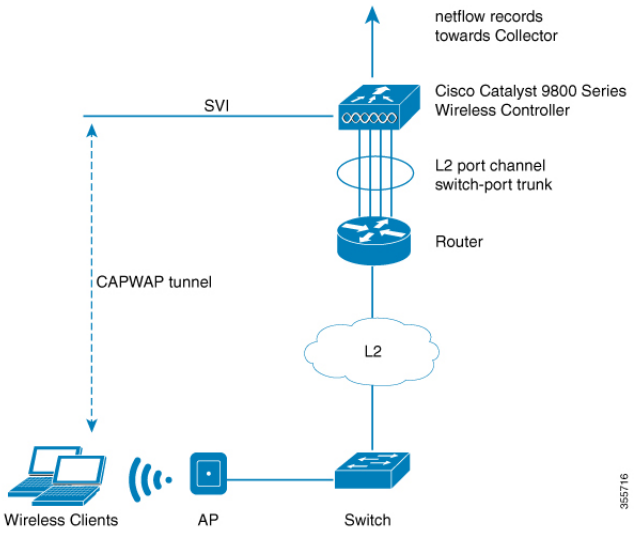
Encrypted Traffic Analytics

- Information About Encrypted Traffic Analytics, on page 1053
- Exporting Records to IPv4 Flow Export Destination, on page 1054
- Configuring ETA Flow Export Destination (GUI), on page 1054
- Enabling In-Active Timer, on page 1055
- Enabling ETA on WLAN Policy Profile, on page 1055
- Attaching Policy Profile to VLAN (GUI), on page 1056
- Attaching Policy Profile to VLAN, on page 1056
- Verifying ETA Configuration, on page 1057

Information About Encrypted Traffic Analytics

The Encrypted Traffic Analytics (ETA) leverages Flexible NetFlow (FNF) technology to export useful information about the flow to the collectors and gain visibility into the network.

Figure 26: Encrypted Traffic Analytics Deployed on Cisco Catalyst 9800 Series Wireless Controller in Local Mode



The wireless clients send data packets to the access point. The packets are then CAPWAP encapsulated and sent to the controller. This means that the actual client data is in the CAPWAP payload. To apply ETA on the client data, you need to strip the CAPWAP header before handing over the packet to the ETA module.

The ETA offers the following advantages:

- Enhanced telemetry based threat analytics.
- Analytics to identify malware.

Exporting Records to IPv4 Flow Export Destination

Follow the procedure given below to enable encrypted traffic analytics and configure a flow export destination:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**et-analytics** **Example:** `Device(config)# et-analytics`	Enables encrypted traffic analytics.
Step 3	**ip flow-export destination** *ip_address port_number* **Example:** `Device(config-et-analytics)# ip flow-export destination 120.0.0.1 2055`	Configures the NetFlow record export. Here, *port_number* ranges from 1 to 65535.
Step 4	**end** **Example:** `Device(config-et-analytics)# end`	Returns to privileged EXEC mode.

Configuring ETA Flow Export Destination (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **NetFlow**.

Step 2 Click the **Add** button. The **Create NetFlow** dialog box appears.

Step 3 Choose any one of the available templates from the **Netflow Template** drop-down list.

Step 4 Enter an IPv4 or IPv6 address in the **Collector Address** field.

Step 5 Enter a port number in the **Exporter Port** field. You must specify a value between 1 and 65535.

Step 6 Choose the desired option from the **Export Interface IP** drop-down list.

Step 7 Choose any one of the sampling methods from the **Sampling Method** drop-down list. The available options are **Deterministic**, **Random**, and **Full Netflow**.

Step 8 Enter a range for the sample. You must specify a value between 32 and 1032.

Step 9 Select the required interfaces/profile from the **Available** pane and move it to the **Selected** pane.

Step 10 Click the **Save & Apply to Device** button.

Enabling In-Active Timer

Follow the procedure given below to enable in-active timer:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**et-analytics** **Example:** `Device(config)# et-analytics`	Configures the encrypted traffic analytics.
Step 3	**inactive-timeout** *timeout-in-seconds* **Example:** `Device(config-et-analytics)# inactive-timeout 15`	Specifies the inactive flow timeout value. Here, *timeout-in-seconds* ranges from 1 to 604800.
Step 4	**end** **Example:** `Device(config-et-analytics)# end`	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Enabling ETA on WLAN Policy Profile

Follow the procedure given below to enable ETA on WLAN policy profile:

Procedure

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

	Command or Action	Purpose
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**et-analytics enable** **Example:** `Device(config-wireless-policy)# et-analytics enable`	Enables encrypted traffic analytics on the policy.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Attaching Policy Profile to VLAN (GUI)

Perform the following steps to attach a policy profile to VLAN.

Procedure

Step 1 Check the **RADIUS Profilling** checkbox.

Step 2 From the **Local Subscriber Policy Name**, choose the required policy name.

Step 3 In the **WLAN Local Profiling** section, enable or disable the **Global State of Device Classification**, check the checkbox for **HTTP TLV Caching** and **DHCL TLV Caching**.

Step 4 In the **VLAN** section, choose the **VLAN/VLAN Group** from the drop-down list. Enter the Muliticast VLAN.

Step 5 In the **WLAN ACL** section, choose the **IPv4 ACL** and **IPv6 ACL** from the drop-down list.

Step 6 In the **URL Filters** section, choose the **Pre Auth** and **Post Auth** from the drop-down list.

Step 7 Click **Save & Apply to Device**.

Attaching Policy Profile to VLAN

Follow the procedure given below to attach a policy profile to VLAN:

Procedure

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

	Command or Action	Purpose
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan vlan-name`	Assigns the policy profile to the VLANs.
Step 4	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.

Verifying ETA Configuration

Verifying ETA Globally

To view the ETA global and interface details, use the following command:

```
Device# show platform software utd chassis active F0 et-analytics global

ET Analytics Global Configuration
ID: 1
All Interfaces: Off
IP address and port and vrf: 192.168.5.2:2055:0
```

To view the ETA global configuration, use the following command:

```
Device# show platform software et-analytics global

ET-Analytics Global state
=========================
 All Interfaces   : Off
 IP Flow-record Destination: 192.168.5.2 : 2055
 Inactive timer: 15
```

Note The **show platform software et-analytics global** command does not display the ETA enabled wireless client interfaces.

To view the ETA global state in datapath, use the following command:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath runtime

ET-Analytics run-time information:

   Feature state: initialized (0x00000004)
   Inactive timeout      : 15 secs (default 15 secs)
   WhiteList information :
```

```
       flag: False
       cgacl w0 :  n/a
       cgacl w1 :  n/a
   Flow CFG information  :
       instance ID       : 0x0
       feature ID        : 0x1
       feature object ID : 0x1
       chunk ID : 0xC
```

To view the ETA memory details, use the following command:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath memory

ET-Analytics memory information:

   Size of FO            : 3200 bytes
   No. of FO allocs      : 0
   No. of FO frees       : 0
```

To view the ETA flow export in datapath, use the following command:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath stats export

ET-Analytics 192.168.5.2:2055 vrf 0 Stats:
    Export statistics:
      Total records exported     : 5179231
      Total packets exported     : 3124873
      Total bytes exported       : 3783900196
      Total dropped records      : 0
      Total dropped packets      : 0
      Total dropped bytes        : 0
      Total IDP records exported :
            initiator->responder : 1285146
            responder->initiator : 979284
      Total SPLT records exported:
            initiator->responder : 1285146
            responder->initiator : 979284
      Total SALT records exported:
            initiator->responder : 0
            responder->initiator : 0
      Total BD records exported  :
            initiator->responder : 0
            responder->initiator : 0
      Total TLS records exported :
            initiator->responder : 309937
            responder->initiator : 329469
```

To view the ETA flow statistics, use the following command:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath stats flow

ET-Analytics Stats:
    Flow statistics:
      feature object allocs : 0
      feature object frees  : 0
      flow create requests  : 0
      flow create matching  : 0
      flow create successful: 0
      flow create failed, CFT handle: 0
      flow create failed, getting FO: 0
      flow create failed, malloc FO : 0
      flow create failed, attach FO : 0
      flow create failed, match flow: 0
      flow create, aging already set: 0
      flow ageout requests          : 0
      flow ageout failed, freeing FO: 0
```

```
      flow ipv4 ageout requests     : 0
      flow ipv6 ageout requests     : 0
      flow whitelist traffic match  : 0
```

Verifying ETA on Wireless Client Interface

To view if a policy is configured with ETA, use the following command:

```
Device# show wireless profile policy detailed default-policy-profile

Policy Profile Name           : default-policy-profile
Description                   : default policy profile
Status                        : ENABLED
VLAN                          : 160
Multicast VLAN                : 0
Passive Client                : DISABLED
ET-Analytics                  : DISABLED
StaticIP Mobility             : DISABLED
WLAN Switching Policy
  Central Switching           : ENABLED
  Central Authentication      : ENABLED
  Central DHCP                : ENABLED
  Flex NAT PAT            : DISABLED
  Central Assoc               : ENABLED
```

To view the ETA status in the wireless client detail, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
<client_mac>

Wlclient Details for Client mac: 0026.c635.ebf8
  ---------------------------------
    Input VlanId  :  160
    Point of Presence      :  0
    Wlclient Input flags   :  9
    Instance ID   :  3
    ETA enabled   :  True
    client_mac_addr        :  0026.c635.ebf8

    bssid_mac_addr:  58ac.7843.037f
    Point of Attachment    :  65497
    Output vlanId :  160
    wlan_output_uidb       :  -1
    Wlclient Output flags  :  9
    Radio ID :  1
    cgacl w0 :  0x0
    cgacl w1 :  0x0
    IPv6 addr number       :  0
    IPv6 addr learning     :  0
```

To view clients in the ETA pending wireless client tree, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless et-analytics
eta-pending-client-tree

CPP IF_H     DPIDX      MAC Address    VLAN  AS  MS WLAN          POA
------------------------------------------------------------------------------
   0X2A     0XA0000001  2c33.7a5b.827b  160   RN  LC xyz_ssid     0x90000003
   0X2B     0XA0000002  2c33.7a5b.80fb  160   RN  LC xyz_ssid     0x90000003
```

To view the QFP interface handle, use the following command:

```
Device#
show platform hardware chassis active qfp interface if-handle <qfp_interface_handle>
```

```
show platform hardware chassis active qfp interface if-handle 0X29
FIA handle - CP:0x27f3ce8  DP:0xd7142000
  LAYER2_IPV4_INPUT_ARL_SANITY
  WLCLIENT_INGRESS_IPV4_FWD
  IPV4_TVI_INPUT_FIA         >>> ETA FIA Enabled
  SWPORT_VLAN_BRIDGING
  IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 1 - ipv4_output
FIA handle - CP:0x27f3d30  DP:0xd7141780
  IPV4_VFR_REFRAG (M)
  IPV4_TVI_OUTPUT_FIA        >>> ETA FIA Enabled
  WLCLIENT_EGRESS_IPV4_FWD
  IPV4_OUTPUT_DROP_POLICY (M)
  DEF_IF_DROP_FIA (M)
```

Note The *qfp_interface_handle* ranges from 1 to 4294967295.

To view the ETA pending wireless client tree statistics, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless et-analytics statistics

Wireless ETA cpp-client plumbing statistics
Number of ETA pending clients : 2
Counter                                          Value
-----------------------------------------------------------------
Enable ETA on wireless client called             0
Delete ETA on wireless client called             0
ETA global cfg init cb TVI FIA enable error      0
ETA global cfg init cb output SB read error      0
ETA global cfg init cb output SB write error     0
ETA global cfg init cb input SB read error       0
ETA global cfg init cb input SB write error      0
ETA global cfg init cb TVI FIA enable success    0
ETA global cfg uninit cb ingress feat disable    0
ETA global cfg uninit cb ingress cfg delete e    0
ETA global cfg uninit cb egress feat disable     0
ETA global cfg uninit cb egress cfg delete er    0
ETA pending list insert entry called             4
ETA pending list insert invalid arg error        0
ETA pending list insert entry exists error       0
ETA pending list insert no memory error          0
ETA pending list insert entry failed             0
ETA pending list insert entry success            4
ETA pending list delete entry called             2
ETA pending list delete invalid arg error        0
ETA pending list delete entry missing            0
ETA pending list delete entry remove error       0
ETA pending list delete entry success            2
```

PART XV

VLAN

- Configuring VLANs, on page 1063
- VLAN Groups, on page 1071

CHAPTER 107

Configuring VLANs

- Information About VLANs, on page 1063
- How to Configure VLANs, on page 1066
- Monitoring VLANs, on page 1070

Information About VLANs

Logical Networks

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any controller port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or a controller supporting fallback bridging. Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information.

VLANs are often associated with IP subnet. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the controller is assigned manually on an interface-by-interface basis. When you assign controller interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Supported VLANs

The controller supports VLANs in VTP client, server, and transparent modes. VLANs are identified by a number from 1 to 4094. VLAN 1 is the default VLAN and is created during system initialization. All of the VLANs except 1002 to 1005 are available for user configuration.

VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that specifies the kind of traffic the port carries and the number of VLANs to which it can belong.

When a port belongs to a VLAN, the controller learns and manages the addresses associated with the port on a per-VLAN basis.

Table 51: Port Membership Modes and Characteristics

Membership Mode	VLAN Membership Characteristics	VTP Characteristics
Static-access	A static-access port can belong to one VLAN and is manually assigned to that VLAN.	VTP is not required. If you do not want VTP to globally propagate information, set the VTP mode to transparent. To participate in VTP, there must be at least one trunk port on the controller connected to a trunk port of a second controller.
Trunk IEEE 802.1Q) : • IEEE 802.1Q—Industry-standard trunking encapsulation.	A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list.	VTP is recommended but not required. VTP maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP exchanges VLAN configuration messages with other controller over trunk links.

Note If a client VLAN has two subnets, a primary subnet and a secondary subnet, the static IP address is not supported on the secondary subnet.

Consider the following SVI configuration example:

interface VlanX

ip address a.b.c.254 255.255.255.0 secondary

ip address a.d.e.254 255.255.255.0

In this scenario, you can't allocate the secondary subnet for clients with static IP addresses.

VLAN Configuration Files

Configurations for VLAN IDs 1 to 1005 are written to the vlan.dat file (VLAN database), and you can display them by entering the **show vlan** privileged EXEC command. The *vlan.dat* file is stored in flash memory. If the VTP mode is transparent, they are also saved in the controller running configuration file.

You use the interface configuration mode to define the port membership mode and to add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the **show running-config** privileged EXEC command.

When you save VLAN and VTP information (including extended-range VLAN configuration information) in the startup configuration file and reboot the controller, the controller configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration, and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.

- If the VTP mode or domain name in the startup configuration does not match the VLAN database, the domain name and VTP mode and configuration for the VLAN IDs 1 to 1005 use the VLAN database information.
- In VTP versions 1 and 2, if VTP mode is server, the domain name and VLAN configuration for VLAN IDs 1 to 1005 use the VLAN database information. VTP version 3 also supports VLANs 1006 to 4094.

Note Ensure that you delete the vlan.dat file along with the configuration files before you reset the switch configuration using **write erase** command. This ensures that the switch reboots correctly on a reset.

Normal-Range VLAN Configuration Guidelines

Follow these guidelines when creating and modifying normal-range VLANs in your network:

- Normal-range VLANs are identified with a number between 1 and 1001.
- VLAN configurations for VLANs 1 to 1005 are always saved in the VLAN database. If the VTP mode is transparent, VTP and VLAN configurations are also saved in the running configuration file.
- If the controller is in VTP server or VTP transparent mode, you can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)
- Extended-range VLANs created in VTP transparent mode are not saved in the VLAN database and are not propagated. VTP version 3 supports extended range VLAN (VLANs 1006 to 4094) database propagation in VTP server mode.

Extended-Range VLAN Configuration Guidelines

Extended-range VLANs are VLANs with IDs from 1006 to 4094.

Follow these guidelines when creating extended-range VLANs:

- VLAN IDs in the extended range are not saved in the VLAN database and are not recognized by VTP unless the device is running VTP version 3.
- You cannot include extended-range VLANs in the pruning eligible range.
- For VTP version 1 or 2, you can set the VTP mode to transparent in global configuration mode. You should save this configuration to the startup configuration so that the device boots up in VTP transparent mode. Otherwise, you lose the extended-range VLAN configuration if the device resets. If you create extended-range VLANs in VTP version 3, you cannot convert to VTP version 1 or 2.

Prerequisites for VLANs

The following are prerequisites and considerations for configuring VLANs:

- To configure VLAN through the Web UI, you must change the number of available Virtual Terminal (VTY) sessions to 50. Web UI uses VTY lines for processing HTTP requests. At times, when multiple

connections are open, the default VTY lines of 15 set by the device gets exhausted. Therefore, you must change the VTY lines to 50 before using the Web UI.

Note To increase the VTY lines in a device, run the following command in the configuration mode:

```
Device# configure terminal
Device(config)# service tcp-keepalives in
Device(config)# service tcp-keepalives out

Device# configure terminal
Device(config)# line vty 16-50
```

- Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration for your network.
- Before adding a VLAN to a VLAN group, you should first create it on the device.

Restrictions for VLANs

The following are restrictions for VLANs:

- You cannot delete a wireless management interface, if the associated VLAN interface is already deleted. To avoid this scenario, you should delete the wireless management interface before deleting the VLAN interface.
- The device supports IEEE 802.1Q trunking methods for sending VLAN traffic over Ethernet ports.
- When client VLAN is not configured for a policy profile, AP native VLAN is used.
- The behavior of VLAN 1 changes depending on the AP mode. These scenarios are described below:
  - **Local mode AP**: If you use *vlan-name*, clients are assigned to VLAN 1. However, if you use *vlan-id* 1, clients are assigned to the wireless management interface.
  - **FlexConnect mode AP**: If you use *vlan-name*, clients are assigned to VLAN 1. However, if you use *vlan-id* 1, clients are assigned to the native VLAN defined in the flex profile.

  By default, the policy profile assigns vlan-id 1 so that clients can use the wireless management VLAN.

How to Configure VLANs

How to Configure Normal-Range VLANs

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

- VLAN ID
- VLAN name

- VLAN type
  - Ethernet
  - TrBRF or TrCRF
- VLAN state (active or suspended)
- Parent VLAN number for TrCRF VLANs
- VLAN number to use when translating from one VLAN type to another

You can cause inconsistency in the VLAN database if you attempt to manually delete the *vlan.dat* file. If you want to modify the VLAN configuration, follow the procedures in this section.

Creating or Modifying an Ethernet VLAN

Before you begin

With VTP version 1 and 2, if the controller is in VTP transparent mode, you can assign VLAN IDs greater than 1006, but they are not added to the VLAN database.

The controller supports only Ethernet interfaces.

Procedure

	Command or Action	Purpose
Step 1	**vlan** *vlan-id* **Example:** `Device(config)# vlan 20`	Enters a VLAN ID, and enters VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. **Note** The available VLAN ID range for this command is 1 to 4094.
Step 2	**name** *vlan-name* **Example:** `Device(config-vlan)# name test20`	(Optional) Enters a name for the VLAN. If no name is entered for the VLAN, the default is to append the *vlan-id* value with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.
Step 3	**media** { **ethernet** | **fd-net** | **trn-net** } **Example:** `Device(config-vlan)# media ethernet`	Configures the VLAN media type.
Step 4	**show vlan** {**name** *vlan-name* | **id** *vlan-id*} **Example:** `Device# show vlan name test20 id 20`	Verifies your entries.

Assigning Static-Access Ports to a VLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Layer2** > **VLAN** > **VLAN**

Step 2 Click the **VLAN** tab.

Step 3 To assign **Port Members**, click the interfaces that are to be included as port members from the **Available** list and click on the arrow to move it to the **Associated** list.

Step 4 Click **Update & Apply to Device**.

Assigning Static-Access Ports to a VLAN

You can assign a static-access port to a VLAN without having VTP globally propagate VLAN configuration information by disabling VTP (VTP transparent mode). For more information on static-access ports, see *VLAN Port Membership Modes*.

If you assign an interface to a VLAN that does not exist, the new VLAN is created.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet2/0/1`	Enters the interface to be added to the VLAN.
Step 3	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Defines the VLAN membership mode for the port (Layer 2 access port).
Step 4	**switchport access vlan** *vlan-id* **Example:** `Device(config-if)# switchport access vlan 2`	Assigns the port to a VLAN. Valid VLAN IDs are 1 to 4094.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config interface** *interface-id* **Example:** `Device# copy running-config startup-config`	Verifies the VLAN membership mode of the interface.
Step 7	**show interfaces** *interface-id* **switchport** **Example:** `Device# show interfaces gigabitethernet2/0/1`	Verifies your entries in the *Administrative Mode* and the *Access Mode VLAN* fields of the display.

How to Configure Extended-Range VLANs

Extended-range VLANs enable service providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any **switchport** commands that allow VLAN IDs.

With VTP version 1 or 2, extended-range VLAN configurations are not stored in the VLAN database, but because VTP mode is transparent, they are stored in the controller running configuration file, and you can save the configuration in the startup configuration file. Extended-range VLANs created in VTP version 3 are stored in the VLAN database.

Creating an Extended-Range VLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Layer2** > **VLAN**.

Step 2 In the VLAN page, click **ADD**.

Step 3 Enter the extended range VLAN ID in the **VLAN ID** field.

The extended range is between range is 1006 and 4094.

Step 4 Enter a VLAN name in the **Name** field.

Step 5 Save the configuration.

Creating an Extended-Range VLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**vlan** *vlan-id* **Example:** `Device(config)# vlan 2000`	Enters an extended-range VLAN ID and enters VLAN configuration mode. The range is 1006 to 4094.
Step 3	**show vlan id** *vlan-id* **Example:** `Device# show vlan id 2000`	Verifies that the VLAN has been created.

Monitoring VLANs

Table 52: Privileged EXEC show Commands

Command	Purpose
show interfaces [**vlan** *vlan-id*]	Displays characteristics for all interfaces or for the specified VLAN configured on the controller.
show vlan [**access-map** *name* | **brief** | **group** |**id** *vlan-id* | **ifindex** | **mtu** | **name** *name* | **summary**]	Displays parameters for all VLANs or the specified VLAN on the controller. The following command options are available: • **brief**—Displays VTP VLAN status in brief. • **group**—Displays the VLAN group with its name and the connected VLANs that are available. • **id**—Displays VTP VLAN status by identification number. • **ifindex**—Displays SNMP ifIndex. • **mtu**—Displays VLAN MTU information. • **name**—Displays the VTP VLAN information by specified name. • **summary**—Displays a summary of VLAN information.

CHAPTER 108

VLAN Groups

- Information About VLAN Groups, on page 1071
- Prerequisites for VLAN Groups, on page 1072
- Restrictions for VLAN Groups, on page 1072
- Creating a VLAN Group (GUI), on page 1072
- Creating a VLAN Group (CLI), on page 1073
- Adding a VLAN Group to Policy Profile (GUI), on page 1073
- Adding a VLAN Group to a Policy Profile, on page 1074
- Viewing the VLANs in a VLAN Group, on page 1074

Information About VLAN Groups

Whenever a client connects to a wireless network (WLAN), the client is placed in a VLAN that is associated with the policy profile mapped to the WLAN. In a large venue, such as an auditorium, a stadium, or a conference room where there are numerous wireless clients, having only a single WLAN to accommodate many clients might be a challenge.

The VLAN group feature uses a single policy profile that can support multiple VLANs. The clients can get assigned to one of the configured VLANs. This feature maps a policy profile to a single VLAN or multiple VLANs using the VLAN groups. When a wireless client associates to the WLAN, the VLAN is derived by an algorithm based on the MAC address of the wireless client. A VLAN is assigned to the client and the client gets the IP address from the assigned VLAN.

The system marks VLAN as *Dirty* for 30 minutes when the clients are unable to receive IP addresses using DHCP. The system might not clear the *Dirty* flag from the VLAN even after 30 minutes for a VLAN group. After 30 minutes, when the VLAN is marked non-dirty, new clients in the IP Learn state can get assigned with IP addresses from the VLAN if free IPs are available in the pool and DHCP scope is defined correctly. This is the expected behavior because the timestamp of each interface has to be checked to see if it is greater than 30 minutes, due to which there is a lag of 5 minutes for the global timer to expire.

Note The Controller marks the VLAN interface as *Dirty* when three or more clients fail to receive IP addresses through DHCP. The VLAN interface is deemed *Dirty* using the Non-Aggressive method, which involves counting one failure per association per client that surpasses the predefined **IP_LEARN_TIMEOUT** duration of 120 seconds. If a client sends a new association request before the **IP_LEARN_TIMEOUT** elapses, it will not be considered a failed client.

In Non-Aggressive method, each client gets a unique hash value derived from its MAC address. This approach ensures that clients belonging to the same vendor, which may differ only by a few bits, do not mistakenly trigger the *Dirty* marking of a VLAN.

Prerequisites for VLAN Groups

- A VLAN should be present in the device for it to be added to the VLAN group.

Restrictions for VLAN Groups

- If the number of VLANs in a VLAN group exceeds 32, the mobility functionality might not work as expected and Layer 2 multicast might break for some VLANs. Therefore, it is the responsibility of network administrators to configure a feasible number of VLANs in a VLAN group.

  For the VLAN Groups feature to work as expected, the VLANs mapped in a group must be present in the controller. The static IP client behavior is not supported.
- The VLAN Groups feature works for access points in local mode.
- The VLAN Groups feature works only in central switching mode and it cannot be used in FlexConnect local switching mode.
- ARP Broadcast feature is not supported on VLAN groups.
- VLAN group Multicast with VLAN group is only supported in local mode AP. Multicast VLAN is required when VLAN group is configured and uses multicast traffic.
- While you configure VLAN groups with multiple VLANs and each VLAN is used by a different subnet, clients having static IP addresses might be assigned to a wrong VLAN if SVIs are not present on the controller. Hence, for every VLAN that belongs to the VLAN group, ensure that you configure an SVI interface with a valid IP address.

Creating a VLAN Group (GUI)

Procedure

Step 1 Choose **Configuration** > **Layer2** > **VLAN**

Step 2 On the **VLAN** > **VLAN** page, click **Add**.

Step 3 Enter the VLAN ID in the **VLAN ID** field.

The valid range is between 2 and 4094.

Step 4 Enter the VLAN name in the **Name** field.

Configure the other parameters if required.

Step 5 Click **Update & Apply to Device**.

Creating a VLAN Group (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**vlan group** *WORD* **vlan-list** *vlan-ID* **Example:** `Device(config)#vlan group vlangrp1 vlan-list 91-95`	Creates a VLAN group with the given group name (vlangrp1) and adds all the VLANs listed in the command. The VLAN list ranges from 1 to 4096 and the maximum number of VLANs supported in a group is 64.
Step 3	**end** **Example:** `Device(config)#end`	Exits the global configuration mode and returns to privileged EXEC mode. Alternatively, press **CTRL-Z** to exit the global configuration mode.

Adding a VLAN Group to Policy Profile (GUI)

Policy profile broadly consists of network and switching policies. Policy profile is a reusable entity across tags. Anything that is a policy for the client that is applied on the AP or controller is moved to the policy profile. For example, VLAN, ACL, QOS, Session timeout, Idle timeout, AVC profile, Bonjour profile, Local profiling, Device classification, BSSID QoS, etc. However, all wireless related security attributes and features on the WLAN are grouped under the WLAN profile.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the**Policy Profile** page, click on a policy profile name.

Step 3 Click **Access Policies** tab.

Step 4 Under **VLAN** section, use the **VLAN/VLAN Group** drop-down list to select a VLAN or VLAN Group.

Step 5 Click **Update & Apply to Device**.

Adding a VLAN Group to a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan-policy-profile-name* **Example:** `Device(config)# wireless profile policy my-wlan-policy`	Configures the WLAN policy profile.
Step 3	**vlan** *vlan-group1* **Example:** `Device(config-wireless-policy)# vlan myvlan-group`	Maps the VLAN group to the WLAN by entering the group name.
Step 4	**end** **Example:** `Device(config-wlan)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Viewing the VLANs in a VLAN Group

Command	Description
show vlan group	Displays the list of VLAN groups with name and the VLANs that are configured.
show vlan group group-name *group_name*	Displays the specified VLAN group details.
show wireless client mac-address *client-mac-addr* **detail**	Displays the VLAN group assigned to the client.
show wireless vlan details	Displays VLAN details.

PART XVI

WLAN

- WLANs, on page 1077
- Remote LANs, on page 1091
- Network Access Server Identifier, on page 1107
- DHCP for WLANs, on page 1113
- WLAN Security, on page 1129
- Workgroup Bridges, on page 1137
- Peer-to-Peer Client Support, on page 1155
- Wireless Guest Access, on page 1157
- 802.11r BSS Fast Transition, on page 1177
- Assisted Roaming, on page 1185
- 802.11v, on page 1191
- 802.11w, on page 1195
- Ethernet over GRE , on page 1203

CHAPTER 109

WLANs

- Information About WLANs, on page 1077
- Prerequisites for WLANs, on page 1080
- Restrictions for WLANs, on page 1080
- How to Configure WLANs, on page 1081
- Verifying WLAN Properties (CLI), on page 1089

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 access points 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 device to access.

Note The **wireless client max-user-login concurrent** command will work as intended even if the **no configure max-user-identity response** command is configured.

Note We recommend that you configure the **password encryption aes** and the **key config-key password-encrypt** *key* commands to encrypt your password.

Note For C9105, C9115, and C9120 APs, when a new WLAN is pushed from the controller and if the existing WLAN functional parameters are changed, the other WLAN clients will disconnect and reconnect.

Band Selection

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 device.

Off-Channel Scanning Deferral

A lightweight access point, in normal operational conditions, periodically goes off-channel and scans another channel. This is in order to perform RRM operations such as the following:

- Transmitting and receiving Neighbor Discovery Protocol (NDP) packets with other APs.
- Detecting rogue APs and clients.
- Measuring noise and interference.

During the off-channel period, which normally is about 70 milliseconds, the AP is unable to transmit or receive data on its serving channel. Therefore, there is a slight impact on its performance and some client transmissions might be dropped.

While the AP is sending and receiving important data, it is possible to configure off-channel scanning deferral so that the AP does not go off-channel and its normal operation is not impacted. You can configure off-channel scanning deferral on a per-WLAN basis, per WMM UP class basis, with a specified time threshold in milliseconds. If the AP sends or receives, on a particular WLAN, a data frame marked with the given UP class within the specified threshold, the AP defers its next RRM off-channel scan. For example, by default, off-channel scanning deferral is enabled for UP classes 4, 5, and 6, with a time threshold of 100 millseconds. Therefore, when RRM is about to perform an off-channel scan, a data frame marked with UP 4, 5, or 6 is received within the last 100 milliseconds, RRM defers going off-channel. The AP radio does not go off-channel when a voice call sending and receiving audio samples is 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.

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 device, 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.

Prerequisites for Configuring Cisco Client Extensions

- The software supports CCX versions 1 through 5, which enables devices 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 device 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 device sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the device and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

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 device, dropped by the device, 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.

Diagnostic Channel

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

Note We recommend that you enable the diagnostic channel feature only for nonanchored SSIDs that use the management interface. CCX Diagnostic feature has been tested only with clients having Cisco ADU card

Prerequisites for WLANs

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

Restrictions for WLANs

- Do not configure PSK and CCKM in a WLAN, as this configuration is not supported and impacts client join flow.
- Ensure that TKIP or AES ciphers are enabled with WPA1 configuration, else ISSU may break during upgrade process.
- When you change the WLAN profile name, then FlexConnect APs (using AP-specific VLAN mapping) will become WLAN-specific. If FlexConnect Groups are configured, the VLAN mapping will become Group-specific.
- Do not enable IEEE 802.1X Fast Transition on Flex Local Authentication enabled WLAN, as client association is not supported with Fast Transition 802.1X key management.
- Peer-to-peer blocking does not apply to multicast traffic.
- In FlexConnect, peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all the FlexConnect APs that broadcast the SSID.
- The WLAN name and SSID can have up to 32 characters.
- WLAN and SSID names support only the following ASCII characters:
  - Numerals: 48 through 57 hex (0 to 9)
  - Alphabets (uppercase): 65 through 90 hex (A to Z)
  - Alphabets (lowercase): 97 through 122 hex (a to z)
  - ASCII space: 20 hex
  - Printable special characters: 21 through 2F, 3A through 40, and 5B through 60 hex, that is: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
- WLAN name cannot be a keyword; for example, if you try to create a WLAN with the name as 's' by entering the **wlan s** command, it results in shutting down all WLANs because 's' is used as a keyword for shutdown.
- You cannot map a WLAN to VLAN 0. Similarly, you cannot map a WLAN to VLANs 1002 to 1006.
- Dual stack clients with a static-IPv4 address is not supported.

- In a dual-stack with IPv4 and IPv6 configured in the Cisco 9800 controller, if an AP tries to join controller with IPv6 tunnel before its IPv4 tunnel gets cleaned, you would see a traceback and AP join will fail.
- 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.
- The SSID that is sent as part of the user profile will work only if **aaa override** command is configured.
- RADIUS server overwrite is not configured on a per WLAN basis, but rather on a per AAA server group basis.
- Downloadable ACL (DACL) is not supported in the FlexConnect mode or the local mode.

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

How to Configure WLANs

Creating WLANs (GUI)

Procedure

Step 1 In the **Configuration** > **Tags & Profiles** > **WLANs** page, click **Add**.

The **Add WLAN** window is displayed.

Step 2 Under the **General** tab and **Profile Name** field, enter the name of the WLAN. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 3 Click **Save & Apply to Device**.

Creating WLANs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id* [*ssid*] **Example:**	Specifies the WLAN name and ID:

	Command or Action	Purpose
	`Device(config)# wlan mywlan 34 mywlan-ssid`	• For the *profile-name*, enter the profile name. The range is from 1 to 32 alphanumeric characters. • For the *wlan-id*, enter the WLAN ID. The range is from 1 to 512. • For the *ssid*, enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID. **Note** • You can create SSID using GUI or CLI. However, we recommend that you use CLI to create SSID. • By default, the WLAN is disabled.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Deleting WLANs (GUI)

Procedure

Step 1 In the **Configuration** > **Tags & Profiles** > **WLANs** page, check the checkbox adjacent to the WLAN you want to delete.

To delete multiple WLANs, select multiple WLANs checkboxes.

Step 2 Click **Delete**.

Step 3 Click **Yes** on the confirmation window to delete the WLAN.

Deleting WLANs

Procedure

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

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

Searching WLANs (CLI)

To verify the list of all WLANs configured on the controller, use the following show command:

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

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

To use wild cards and search for WLANs, use the following `show` command:

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

Enabling WLANs (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **WLANs** page, click the WLAN name.

Step 3 In the **Edit WLAN** window, toggle the **Status** button to **ENABLED**.

Step 4 Click **Update & Apply to Device**.

Enabling WLANs (CLI)

Procedure

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

Disabling WLANs (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.
Step 2 In the **WLANs** window, click the WLAN name.
Step 3 In the **Edit WLAN** window, set the **Status** toggle button as **DISABLED**.
Step 4 Click **Update & Apply to Device**.

Disabling WLANs (CLI)

Procedure

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

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

Configuring General WLAN Properties (CLI)

You can configure the following properties:

- Media stream
- Broadcast SSID
- Radio

Procedure

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

	Command or Action	Purpose
	`Device(config-wlan)# broadcast-ssid`	
Step 5	**dot11bg 11g** **Example:** `Device(config-wlan)# dot11bg 11g`	Configures the WLAN radio policy for dot11 radios.
Step 6	**media-stream multicast-direct** **Example:** `Device(config-wlan)# media-stream multicast-direct`	Enables multicast VLANs on this WLAN.
Step 7	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 8	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Configuring Advanced WLAN Properties (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**chd** **Example:** `Device(config-wlan)# chd`	Enables coverage hole detection for this WLAN.
Step 4	**ccx aironet-iesupport** **Example:** `Device(config-wlan)# ccx aironet-iesupport`	Enables support for Aironet IEs for this WLAN.

	Command or Action	Purpose
Step 5	**client association limit** {*clients-per-wlan* | **ap** *clients-per-ap-per-wlan* | **radio***clients-per-ap-radio--per-wlan*} **Example:** `Device(config-wlan)# client association limit ap 400`	Sets the maximum number of clients, clients per AP, or clients per AP radio that can be configured on a WLAN.
Step 6	**ip access-group web** *acl-name* **Example:** `Device(config-wlan)# ip access-group web test-acl-name`	Configures the IPv4 WLAN web ACL. The variable *acl-name* specifies the user-defined IPv4 ACL name.
Step 7	**peer-blocking** [**drop** | **forward-upstream**] **Example:** `Device(config-wlan)# peer-blocking drop`	Configures peer to peer blocking parameters. The keywords are as follows: • **drop**—Enables peer-to-peer blocking on the drop action. • **forward-upstream**—No action is taken and forwards packets to the upstream. **Note** The **forward-upstream** option is not supported for Flex local switching. Traffic is dropped even if this option is configured. Also, peer to peer blocking for local switching SSIDs are available only for the clients on the same AP.
Step 8	**channel-scan** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}} **Example:** `Device(config-wlan)# channel-scan defer-priority 6`	Sets the channel scan defer priority and defer time. The arguments are as follows: • **defer-priority**—Specifies the priority markings for packets that can defer off-channel scanning. The range is from 0 to 7. The default is 3. • **defer-time**—Deferral time in milliseconds. The range is from 0 to 6000. The default is 100.
Step 9	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Configuring Advanced WLAN Properties (GUI)

Before you begin

Ensure that you have configured an AP Join Profile prior to configuring the primary and backup controllers.

Procedure

Step 1 Choose **Configuration** > **Wireless** > **WLANs** > **Wireless Networks**.

Step 2 In the **Wireless Networks** window, click **Add**.

Step 3 Under the **Advanced** tab, check the **Coverage Hole Detection** check box.

Step 4 Check the **Aironet IE** check box to enable Aironet IE on the WLAN.

Step 5 Check the **Diagnostic Channel** check box to enable diagnostic channel on the WLAN.

Step 6 From the **P2P Blocking Action** drop-down list, choose the required value.

Step 7 Set the **Multicast Buffer** toggle button as enabled or diabled.

Step 8 Check the **Media Stream Multicast-Direct** check box to enable the feature.

Step 9 In the **Max Client Connections** section, specify the maximumui number of client connections for the following:

- In the **Per WLAN** field, enter a value. The valid range is between 0 and 10000.
- In the **Per AP Per WLAN** field, enter a value. The valid range is between 0 and 400.
- In the **Per AP Radio Per WLAN** field, enter a value. The valid range is between 0 and 200.

Step 10 In the **11v BSS Transition Support** section, perform the following configuration tasks:

a) Check the BSS Transition check box to enable 802.11v BSS Transition support.
b) In the **Disassociation Imminent** field, enter a value. The valid range is between 0 and 3000.
c) In the **Optimized Roaming Disassociation Timer** field, enter a value. The valid range is between 0 and 40.
d) Select the check box to enable the following:

- BSS Max Idle Service
- BSS Max Idle Protected
- Disassociation Imminent Service
- Directed Multicast Service
- Universal Admin
- Load Balance
- Band Select
- IP Source Guard

Step 11 From the **WMM Policy** drop-down list, choose the policy as Allowed, Disabled, or Required. By default, the WMM policy is Allowed.

Step 12 In the **Off Channel Scanning Defer** section, choose the appropriate **Defer Priority** values and then specify the required Scan Defer Time value in milliseconds.

Step 13 In the **Assisted Roaming (11k)** section, choose the appropriate status for the following:

- Prediction Optimization
- Neighbor List
- Dual-Band Neighbor List

Step 14 In the **DTIM Period (in beacon intervals)** section, specify a value for 802.11a/n and 802.11b/g/n radios. The valid range is from 1 to 255.

Step 15 Click **Save & Apply to Device**.

Verifying WLAN Properties (CLI)

To verify the WLAN properties based on the WLAN ID, use the following `show` command:

```
Device# show wlan id wlan-id
```

To verify the WLAN properties based on the WLAN name, use the following `show` command:

```
Device# show wlan name wlan-name
```

To verify the WLAN properties of all the configured WLANs, use the following `show` command:

```
Device# show wlan all
```

To verify the summary of all WLANs, use the following `show` command:

```
Device# show wlan summary
```

To verify the running configuration of a WLAN based on the WLAN name, use the following `show` command:

```
Device# show running-config wlan wlan-name
```

To verify the running configuration of all WLANs, use the following `show` command:

```
Device# show running-config wlan
```

CHAPTER 110

Remote LANs

- Information About Remote LANs, on page 1091
- Configuring Remote LANs (RLANs), on page 1093

Information About Remote LANs

A Remote LAN (RLAN) is used for authenticating wired clients using the controller. Once the wired client successfully joins the controller, the LAN ports switch the traffic between central or local switching modes. The traffic from wired client is treated as wireless client traffic.

The RLAN in Access Point (AP) sends the authentication request to authenticate the wired client. The authentication of wired client in RLAN is similar to the central authenticated wireless client.

The supported AP models are:

- Cisco Catalyst 9105AXW
- Cisco Aironet OEAP 1810 series
- Cisco Aironet 1815T series
- Cisco Aironet 1810W series
- Cisco Aironet 1815W

Information About Ethernet (AUX) Port

The second Ethernet port in Cisco Aironet 1850, 2800, and 3800 Series APs is used as a link aggregation (LAG) port, by default. It is possible to use this LAG port as an RLAN port when LAG is disabled.

The following APs use LAG port as an RLAN port:

- 1852E
- 1852I
- 2802E
- 2802I
- 3802E
- 3802I

- 3802P
- 4802

Limitation for RLAN

- RLAN supports only a maximum of four wired clients regardless of the AP model.
- RLAN support with Virtual Routing and Forwarding (VRF) is not available.

Limitations for Using AUX port in Cisco 2700 Access Points

- RLAN supports AUX port and non-native VLAN for this port.
- Local mode supports wired client traffic on central switch. Whereas, Flexconnect mode does not support central switch.
- Flexconnect mode supports wired client traffic on local switch and not on central switch.
- AUX port cannot be used as a trunk port. Even switches or bridges cannot be added behind the port.
- AUX port does not support dot1x.

Role of Controller

- The controller acts as an authenticator, and Extensible Authentication Protocol (EAP) over LAN (EAPOL) messages from the wired client reaching the controller through an AP.
- The controller communicates with the configured Authentication, Authorization, and Accounting (AAA) server.
- The controller configures the LAN ports for an AP and pushes them to the corresponding AP.

Note

- RLAN is supported in APs that have more than one Ethernet port.
- APs in local mode central switching do not support VLAN tagged traffic from RLAN clients, and the traffic gets dropped.
- The VLAN name (without any numerals) configured in remote-lan-policy does not provide the mapped VLAN ID for central switching.

Configuring Remote LANs (RLANs)

Enabling or Disabling all RLANs

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	[**no**] **ap remote-lan shutdown** **Example:** `Device(config)# [no] ap remote-lan shutdown`	Enables or disables all RLANs.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating RLAN Profile (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > Remote LAN**.

Step 2 Click **Add**.

Step 3 Enter the **Profile Name**, **RLAN ID** and enable or disable the **Status** toggle button. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Click **Apply to Device**.

Creating RLAN Profile (CLI)

Procedure

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

	Command or Action	Purpose
Step 2	**ap remote-lan profile-name** *remote-lan-profile-name rlan-id* **Example:** `Device(config)# ap remote-lan profile-name rlan_profile_name 3`	Configures remote LAN profile. • *remote-lan-profile*—Is the remote LAN profile name. Range is from 1 to 32 alphanumeric characters. • *rlan-id*—Is the remote LAN identifier. Range is from 1 to 128. **Note** You can create a maximum of 128 RLANs. You cannot use the *rlan-id* of an existing RLAN while creating another RLAN. Both RLAN and WLAN profile cannot have the same names. Similarly, RLAN and WLAN policy profile cannot have the same names.

Configuring RLAN Profile Parameters (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > Remote LAN**.

Step 2 On the **RLAN Profile** tab, click **Add**.

The **Add RLAN Profile** window is displayed.

Step 3 In the **General** tab:

a) Enter a **Name** and **RLAN ID** for the RLAN profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

b) Set the number of client connections per RLAN in the **Client Association Limit** field.

The range depends on the maximum number of clients supported by the platform.

c) To enable the profile, set the status as **Enable**.

Step 4 In the **Security** > **Layer2** tab

a) To enable 802.1x for an RLAN, set the **802.1x** status as **Enabled**.

Note You can activate either web or 802.1x authentication list at a time.

b) Choose the authorization list name from the **MAC Filtering** drop-down list.

c) Choose the 802.1x for an RLAN authentication list name from the **Authentication List** drop-down list.

Step 5 In the **Security** > **Layer3** tab

a) To enable web authentication for an RLAN, set the **Web Auth** status as **Enabled**.

Note You can activate either web or 802.1x authentication list at a time.

b) Choose the web authentication parameter map from the **Webauth Parameter Map** drop-down list.
c) Choose the web authentication list name from the **Authentication List** drop-down list.

Step 6 In the **Security** > **AAA** tab

a) Set the **Local EAP Authentication** to enabled. Also, choose the required **EAP Profile Name** from the drop-down list.

Step 7 Save the configuration.

Configuring RLAN Profile Parameters (CLI)

Before you begin

The configurations in this section are not mandatory for an RLAN profile.

In case of central switching mode, you need to configure both central switching and central DHCP.

Procedure

	Command or Action	Purpose
Step 1	**client association limit** *client-connections* **Example:** `Device(config-remote-lan)# client association limit 1`	Configures client connections per RLAN. *client-connections*—Is the maximum client connections per RLAN. Range is from 0 to 10000. 0 refers to unlimited.
Step 2	**ip access-group web** *IPv4-acl-name* **Example:** `Device(config-remote-lan)# ip access-group web acl_name`	Configures RLAN IP configuration commands. *IPv4-acl-name*—Refers to the IPv4 ACL name or ID.
Step 3	**local-auth** *profile name* **Example:** `Device(config-remote-lan)# local-auth profile_name`	Sets EAP Profile on an RLAN. *profile name*—Is the EAP profile on an RLAN.
Step 4	**mac-filtering** *mac-filter-name* **Example:** `Device(config-remote-lan)# mac-filtering mac_filter`	Sets MAC filtering support on an RLAN. *mac-filter-name*—Is the authorization list name.
Step 5	**security dot1x authentication-list** *list-name* **Example:** `Device(config-remote-lan)# security dot1x authentication-list dot1_auth_list`	Configures 802.1X for an RLAN. *list-name*—Is the authentication list name.
Step 6	**security web-auth authentication-list** *list-name*	Configures web authentication for an RLAN. *list-name*—Is the authentication list name.

	Command or Action	Purpose
	Example: `Device(config-remote-lan)# security web-auth authentication-list web_auth_list`	**Note** You can activate either web or dot1x authentication list at a time.
Step 7	[**no**] **shutdown** **Example:** `Device(config-remote-lan)# shutdown`	Enables or disables RLAN profile.
Step 8	**end** **Example:** `Device(config-remote-lan)# end`	Returns to privileged EXEC mode.

Creating RLAN Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Remote LAN** > **RLAN Policy**

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Policy Name**.

Step 4 Click **Apply to Device**.

Creating RLAN Policy Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap remote-lan-policy policy-name** *profile name* **Example:** `Device(config)# ap remote-lan-policy policy-name rlan_policy_prof_name`	Configures RLAN policy profile and enters wireless policy configuration mode.

Configuring RLAN Policy Profile Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Remote LAN**.

Step 2 On the **Remote LAN** page, click **RLAN Policy** tab.

Step 3 On the **RLAN Policy** page, click the name of the **Policy** or click **Add** to create a new one.

The **Add/Edit RLAN Policy** window is displayed.

Step 4 In the **General** tab:

a) Enter a **Name** and **Description** for the policy profile.
b) Set **Central Authentication** to **Enabled** state.
c) Set **Central DHCP** to **Enabled** state.
d) Set the **PoE** check box to enable or disable state.
e) To enable the policy, set the status as **Enable**.

Step 5 In the **Access Policies** Tab, choose the VLAN name or number from the **VLAN** drop-down list.

Note When central switching is disabled, the VLAN in the RLAN policy cannot be configured as the AP's native VLAN. To use the AP's native VLAN for client IP, the VLAN should be configured as either **no vlan** or **vlan 1** in the RLAN policy profile.

Step 6 From the **Host Mode** drop-down list, choose the **Host Mode** for the remote-LAN802.1x from the following options:

- Single-Host Mode—Is the default host mode. In this mode, the switch port allows only a single host to be authenticated and passes traffic one by one.
- Multi-Host Mode—The first device to authenticate opens up to the switch port, so that all other devices can use the port. You need not authenticate other devices independently, if the authenticated device becomes authorized the switch port is closed.
- Multi-Domain Mode—The authenticator allows one host from the data domain and another from the voice domain. This is a typical configuration on switch ports with IP phones connected.

Note For an RLAN profile with open-auth configuration, you must map the RLAN-policy with single host mode. Mapping RLAN-policy with multi-host or multi-domain mode is not supported.

Step 7 Configure IPv6 ACL or Flexible Netflow.

- Under the **Access Policies** > **Remote LAN ACL** section, choose the **IPv6 ACL** from the drop-down list.
- Under the **Access Policies** > **AVC** > **Flow Monitor IPv6** section, check the **Egress Status** and **Ingress Status** check boxes and choose the policies from the drop-down lists.

Step 8 Click the **Advanced** tab.

a) Configure the violation mode for Remote-LAN 802.1x from the **Violation Mode** drop-down list, choose the violation mode type from the following options:

- 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.

b) Enter the **Session Timeout (sec)** value to define the client's duration of a session.

The range is between 20 and 86400 seconds.

c) Under **AAA Policy Params** section, check the **AAA Override** check box to enable AAA override.

d) Under the **Exclusionlist Params** section, check the **Exclusionlist** check box and enter the **Exclusionlist Timeout** value.

This sets the exclusion time for a client. The range is between 0 and 2147483647 seconds. 0 refers to no timeout.

Step 9 Save the configuration.

Configuring RLAN Policy Profile Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**central switching** **Example:** `Device(config-remote-lan-policy)# central switching`	Configures central switching.
Step 2	**central dhcp** **Example:** `Device(config-remote-lan-policy)# central dhcp`	Configures central DHCP.
Step 3	**exclusionlist timeout** *timeout* **Example:** `Device(config-remote-lan-policy)# exclusionlist timeout 200`	Sets exclusion-listing on RLAN. *timeout*—Sets the time, up to which the client will be in excluded state. Range is from 0 to 2147483647 seconds. 0 refers to no timeout.
Step 4	**vlan** *vlan* **Example:** `Device(config-remote-lan-policy)# vlan vlan1`	Configures VLAN name or ID. - *vlan*—Is the vlan name.
Step 5	**Example:** `Device(config-remote-lan-policy)# ipv6 acl ipv6_acl`	

	Command or Action	Purpose
Step 6	**aaa-override** **Example:** `Device(config-remote-lan-policy)# aaa-override`	Configures AAA policy override.
Step 7	**session-timeout** *timeout in seconds* **Example:** `Device(config-remote-lan-policy)# session-timeout 21`	Configures client session timeout. *timeout in seconds*—Defines the duration of a session. Range is from 20 to 86400 seconds.
Step 8	**host-mode** {**multidomain** *voice domain* | **multihost** |**singlehost**} **Example:** `Device(config-remote-lan-policy)# host-mode multidomain`	Configures host mode for remote-LAN 802.1x. *voice domain*—Is the RLAN voice domain VLAN ID. Range is from 0 to 65535. You can configure the following IEEE 802.1X authentication modes: • Multi-Domain Mode—The authenticator allows one host from the data domain and another from the voice domain. This is a typical configuration on switch ports with IP phones connected. • Multi-Host Mode—The first device to authenticate opens up to the switch port, so that all other devices can use the port. You need not authenticate other devices independently, if the authenticated device becomes authorized the switch port is closed. • Single-Host Mode—Is the default host mode. In this mode, the switch port allows only a single host to be authenticated and passes traffic one by one.
Step 9	**violation-mode** {**protect** | **replace** | **shutdown**} **Example:** `Device(config-remote-lan-policy)# violation-mode protect`	Configures violation mode for Remote-LAN 802.1x. 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

	Command or Action	Purpose
		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.
Step 10	[**no**] **poe** **Example:** `Device(config-remote-lan-policy)# poe`	Enables or disables PoE.
Step 11	[**no**] **shutdown** **Example:** `Device(config-remote-lan-policy)# shutdown`	Enables or disables an RLAN policy profile.
Step 12	**end** **Example:** `Device(config-remote-lan-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Policy Tag and Mapping an RLAN Policy Profile to an RLAN Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config)# wireless tag policy remote-lan-policy-tag`	Configures policy tag and enters policy tag configuration mode.
Step 3	**remote-lan** *remote-lan-profile-name* **policy** *rlan-policy-profile-name* **port-id** *port-id* **Example:** `Device(config-policy-tag)# remote-lan rlan_profile_name policy rlan_policy_profile port-id 2`	Maps an RLAN policy profile to an RLAN profile. • *remote-lan-profile-name*—Is the name of the RLAN profile. • *rlan-policy-profile-name*—Is the name of the policy profile.

	Command or Action	Purpose
		• *port-id*—Is the LAN port number on the access point. Range is from 1 to 4.
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring LAN Port (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap name* **lan port-id** *lan port id* {**disable** | **enable**} **Example:** `Device# ap name L2_1810w_2 lan port-id 1 enable`	Configures a LAN port. • enable—Enables the LAN port. • disable—Disables the LAN port.

Attaching Policy Tag to an Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.
Step 2 Select the AP to attach the Policy Tag.
Step 3 Under the **Tags** section, use the **Policy** drop-down to select a policy tag.
Step 4 Click **Update & Apply to Device**.

Attaching Policy Tag to an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *ap-ethernet-mac* **Example:**	Configures MAP address for an AP and enters AP configuration mode.

	Command or Action	Purpose
	`Device(config)# ap 00a2.891c.21e0`	
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag remote-lan-policy-tag`	Attaches policy tag to the access point. *policy-tag-name*—Is the name of the policy tag defined earlier.
Step 4	**end** **Example:** `Device(config-ap-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying RLAN Configuration

To view the summary of all RLANs, use the following command:

```
Device# show remote-lan summary

Number of RLANs: 1

RLAN        Profile Name                      Status
------------------------------------------------------------------
1            rlan_test_1                       Enabled
```

To view the RLAN configuration by ID, use the following command:

```
Device# show remote-lan id <id>

Remote-LAN Profile Name              : rlan_test_1
=====================================================
Identifier                                  : 1
Status                                      : Enabled
Mac-filtering                               : Not Configured
Number of Active Clients                    : 1
Security_8021X                              : Disabled
8021.x Authentication list name             : Not Configured
Local Auth eap Profile Name                 : Not Configured
Web Auth Security                           : Disabled
Webauth Authentication list name            : Not Configured
Web Auth Parameter Map                      : Not Configured
Client association limit                    : 0
Ipv4 Web Pre Auth Acl                       : Not Configured
Ipv6 Web Pre Auth Acl                       : Not Configured
```

To view the RLAN configuration by profile name, use the following command:

```
Device# show remote-lan name <profile-name>

Remote-LAN Profile Name                     : rlan_test_1
=========================================================
Identifier                                  : 1
Status                                      : Enabled
Mac-filtering                               : Not Configured
Number of Active Clients                    : 1
Security_8021X                              : Disabled
8021.x Authentication list name             : Not Configured
Local Auth eap Profile Name                 : Not Configured
Web Auth Security                           : Disabled
Webauth Authentication list name            : Not Configured
```

```
Web Auth Parameter Map                      : Not Configured
Client association limit                    : 0
Ipv4 Web Pre Auth Acl                       : Not Configured
Ipv6 Web Pre Auth Acl                       : Not Configured
```

To view the detailed output of all RLANs, use the following command:

```
Device# show remote-lan all

Remote-LAN Profile Name            : rlan_test_1
================================================
Identifier                         : 1
Status                             : Enabled
Mac-filtering                      : Not Configured
Number of Active Clients           : 1
Security_8021X                     : Disabled
8021.x Authentication list name    : Not Configured
Local Auth eap Profile Name        : Not Configured
Web Auth Security                  : Disabled
Webauth Authentication list name   : Not Configured
Web Auth Parameter Map             : Not Configured
Client association limit           : 0
Ipv4 Web Pre Auth Acl              : Not Configured
Ipv6 Web Pre Auth Acl              : Not Configured

Remote-LAN Profile Name            : rlan_test_2
================================================
Identifier                         : 2
Status                             : Enabled
Mac-filtering                      : Not Configured
Number of Active Clients           : 1
Security_8021X                     : Disabled
8021.x Authentication list name    : Not Configured
Local Auth eap Profile Name        : Not Configured
Web Auth Security                  : Disabled
Webauth Authentication list name   : Not Configured
Web Auth Parameter Map             : Not Configured
Client association limit           : 0
Ipv4 Web Pre Auth Acl              : Not Configured
Ipv6 Web Pre Auth Acl              : Not Configured
```

```
Device# show remote-lan policy summary
Number of Policy Profiles: 1

Profile Name                      Description                              Status
-------------------------------------------------------------------------------------------
rlan_named_pp1                Testing RLAN policy profile              Enabled
```

To view the LAN port configuration of a Cisco AP, use the following command:

```
Device# show ap name <ap_name> lan port summary
LAN Port status for AP L2_1815w_1
Port ID      status       vlanId      poe
-----------------------------------------
LAN1         Enabled       20          Disabled
LAN2         Enabled       20          NA
LAN3         Disabled      0           NA
```

To view the summary of all clients, use the following command:

```
Device# show wireless client summary
Number of Local Clients: 1

MAC Address       AP Name         WLAN         State    Protocol    Method     Role
-----------------------------------------------------------------------------------------
d8eb.97b6.fcc6    L2_1815w_1      1            * Run     Ethernet    None      Local
```

To view the client details with the specified username, use the following command:

```
Device# show wireless client username cisco
MAC Address        AP Name          Status      WLAN      Auth Protocol
-------------------------------------------------------------------------------------------------
0014.d1da.a977    L2_1815w_1        Run 1 *      Yes        Ethernet
d8eb.97b6.fcc6    L2_1815w_1        Run 1 *      Yes        Ethernet
```

To view the detailed information for a client by MAC address, use the following command:

```
Device# show wireless client mac-address d8eb.97b6.fcc6 detail
Client MAC Address : d8eb.97b6.fcc6
Client IPv4 Address : 9.2.20.78
Client IPv6 Addresses : fe80::1863:292f:feaa:2cf
Client Username: N/A
AP MAC Address : 707d.b99e.c2e0
AP Name: L2_1815w_1
AP slot : 2
Client State : Associated
Policy Profile : rlan_named_pp1
Flex Profile : rlan-flex-profile
Remote LAN Id : 1
Remote LAN Name: rlan_test_1
BSSID : 707d.b99e.c2e1
Connected For : 1159 seconds
Protocol : Ethernet
Channel : 0
Port ID: 2
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Session Timeout : 1800 sec (Remaining time: 641 sec)
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Disabled
Fastlane Support : Disabled
Power Save : OFF
Current Rate : 0.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 07/06/2018 11:25:26 IST
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 1159 seconds
Policy Type : N/A
Encryption Cipher : None
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : 20
Access VLAN : 20
Anchor VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
```

```
Session Manager:
  Interface        : capwap_90000008
  IIF ID           : 0x90000008
  Authorized       : TRUE
  Session timeout  : 1800
  Common Session ID: 32130209000000136C48A29D
  Acct Session ID  : 0x00000000
  Aaa Server Details
  Server IP        :
  Auth Method Status List
   Method : None
  Local Policies:
   Service Template : wlan_svc_rlan_named_pp1_local (priority 254)
    Absolute-Timer   : 1800
    VLAN             : 20
  Server Policies:
  Resultant Policies:
    VLAN             : 20
    Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Central
FlexConnect Dhcp Status : Central
FlexConnect Authentication : Central
FlexConnect Central Association : No
Client Statistics:
  Number of Bytes Received : 6855
  Number of Bytes Sent : 1640
  Number of Packets Received : 105
  Number of Packets Sent : 27
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : 0 dBm
  Signal to Noise Ratio : 0 dB
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
```

To view the summary of all AP tags, use the following command:

```
Device# show ap tag summary
Number of APs: 2

AP Name             AP Mac               Site Tag Name         Policy Tag Name         RF
Tag Name               Misconfigured     Tag Source
-------------------------------------------------------------------------------------------
L2_1810d_1        0008.3296.24c0       default-site-tag        default-policy-tag
default-rf-tag             No              Default
L2_1810w_2        00b0.e18c.5880       rlan-site-tag              rlan_pt_1
default-rf-tag             No              Static
```

To view the summary of all policy tags, use the following command:

```
Device# show wireless tag policy summary
Number of Policy Tags: 2
```

```
Policy Tag Name                   Description
------------------------------------------------------------------------
rlan_pt_1
default-policy-tag                default policy-tag
```

To view details of a specific policy tag, use the following command:

```
Device# show wireless tag policy detailed <rlan_policy_tag_name>
Policy Tag Name : rlan_pt_1
Description     :

Number of WLAN-POLICY maps: 0

Number of RLAN-POLICY maps: 2
REMOTE-LAN Profile Name           Policy Name                              Port Id

-------------------------------------------------------------------------------------------
rlan_test_1                       rlan_named_pp1                              1

rlan_test_1                       rlan_named_pp1                              2
```

CHAPTER 111

Network Access Server Identifier

- Information About Network Access Server Identifier, on page 1107
- Creating a NAS ID Policy(GUI), on page 1108
- Creating a NAS ID Policy, on page 1108
- Attaching a Policy to a Tag (GUI), on page 1109
- Attaching a Policy to a Tag (CLI), on page 1109
- Verifying the NAS ID Configuration, on page 1110

Information About Network Access Server Identifier

Network access server identifier (NAS-ID) is used to notify the source of a RADIUS access request, which enables the RADIUS server to choose a policy for that request. You can configure one on each WLAN profile, VLAN interface, or access point group. The NAS-ID is sent to the RADIUS server by the controller through an authentication request to classify users to different groups. This enables the RADIUS server to send a customized authentication response.

Note The acct-session-id is sent with the RADIUS access request only when accounting is enabled on the policy profile.

If you configure a NAS-ID for an AP group, it overrides the NAS-ID that is configured for a WLAN profile or the VLAN interface. Similarly, if you configure a NAS-ID for a WLAN profile, it overrides the NAS-ID that is configured for the VLAN interface.

The following options can be configured for a NAS ID:

- sys-name (System Name)
- sys-ip (System IP Address)
- sys-mac (System MAC Address)
- ap-ip (AP's IP address)
- ap-name (AP's Name)
- ap-mac (AP's MAC Address)
- ap-eth-mac (AP's Ethernet MAC Address)

- ap-policy-tag (AP's policy tag name)
- ap-site-tag (AP's site tag name)
- ssid (SSID Name)
- ap-location (AP's Location)

Creating a NAS ID Policy(GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Wireless AAA Policy**.

Step 2 On the **Wireless AAA Policy** page, click the name of the **Policy** or click **Add** to create a new one.

Step 3 In the **Add/Edit Wireless AAA Policy** window that is displayed, enter the name of the policy in the **Policy Name** field.

Step 4 Choose from one of the NAS ID options from the **Option 1** drop-down list.

Step 5 Choose from one of the NAS ID options from the **Option 2** drop-down list.

Step 6 Choose from one of the NAS ID options from the **Option 3** drop-down list.

Step 7 Save the configuration.

Creating a NAS ID Policy

Follow the procedure given below to create NAS ID policy:

Before you begin

- NAS ID can be a combination of multiple NAS ID options; the maximum options are limited to 3.
- The maximum length of the NAS ID attribute is 253. Before adding a new attribute, the attribute buffer is checked, and if there is no sufficient space, the new attribute is ignored.
- By default, a wirleess aaa policy (default-aaa-policy) is created with the default configuration (sys-name). You can update this policy with various NAS ID options. However, the default-aaa-policy cannot be deleted.
- If a NAS ID is not configured, the default sys-name is considered as the NAS ID for all wireless-specific RADIUS packets (authentication and accounting) from the controller .

Procedure

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

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**wireless aaa policy** *policy-name* **Example:** `Device(config)# wireless aaa policy test`	Configures a new AAA policy.
Step 3	**nas-id option1 sys-name** **Example:** `Device(config-aaa-policy)# nas-id option1 sys-name`	Configures NAS ID for option1.
Step 4	**nas-id option2 sys-ip** **Example:** `Device(config-aaa-policy)# nas-id option2 sys-ip`	Configures NAS ID for option2.
Step 5	**nas-id option3 sys-mac** **Example:** `Device(config-aaa-policy)# nas-id option3 sys-mac`	Configures NAS ID for option3.

Attaching a Policy to a Tag (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > Tags** page, click **Policy** tab.

Step 2 Click **Add** to view the **Add Policy Tag** window.

Step 3 Enter a name and description for the policy tag.

Step 4 Click **Add** to map WLAN profile and Policy profile.

Step 5 Choose the **WLAN Profile** to map with the appropriate **Policy Profile**, and click the tick icon.

Step 6 Click **Save & Apply to Device**.

Attaching a Policy to a Tag (CLI)

Follow the procedure given below to attach a NAS ID policy to a tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-name* **Example:** `Device(config)# wireless profile policy test1`	Configures a WLAN policy profile.
Step 3	**aaa-policy** *aaa-policy-name* **Example:** `Device(config-wireless-policy)# aaa-policy policy-aaa`	Configures a AAA policy profile.
Step 4	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.
Step 5	**wireless tag policy** *policy-tag* **Example:** `Device(config)# wireless tag policy policy-tag1`	Configures a wireless policy tag.
Step 6	**wlan wlan1 policy** *policy-name* **Example:** `Device(config)# wlan wlan1 policy test1`	Maps a WLAN profile to a policy profile. **Note** You can also use the **ap-tag** option to configure a NAS ID for an AP group, which will override the NAS ID that is configured for a WLAN profile or the VLAN interface.

Verifying the NAS ID Configuration

Use the following **show** command to verify the NAS ID configuration:

```
Device# show wireless profile policy detailed test1

Policy Profile Name           : test1
Description                   :
Status                        : ENABLED
VLAN                          : 1
Client count                  : 0

:
:
AAA Policy Params
```

```
AAA Override                : DISABLED
NAC                         : DISABLED
AAA Policy name             : test
```

CHAPTER 112

DHCP for WLANs

- Information About Dynamic Host Configuration Protocol, on page 1113
- Restrictions for Configuring DHCP for WLANs, on page 1116
- How to Configure DHCP for WLANs, on page 1116
- Configuring the Internal DHCP Server, on page 1118

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 device contains an internal DHCP server. This server is typically used in branch offices that do not 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 APs are supported. If you want to use the internal DHCP server, ensure that you configure SVI for the client VLAN, and set the IP address as DHCP server IP address.

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

When clients use the internal DHCP server of the device, 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.

General Guidelines

- Internal DHCP server serves both wireless client and wired client (wired client includes AP).

- To serve wireless client with internal DHCP server, an unicast DHCP server IP address must be configured for wireless client. Internal DHCP server IP address must be configured under the server facing interface, which can be loopback interface, SVI interface, or L3 physical interface.
- To use internal DHCP server for both wireless and wired client VLAN, an IP address must be configured under client VLAN SVI interface.
- For wireless client, in DHCP helper address configuration, the IP address of the internal DHCP server must be different from address of wireless client VLAN SVI interface.
- For wireless client with internal DHCP server support, the internal DHCP server can be configured using global configuration command, under the client VLAN SVI interface or under the wireless policy profile.
- An internal DHCP server pool can also serve clients of other controllers .

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 in 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 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 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 ask all clients to obtain their IP addresses from a DHCP server. To enforce this requirement, you can configure all the WLANs with a DHCP Address. Assignment Required setting, which disallows client static IP addresses. If DHCP Address Assignment Required is selected, clients must obtain an IP address through 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 to the DHCP server and as a DHCP server at the virtual IP address to wireless clients.

You can create WLANs with DHCP Address Assignment Required disabled. If you do this, clients have the option of using a static IP address or obtaining an IP address from a designated DHCP server. However, note that this might compromise security.

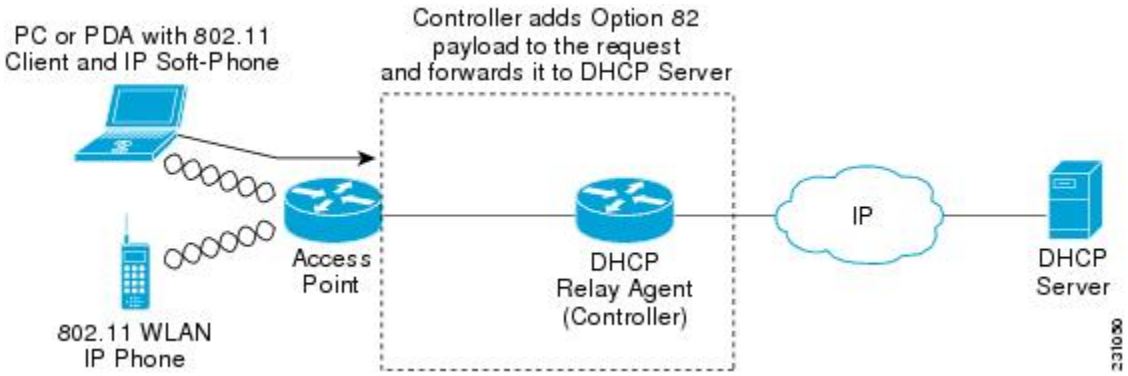
Note DHCP Address Assignment Required is not supported for wired guest LANs.

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

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 27: DHCP Option 82



The AP forwards all the 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 AP, depending on how you configure this option.

Note 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.

Restrictions for Configuring DHCP for WLANs

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

  You can configure DHCP service in either of the following ways:

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

How to Configure DHCP for WLANs

Configuring DHCP Scopes (GUI)

Procedure

Step 1	Choose **Administration** > **DHCP Pools**.
Step 2	In the **Pools** section, click **Add** to add a new DHCP pool. The **Create DHCP Pool** dialog box is displayed.
Step 3	In the **DHCP Pool Name** field, enter a name for the new DHCP pool.
Step 4	From the **IP Type** drop-down list, choose the IP address type.
Step 5	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 in the **Interfaces** window.
Step 6	In the **Subnet Mask** field, enter the subnet mask assigned to all the wireless clients.
Step 7	In the **Starting ip** field, enter the starting IP address.
Step 8	In the **Ending ip** field, enter the trailing IP address.
Step 9	In the **Reserved Only** field, enable or disable it.
Step 10	From the **Lease** drop-down list, choose the lease type as either **User Defined** or **Never Expires**. If you choose User Defined, you can enter the amount of time that an IP address is granted to a client.
Step 11	To perform advanced configuration for DHCP scope, click **Advanced**.
Step 12	Check the **Enable DNS Proxy** check box to enable DNS proxy.

Step 13 In the **Default Router(s)** field, enter the IP address of the optional router or routers that connect to the device and click the + icon to add them to the list. Each router must include a DHCP forwarding agent that enables a single device to serve the clients of multiple devices.

Step 14 In the **DNS Server(s)** field, enter the IP address of the optional DNS server or servers and click the + icon to add them to the list. Each DNS server must be able to update a client's DNS entry to match the IP address assigned by the DHCP scope.

Step 15 In the **NetBios Name Server(s)** field, enter the IP address of the optional Microsoft NetBIOS name server or servers, such as Microsoft Windows Internet Naming Service (WINS) server, and click the + icon to add them to the list.

Step 16 In the **Domain** field, enter the optional domain name of the DHCP scope for use with one or more DNS servers.

Step 17 To add **DHCP** options, click **Add** in the **DHCP Options List** section. DHCP provides an internal framework for passing configuration parameters and other control information, such as DHCP options, to the clients on your network. DHCP options carry parameters as tagged data stored within protocol messages exchanged between the DHCP server and its clients.

Step 18 Enter the **DHCP** option that you want to add.

Step 19 Click **Save & Apply to Device**.

Configuring DHCP Scopes (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip dhcp pool** *pool-name* **Example:** `Device(config)# ip dhcp pool test-pool`	Configures the DHCP pool address.
Step 3	**network** *network-name mask-address* **Example:** `Device(dhcp-config)# network 209.165.200.224 255.255.255.0`	Specifies the network number in dotted-decimal notation and the mask address.
Step 4	**dns-server** *hostname* **Example:** `Device(dhcp-config)# dns-server example.com`	Specifies the DNS name server. You can specify an IP address or a hostname.
Step 5	**end** **Example:** `Device(dhcp-config)# end`	Returns to privileged EXEC mode.

Configuring the Internal DHCP Server

Configuring the Internal DHCP Server Under Client VLAN SVI (GUI)

Procedure

Step 1 Choose **Configuration** > **Layer2** > **VLAN** > **SVI**.

Step 2 Click an SVI.

Step 3 Click the **Advanced** tab.

Step 4 Under **DHCP Relay** settings, enter the **IPV4 Helper Address**.

Step 5 Click **Update & Apply to Device**.

Configuring the Internal DHCP Server Under Client VLAN SVI (CLI)

Before you begin

- For wireless clients, only two DHCP servers are supported.
- To use the internal DHCP server for both wireless and wired client VLAN, an IP address must be configured under the client VLAN SVI.
- For wireless clients, the IP address of the internal DHCP server must be different from the address of the wireless client VLAN SVI (in the DHCP helper address configuration).
- For wireless clients, the internal DHCP server can be configured under the client VLAN SVI or under the wireless policy profile.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface loopback** *interface-number* **Example:** `Device(config)# interface Loopback0`	Creates a loopback interface and enters interface configuration mode.
Step 3	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 10.10.10.1 255.255.255.255`	Configures the IP address for the interface.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 5	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 32`	Configures the VLAN ID.
Step 6	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 192.168.32.100 255.255.255.0`	Configures the IP address for the interface.
Step 7	**ip helper-address** *ip-address* **Example:** `Device(config-if)# ip helper-address 10.10.10.1`	Configures the destination address for UDP broadcasts. **Note** If the IP address used in the **ip helper-address** command is an internal address of the controller an internal DHCP server is used. Otherwise, the external DHCP server is used.
Step 8	**no mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables the Maintenance Operation Protocol (MOP) for an interface.
Step 9	**no mop sysid** **Example:** `Device(config-if)# no mop sysid`	Disables the task of sending MOP periodic system ID messages.
Step 10	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 11	**ip dhcp excluded-address** *ip-address* **Example:** `Device(config)# ip dhcp excluded-address 192.168.32.1`	Specifies the IP address that the DHCP server should not assign to DHCP clients.
Step 12	**ip dhcp excluded-address** *ip-address* **Example:** `Device(config)# ip dhcp excluded-address 192.168.32.100`	Specifies the IP addresses that the DHCP server should not assign to DHCP clients.

	Command or Action	Purpose
Step 13	**ip dhcp pool** *pool-name* **Example:** `Device(config)# ip dhcp pool pool-vlan32`	Configures the DHCP pool address.
Step 14	**network** *network-name mask-address* **Example:** `Device(dhcp-config)# network 192.168.32.0 255.255.255.0`	Specifies the network number in dotted-decimal notation, along with the mask address.
Step 15	**default-router** *ip-address* **Example:** `Device(dhcp-config)# default-router 192.168.32.1`	Specifies the IP address of the default router for a DHCP client.
Step 16	**exit** **Example:** `Device(dhcp-config)# exit`	Exits DHCP configuration mode.
Step 17	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures the WLAN policy profile and enters wireless policy configuration mode.
Step 18	**central association** **Example:** `Device(config-wireless-policy)# central association`	Configures central association for locally switched clients.
Step 19	**central dhcp** **Example:** `Device(config-wireless-policy)# central dhcp`	Configures the central DHCP for locally switched clients.
Step 20	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures WLAN for central switching.
Step 21	**description** *policy-proile-name* **Example:** `Device(config-wireless-policy)# description "default policy profile"`	Adds a description for the policy profile
Step 22	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan 32`	Assigns the profile policy to the VLAN.

	Command or Action	Purpose
Step 23	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless profile policy.

Configuring the Internal DHCP Server Under a Wireless Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click a policy name.

Step 3 Click the **Advanced** tab.

Step 4 Under **DHCP** settings, check or uncheck the **IPv4 DHCP Required** check box and enter the **DHCP Server IP Address**.

Step 5 Click **Update & Apply to Device**.

Configuring the Internal DHCP Server Under a Wireless Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface loopback** *interface-number* **Example:** `Device(config)# interface Loopback0`	Creates a loopback interface and enters interface configuration mode.
Step 3	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 10.10.10.1 255.255.255.255`	Configures the IP address for the interface.
Step 4	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 5	**interface vlan** *vlan-id* **Example:**	Configures the VLAN ID.

	Command or Action	Purpose
	`Device(config)# interface vlan 32`	
Step 6	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 192.168.32.100 255.255.255.0`	Configures the IP address for the interface.
Step 7	**no mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables the Maintenance Operation Protocol (MOP) for an interface.
Step 8	**no mop sysid** **Example:** `Device(config-if)# no mop sysid`	Disables the task of sending MOP periodic system ID messages.
Step 9	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 10	**ip dhcp excluded-address** *ip-address* **Example:** `Device(config)# ip dhcp excluded-address 192.168.32.100`	Specifies the IP address that the DHCP server should not assign to DHCP clients.
Step 11	**ip dhcp pool** *pool-name* **Example:** `Device(config)# ip dhcp pool pool-vlan32`	Configures the DHCP pool address.
Step 12	**network** *network-name mask-address* **Example:** `Device(dhcp-config)# network 192.168.32.0 255.255.255.0`	Specifies the network number in dotted-decimal notation along with the mask address.
Step 13	**default-router** *ip-address* **Example:** `Device(dhcp-config)# default-router 192.168.32.1`	Specifies the IP address of the default router for a DHCP client.
Step 14	**exit** **Example:** `Device(dhcp-config)# exit`	Exits DHCP configuration mode.
Step 15	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures a WLAN policy profile and enters wireless policy configuration mode.

	Command or Action	Purpose
Step 16	**central association** **Example:** `Device(config-wireless-policy)# central association`	Configures central association for locally switched clients.
Step 17	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures local switching.
Step 18	**description** *policy-proile-name* **Example:** `Device(config-wireless-policy)# description "default policy profile"`	Adds a description for the policy profile.
Step 19	**ipv4 dhcp opt82** **Example:** `Device(config-wireless-policy)# ipv4 dhcp opt82`	Enables DHCP Option 82 for the wireless clients.
Step 20	**ipv4 dhcp opt82 ascii** **Example:** `Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	Enables ASCII on DHCP Option 82.
Step 21	**ipv4 dhcp opt82 format vlan_id** **Example:** `Device(config-wireless-policy)# ipv4 dhcp opt82 format vlan32`	Enables VLAN ID.
Step 22	**ipv4 dhcp opt82 rid** *vlan_id* **Example:** `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	Supports the addition of Cisco 2-byte Remote ID (RID) for DHCP Option 82.
Step 23	**ipv4 dhcp server** *ip-address* **Example:** `Device(config-wireless-policy)#  ipv4 dhcp server 10.10.10.1`	Configures the WLAN's IPv4 DHCP server.
Step 24	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan 32`	Assigns the profile policy to the VLAN.
Step 25	**no shutdown** **Example:**	Enables the wireless profile policy.

	Command or Action	Purpose
	`Device(config-wireless-policy)# no shutdown`	

Configuring the Internal DHCP Server Globally (GUI)

Procedure

Step 1 Choose **Administration** > **DHCP Pools** > **Pools**.

Step 2 Click **Add**.

The **Create DHCP Pool** window is displayed.

Step 3 Enter the **DHCP Pool Name**, **Network**, **Starting ip**, and **Ending ip**.

Step 4 From the **IP Type**, **Subnet Mask**, and **Lease** drop-down lists, choose a value.

Step 5 Click the **Reserved Only** toggle button.

Step 6 Click **Apply to Device**.

Configuring the Internal DHCP Server Globally (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface loopback** *interface-num* **Example:** `Device(config)# interface Loopback0`	Creates a loopback interface and enters interface configuration mode.
Step 3	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 10.10.10.1 255.255.255.255`	Configures the IP address for the interface.
Step 4	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 5	**interface vlan***vlan-id* **Example:** `Device(config)# interface vlan 32`	Configures the VLAN ID.

	Command or Action	Purpose
Step 6	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 192.168.32.100 255.255.255.0`	Configures the IP address for the interface.
Step 7	**no mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables the Maintenance Operation Protocol (MOP) for an interface.
Step 8	**no mop sysid** **Example:** `Device(config-if)# no mop sysid`	Disables the task of sending the MOP periodic system ID messages.
Step 9	**exit** **Example:** `Device(config-if)# exit`	Exits the interface configuration mode.
Step 10	**ip dhcp-server** *ip-address* **Example:** `Device(config)# ip dhcp-server 10.10.10.1`	Specifies the target DHCP server parameters.
Step 11	**ip dhcp excluded-address** *ip-address* **Example:** `Device(config)# ip dhcp excluded-address 192.168.32.100`	Specifies the IP address that the DHCP server should not assign to DHCP clients.
Step 12	**ip dhcp pool** *pool-name* **Example:** `Device(config)# ip dhcp pool pool-vlan32`	Configures the DHCP pool address.
Step 13	**network** *network-name mask-address* **Example:** `Device(dhcp-config)# network 192.168.32.0 255.255.255.0`	Specifies the network number in dotted-decimal notation along with the mask address.
Step 14	**default-router** *ip-address* **Example:** `Device(dhcp-config)# default-router 192.168.32.1`	Specifies the IP address of the default router for a DHCP client.
Step 15	**exit** **Example:** `Device(dhcp-config)# exit`	Exits DHCP configuration mode.

	Command or Action	Purpose
Step 16	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 17	**central association** **Example:** `Device(config-wireless-policy)# central association`	Configures central association for locally switched clients.
Step 18	**central dhcp** **Example:** `Device(config-wireless-policy)# central dhcp`	Configures central DHCP for locally switched clients.
Step 19	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures local switching.
Step 20	**description** *policy-proile-name* **Example:** `Device(config-wireless-policy)# description "default policy profile"`	Adds a description for the policy profile.
Step 21	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan 32`	Assigns the profile policy to the VLAN.
Step 22	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the profile policy.

Verifying Internal DHCP Configuration

To verify client binding, use the following command:

```
Device# show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration        Type       State
Interface
                Hardware address/
                User name
192.168.32.3    0130.b49e.491a.53       Mar 23 2018 06:42 PM    Automatic  Active
Loopback0
```

To verify the DHCP relay statistics for a wireless client, use the following command:

```
Device# show wireless dhcp relay statistics

DHCP Relay Statistics
---------------------

DHCP Server IP :   10.10.10.1

Message              Count
--------------------------
DHCPDISCOVER      :  1
BOOTP FORWARD     :  137
BOOTP REPLY       :  0
DHCPOFFER         :  0
DHCPREQUEST       :  54
DHCPACK           :  0
DHCPNAK           :  0
DHCPDECLINE       :  0
DHCPRELEASE       :  0
DHCPINFORM        :  82

Tx/Rx Time :
------------
LastTxTime : 18:42:18
LastRxTime : 00:00:00

Drop Counter :
-------------
TxDropCount : 0
```

To verify the DHCP packet punt statistics in CPP, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless punt statistics

CPP Wireless Punt stats:

                                App Tag     Packet Count
                                -------     ------------
         CAPWAP_PKT_TYPE_DOT11_PROBE_REQ           14442
              CAPWAP_PKT_TYPE_DOT11_MGMT              50
              CAPWAP_PKT_TYPE_DOT11_IAPP            9447
              CAPWAP_PKT_TYPE_DOT11_RFID               0
               CAPWAP_PKT_TYPE_DOT11_RRM               0
            CAPWAP_PKT_TYPE_DOT11_DOT1X                0
       CAPWAP_PKT_TYPE_CAPWAP_KEEPALIVE             2191
     CAPWAP_PKT_TYPE_MOBILITY_KEEPALIVE                0
           CAPWAP_PKT_TYPE_CAPWAP_CNTRL             7034
            CAPWAP_PKT_TYPE_CAPWAP_DATA                0
        CAPWAP_PKT_TYPE_MOBILITY_CNTRL                 0
                      WLS_SMD_WEBAUTH                  0
                    SISF_PKT_TYPE_ARP              5292
                   SISF_PKT_TYPE_DHCP               140
                  SISF_PKT_TYPE_DHCP6              1213
                SISF_PKT_TYPE_IPV6_ND               350
              SISF_PKT_TYPE_DATA_GLEAN                44
           SISF_PKT_TYPE_DATA_GLEAN_V6                51
              SISF_PKT_TYPE_DHCP_RELAY               122
         CAPWAP_PKT_TYPE_CAPWAP_RESERVED                0
```

CHAPTER 113

WLAN Security

- Information About WPA1 and WPA2, on page 1129
- Information About AAA Override, on page 1130
- Prerequisites for Layer 2 Security, on page 1130
- How to Configure WLAN Security, on page 1131

Information About WPA1 and WPA2

Wi-Fi Protected Access (WPA or WPA1) and WPA2 are standards-based security solutions from the Wi-Fi Alliance that provide data protection and access control for wireless LAN systems. WPA1 is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification; WPA2 is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard.

By default, WPA1 uses Temporal Key Integrity Protocol (TKIP) and Message Integrity Check (MIC) for data protection while WPA2 uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). By default, both WPA1 and WPA2 use the 802.1X for authenticated key management. However, the following options are also available:

- 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 clients and authentication server.
- Cisco Centralized Key Management 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). Cisco Centralized Key Management reduces the time required by the client to mutually authenticate with the new access point and derive a new session key during reassociation. Cisco Centralized Key Management 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. Cisco Centralized Key Management is a CCXv4-compliant feature. If Cisco Centralized Key Management is selected, only Cisco Centralized Key Management clients are supported.

  When Cisco Centralized Key Management 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 Cisco Centralized Key Management enabled in a Robust Secure Network Information Element (RSN IE) but Cisco Centralized Key Management 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 Cisco Centralized Key Management enabled in RSN IE and Cisco Centralized Key Management IE is encoded and only PMKID is present in the RSN IE, then the AP does a full authentication. The access point does not use PMKID sent with the association request when Cisco Centralized Key Management is enabled in RSN IE.

- 802.1X+Cisco Centralized Key Management—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 Cisco Centralized Key Management fast secure roaming, Cisco Centralized Key Management-enabled clients securely roam from one access point to another without the need to reauthenticate to the RADIUS server. 802.1X+Cisco Centralized Key Management is considered as an optional Cisco Centralized Key Management because both Cisco Centralized Key Management and non-Cisco Centralized Key Management clients are supported when this option is selected.

On a single WLAN, you can allow WPA1, WPA2, and 802.1X/PSK/Cisco Centralized Key Management/802.1X+Cisco Centralized Key Management clients to join. All of the access points on such a WLAN advertise WPA1, WPA2, and 802.1X/PSK/Cisco Centralized Key Management/ 802.1X+Cisco Centralized Key Management 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.

Information About AAA Override

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

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)
- 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)

How to Configure WLAN Security

Configuring Static WEP Layer 2 Security Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **WLANs** page, click the name of the WLAN.

Step 3 In the **Edit WLAN** window, click the **Security** tab.

Step 4 From the **Layer 2 Security Mode** drop-down list, select the **Static WEP** option.

Step 5 (Optional) Check the **Shared Key Authentication** check box to set the authentication type as shared. By leaving the check box unchecked, the authentication type is set to open.

Step 6 Set the **Key Size** as either **40 bits** or **104 bits**.

- 40 bits: The keys with 40-bit encryption must contain 5 ASCII text characters or 10 hexadecimal characters.
- 104 bits: The keys with 104-bit encryption must contain 13 ASCII text characters or 26 hexadecimal characters.

Step 7 Set the appropriate **Key Index**; you can choose between 1 to 4.

Step 8 Set the **Key Format** as either **ASCII** or **Hex**.

Step 9 Enter a valid **Encryption Key**.

- 40 bits: The keys with 40-bit encryption must contain 5 ASCII text characters or 10 hexadecimal characters.
- 104 bits: The keys with 104-bit encryption must contain 13 ASCII text characters or 26 hexadecimal characters.

Step 10 Click **Update & Apply to Device**.

Configuring Static WEP Layer 2 Security Parameters (CLI)

Before you begin

You must have administrator privileges.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device# wlan test4 1 test4`	Enters the WLAN configuration submode. *profile-name* is the profile name of the configured WLAN. *wlan-id* is the wireless LAN identifier. The range is 1 to 512. *SSID_Name* is the SSID which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *profile-name* command.
Step 3	**disable ft** **Example:** `Device(config-wlan)# disable ft`	Disables fast transition.
Step 4	**no security ft over-the-ds** **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables fast transition over the data source on the WLAN.
Step 5	**no security ft** **Example:** `Device(config-wlan)# no security ft`	Disables 802.11r Fast Transition on the WLAN.
Step 6	**no security wpa**{**akm** | **wpa1** | **wpa2**} **Example:** `Device(config-wlan)# no security wpa wpa1 ciphers tkip`	Disables the WPA/WPA2 support for a WLAN.
Step 7	**security static-wep-key** [**authentication** {**open** | **shared**}] **Example:** `Device(config-wlan)# security static-wep-key authentication open`	The keywords are as follows: • **static-wep-key**—Configures Static WEP Key authentication. • **authentication**—Specifies the authentication type you can set. The values are open and shared.
Step 8	**security static-wep-key** [**encryption** {**104** | **40**} {**ascii** | **hex**} [**0** | **8**]]	The keywords are as follows:

	Command or Action	Purpose
	Example: `Device(config-wlan)# security static-wep-key encryption 104 ascii 0 1234567890123 1`	• **static-wep-key**—Configures Static WEP Key authentication. • **encryption**—Specifies the encryption type that you can set. The valid values are 104 and 40. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters. • **ascii**—Specifies the key format as ASCII. • **hex**—Specifies the key format as HEX.
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring WPA + WPA2 Layer 2 Security Parameters (GUI)

Procedure

Step 1 Click **Configuration** > **Tags and Profiles** > **WLANs**.

Step 2 Click **Add** to add a new WLAN Profile or click the one you want to edit.

Step 3 In the **Edit WLAN** window, click **Security** > **Layer2**.

Step 4 From **Layer 2 Security Mode** drop-down menu, select **WPA + WPA2**.

Step 5 Configure the security parameters and then click **Save and Apply to Device**.

Configuring WPA + WPA2 Layer 2 Security Parameters (CLI)

Note The default values for security policy WPA2 are:

- Encryption is AES.
- Authentication Key Management (AKM) is dot1x.

Before you begin

You must have administrator privileges.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device# wlan test4 1 test4`	Enters the WLAN configuration submode. • *profile-name* is the profile name of the configured WLAN. • *wlan-id* is the wireless LAN identifier. The range is 1 to 512. • *SSID_Name* is the SSID that contains 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *profile-name* command.
Step 3	**security wpa {akm | wpa1 | wpa2}** **Example:** `Device(config-wlan)# security wpa`	Enables WPA or WPA2 support for WLAN.
Step 4	**security wpa wpa1** **Example:** `Device(config-wlan)# security wpa wpa1`	Enables WPA.
Step 5	**security wpa wpa1 ciphers** [**aes** | **tkip**] **Example:** `Device(config-wlan)# security wpa wpa1 ciphers aes`	Specifies the WPA1 cipher. Choose one of the following encryption types: • **aes**—Specifies WPA/AES support. • **tkip**—Specifies WPA/TKIP support. The default values are TKIP for WPA1 and AES for WPA2. **Note** You can enable or disable TKIP encryption only using the CLI. Configuring TKIP encryption is not supported in GUI. When you have VLAN configuration on WGB, you need to configure the encryption cipher mode and keys for a particular VLAN, for example, **encryption vlan 80 mode ciphers tkip**. Then, you need to configure the encryption cipher mode globally on the

	Command or Action	Purpose
		multicast interface by entering the following command: **encryption mode ciphers tkip**.
Step 6	**security wpa akm** {**cckm**| **dot1x**	**dot1x-sha256**	**ft**	**psk** |**psk-sha256**} **Example:** `Device(config-wlan)# security wpa akm psk-sha256`	Enable or disable Cisco Centralized Key Management, 802.1x, 802.1x with SHA256 key derivation type, Fast Transition, PSK or PSK with SHA256 key derivation type. **Note** • You cannot enable 802.1x and PSK with SHA256 key derivation type simultaneously. • When you configure Cisco Centralized Key Management SSID, you must enable the **ccx aironet-iesupport** for Cisco Centralized Key Management to work. • WPA3 Enterprise dot1x-sha256 is supported only in local mode.
Step 7	**security wpa psk set-key** {**ascii**	**hex**} {**0**	**8**} *password* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 test`	Enter this command to specify a preshared key, if you have enabled PSK. WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
Step 8	**security wpa akm ft** {**dot1x**	**psk**	**sae**} **Example:** `Device(config-wlan)# security wpa akm ft psk`	Enable or disable authentication key management suite for fast transition. **Note** You can now choose between PSK and fast transition PSK as the AKM suite.
Step 9	**security wpa wpa2** **Example:** `Device(config-wlan)# security wpa wpa2`	Enables WPA2.
Step 10	**security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# security wpa wpa2` **Example:**	Configure WPA2 cipher. • **aes**—Specifies WPA/AES support.
Step 11	**show wireless pmk-cache**	Displays the remaining time before the PMK cache lifetime timer expires.

	Command or Action	Purpose
		If you have enabled WPA2 with 802.1X authenticated key management or WPA1 or WPA2 with Cisco Centralized Key Management 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. **Note** • The command will show VLAN ID with VLAN pooling feature in VLAN-Override field. • Sticky key caching (SKC) is not supported.

CHAPTER 114

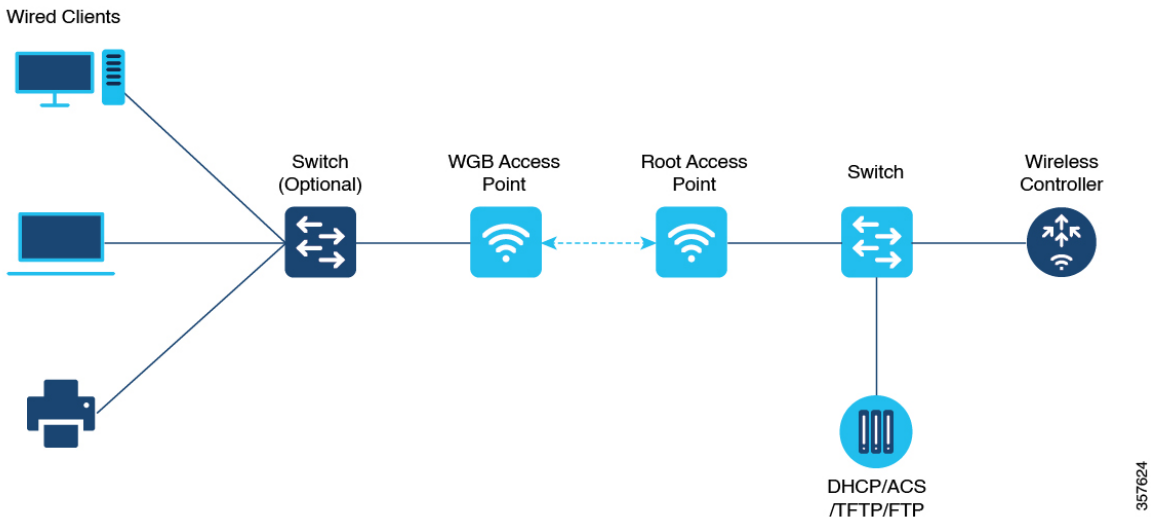
Workgroup Bridges

- Cisco Workgroup Bridges, on page 1137
- Configuring Workgroup Bridge on a WLAN, on page 1139
- Verifying the Status of a Workgroup Bridge on the Controller, on page 1140
- Configuring Access Points as Workgroup Bridge, on page 1141

Cisco Workgroup Bridges

A workgroup bridge (WGB) is an Access Point (AP) mode to provide wireless connectivity to wired clients that are connected to the Ethernet port of the WGB AP. A WGB connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the WLC through infrastructure AP using Internet Access Point Protocol (IAPP) messaging. The WGB establishes a single wireless connection to the root AP, which in turn, treats the WGB as a wireless client.

Figure 28: Example of a WGB



The following features are supported for use with a WGB:

Table 53: WGB Feature Matrix

Feature	Cisco Wave 1 APs	Cisco Wave 2
802.11r	Supported	Supported
QOS	Supported	Supported
UWGB mode	Supported	Supported on Wave 2 APs
IGMP Snooping or Multicast	Supported	Supported
802.11w	Supported	Supported
PI support (without SNMP)	Supported	Not supported
IPv6	Supported	Supported
VLAN	Supported	Supported
802.11i (WPAv2)	Supported	Supported
Broadcast tagging/replicate	Supported	Supported
Unified VLAN client	Implicitly supported (No CLI required)	Supported
WGB client	Supported	Supported
802.1x – PEAP, EAP-FAST, EAP-TLS	Supported	Supported
NTP	Supported	Supported
Wired client support on all LAN ports	Supported in Wired-0 and Wired-1 interfaces	Supported in all Wired-0, 1 and LAN ports 1, 2, and 3

The following table shows the supported and unsupported authentication and switching modes for Cisco APs when connecting to a WGB.

Table 54: Supported Access Points and Requirements

Access Points	Requirements
Cisco Aironet 2700, 3700, and 1572 Series	Requires autonomous image.
Cisco Aironet 2800, 3800, 4800, 1562, and Cisco Catalyst 9105, 9115, IW6300 and ESW6300 Series	CAPWAP image starting from Cisco AireOS 8.8 release.

- MAC filtering is not supported for wired clients.
- Idle timeout is not supported for both WGB and wired clients.
- Session timeout is not applicable for wired clients.
- Web authentication is not supported.

- WGB supports only up to 20 clients.
- If you want to use a chain of certificates, copy all the CA certificates to a file and install it under a trust point on the WGB, else server certificate validation may fail.
- 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 root AP, create a WLAN and make sure that Aironet IE is enabled under the Advanced settings.

Configuring Workgroup Bridge on a WLAN

Follow the procedure given below to configure a WGB on a WLAN:

For WGB to join a wireless network there are specific settings on the WLAN and on the related policy profile.

Note For the configuration given below, it is assumed that the WLAN security is already configured.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan WGB_Test`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**ccx aironet-iesupport** **Example:** `Device(config-wlan)# ccx aironet-iesupport`	Configures the Cisco Client Extensions option and sets the support of Aironet IE on the WLAN.
Step 4	**exit** **Example:** `Device(config-wlan)# exit`	Exits the WLAN configuration submode.
Step 5	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy test-wgb`	Configures WLAN policy profile and enters the wireless policy configuration mode.

	Command or Action	Purpose
Step 6	**description** *description* **Example:** `Device(config-wireless-policy)# description "test-wgb"`	Adds a description for the policy profile.
Step 7	**vlan** *vlan-no* **Example:** `Device(config-wireless-policy)# vlan 48`	Assigns the profile policy to the VLAN.
Step 8	**wgb vlan** **Example:** `Device(config-wireless-policy)# wgb vlan`	Configures WGB VLAN client support.
Step 9	**wgb broadcast-tagging** **Example:** `Device(config-wireless-policy)# wgb broadcast-tagging`	Configures WGB broadcast tagging on a WLAN.
Step 10	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Restarts the policy profile.
Step 11	**exit** **Example:** `Device(config-wireless-policy)# exit`	Exits the wireless policy configuration mode.
Step 12	**wireless tag policy** *policy-tag* **Example:** `Device(config)# wireless tag policy WGB_Policy`	Configures policy tag and enters policy tag configuration mode.
Step 13	**wlan** *profile-name* **policy** *profile-policy* **Example:** `Device(config-policy-tag)# wlan WGB_Test policy test-wgb`	Maps a policy profile to a WLAN profile.
Step 14	**end** **Example:** `Device(config-policy-tag)# end`	Exits policy tag configuration mode, and returns to privileged EXEC mode.

Verifying the Status of a Workgroup Bridge on the Controller

Use the following commands to verify the status of a WGB.

To display the wireless-specific configuration of active clients, use the following command:

```
Device# show wireless client summary
```

To display the WGBs on your network, use the following command:

```
Device# show wireless wgb summary
```

To display the details of wired clients that are connected to a particular WGB, use the following command:

```
Device# show wireless wgb mac-address 00:0d:ed:dd:25:82 detail
```

Configuring Access Points as Workgroup Bridge

Turning Cisco Aironet 2700/3700/1572 Series AP into Autonomous Mode

Before you begin

Download the autonomous image for the specific access point from software.cisco.com and place it on a TFTP server.

Procedure

	Command or Action	Purpose
Step 1	**debug capwap console cli** **Example:** `Device# debug capwap console cli`	Enables the console CLI.
Step 2	**archive download-sw force-reload overwrite tftp:***ipaddress filepath filename* **Example:** `Device(config)# archive download-sw force-reload overwrite tftp://10.10.10.1/tftp/c1800.tar`	Downloads the autonomous image to the access point.

Configuring Cisco Wave 2 APs in Workgroup Bridge or CAPWAP AP Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters in to the privileged mode of the AP.

	Command or Action	Purpose
Step 2	**ap-type workgroup-bridge** **Example:** `Device# ap-type workgroup-bridge`	Moves the AP in to the Workgroup Bridge mode.

Step 3	**configure ap address ipv4 dhcp** or **configure ap address ipv4 static***ip-address netmask gateway-ipaddress*
	Example:
	DHCP IP Address
	`Device# configure ap address ipv4 dhcp`
	Static IP Address
	`Device# configure ap address ipv4 static 10.10.10.2 255.255.255.234 192.168.4.1`
		Configures DHCP or Static IP address.

Step 4	**configure ap management add username** *username* **password** *password* **secret** *secret* **Example:** `Device# configure ap management add username xyz-user password ****** secret cisco`	Configures an username for the AP management.
Step 5	**configure ap hostname***host-name* **Example:** `Device# configure ap hostname xyz-host`	Configures the AP hostname.

Configure an SSID Profile for Cisco Wave 2 APs (CLI)

This procedure is an AP procedure. The CLIs listed in the procedure given below work only on the AP console and not on the controller.

Procedure

	Command or Action	Purpose
Step 1	**configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication** {**open** | **psk** *preshared-key* **key-management** {**dot11r** | **wpa2** | **dot11w** |{**optional** | **required** }}| **eap profile** *eap-profile-name* **key-management** {**dot11r** | **wpa2** | **dot11w**|{**optional** | **required**}} **Example:** SSID profile with open authentication. `Device# configure ssid-profile test WRT s1 authentication open`	Choose an authentication protocol (Open, PSK, or EAP) for the SSID profile.

	Command or Action	Purpose

	SSID profile with PSK authentication.
	`Device# configure ssid-profile test WRT s1 authentication psk 1234 key-management dot11r optional`
	SSID profile with EAP authentication.
	`Device# configure ssid-profile test WRT s1 authentication eap profile test2 key-management dot11r optional`	

Step 2	**configure dot11radio** *radio-interface* **mode wgb ssid-profile** *profle-name* **Example:** `Device# configure dot11radio r1 mode wgb ssid-profile doc-test`	Attaches an SSID profile to a radio interface.
Step 3	**configure ssid-profile** *profle-name***delete** **Example:** `Device# configure ssid-profile doc-test delete`	(Optional) Deletes an SSID profile.
Step 4	**show wgb ssid** **Example:** `Device# show wgb ssid`	(Optional) Displays summary of configured and connected SSIDs.
Step 5	**show wgb packet statistics** **Example:** `Device# show wgb packet statistics`	(Optional) Displays management, control, and data packet statistics.

Configuring a Dot1X Credential (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure dot1x credential** *profile-name* **username** *name* **password** *password* **Example:** `Device# configure dot1x credential test1 username XYZ password *****`	Configures a dot1x credential.
Step 2	**configure dot1x credential** *profile-name* **delete** **Example:** `Device# configure dot1x credential test1 delete`	Removes a dot1x profile.

	Command or Action	Purpose
Step 3	**clear wgb client** {**all** | **single** *mac-addr* } **Example:** `Device# clear wgb client single xxxx.xxxx.xxxx.xxxx`	Deauthenticates a WGB client.

Configuring an EAP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure eap-profile** *profile-name* **method** {**fast** | **leap** | **peap** | **tls**} **Example:** `Device# configure eap-profile test-eap method fast`	Configures an EAP profile.

Step 2	**configure eap-profile** *profile-name* **trustpoint default** or **configure eap-profile** *profile-name* **trustpoint name** *trustpoint-name*
	Example:
	EAP Profile to Trustpoint with MIC Certificate.
	`Device# configure eap-profile test-eap trustpoint default`
	EAP Profile to Trustpoint with CA Certificate.
	`Device# configure eap-profile test-eap trustpoint cisco`
		Configures an EAP profile with a trustpoint.

Step 3	**configure eap-profile** *profile-name* **trustpoint** {**default** | **name** *trustpoint-name*} **Example:** `Device# configure eap-profile test-eap trustpoint default`	Attaches the CA trustpoint. **Note** With the default profile, WGB uses the internal MIC certificate for authentication.
Step 4	**configure eap-profile** *profile-name* **dot1x-credential** *profile-name* **Example:** `Device# configure eap-profile test-eap dot1x-credential test-profile`	Configures the 802.1X credential profile.
Step 5	**configure eap-profile** *profile-name* **delete** **Example:** `Device# configure eap-profile test-eap delete`	(Optional) Deletes an EAP profile.

	Command or Action	Purpose
Step 6	**show wgb eap dot1x credential profile** **Example:** `Device# show wgb eap dot1x credential profile`	(Optional) Displays the WGB EAP dot1x profile summary.
Step 7	**show wgb eap profile** **Example:** `Device# show wgb eap profile`	(Optional) Displays the EAP profile summary.
Step 8	**show wgb eap profile all** **Example:** `Device# show wgb eap profile all`	(Optional) Displays the EAP and dot1x profiles.

Configuring Manual-Enrollment of a Trustpoint for Workgroup Bridge (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure crypto pki trustpoint** *ca-server-name* **enrollment terminal** **Example:** `Device# configure crypto pki trustpoint ca-server-US enrollment terminal`	Configures a trustpoint in WGB.
Step 2	**configure crypto pki trustpoint** *ca-server-name* **authenticate** **Example:** `Device# configure crypto pki trustpoint ca-server-US authenticate`	Authenticates a trustpoint manuallly. Enter the base 64 encoded CA certificate and end the certificate by entering **quit** in a new line.
Step 3	**configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* **Example:** `Device# configure crypto pki trustpoint ca-server-Us key-size 60`	Configures a private key size.
Step 4	**configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* [*2ltr-country-code* |*state-name* |*locality* |*org-name* |*org-unit* |*email*] **Example:**	Configures the subject name.

	Command or Action	Purpose
	`Device# configure crypto pki trustpoint ca-server-US subject-name test US CA abc cisco AP test@cisco.com`	
Step 5	**configure crypto pki trustpoint** *ca-server-name* **enrol** **Example:** `Device# configure crypto pki trustpoint ca-server-US enroll`	Generates a private key and Certificate Signing Request (CSR). Afterwards, create the digitally signed certificate using the CSR output in the CA server.
Step 6	**configure crypto pki trustpoint** *ca-server-name* **import certificate** **Example:** `Device# configure crypto pki trustpoint ca-server-US import certificate`	Import the signed certificate in WGB. Enter the base 64 encoded CA certificate and end the certificate by using **quit** command in a new line.
Step 7	**configure crypto pki trustpoint** *ca-server-name* **delete** **Example:** `Device# configure crypto pki trustpoint ca-server-US delete`	(Optional) Delete a trustpoint.
Step 8	**show crypto pki trustpoint** **Example:** `Device# show crypto pki trustpoint`	(Optional) Displays the trustpoint summary.
Step 9	**show crypto pki trustpoint** *trustpoint-name* **certificate** **Example:** `Device# show crypto pki trustpoint ca-server-US certificate`	(Optional) Displays the content of the certificates that are created for a trustpoint.

Configuring Auto-Enrollment of a Trustpoint for Workgroup Bridge (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure crypto pki trustpoint** *ca-server-name* **enrollment url** *ca-server-url* **Example:** `Device# configure crypto pki trustpoint`	Enrols a trustpoint in WGB using the server URL.

	Command or Action	Purpose
	`ca-server-US enrollment url https://cisco/certsrv`	
Step 2	**configure crypto pki trustpoint** *ca-server-name* **authenticate** **Example:** `Device# configure crypto pki trustpoint ca-server-US authenticate`	Authenticates a trustpoint by fetching the CA certificate from CA server automatically.
Step 3	**configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* **Example:** `Device# configure crypto pki trustpoint ca-server-Us key-size 60`	Configures a private key size.
Step 4	**configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* [*2ltr-country-code* |*state-name* |*locality* |*org-name* |*org-unit* |*email*] **Example:** `Device# configure crypto pki trustpoint ca-server-US subject-name test US CA abc cisco AP test@cisco.com`	Configures the subject name.
Step 5	**configure crypto pki trustpoint** *ca-server-name* **enrol l** **Example:** `Device# configure crypto pki trustpoint ca-server-US enroll`	Enrols the trustpoint. Request the digitally signed certificate from the CA server.
Step 6	**configure crypto pki trustpoint** *ca-server-name* **auto-enroll enable** *renew-percentage* **Example:** `Device# configure crypto pki trustpoint ca-server-US auto-enroll enable  10`	Enable sauto-enroll of the trustpoint. You can disable auto-enrolling by using the **disable** option in the command.
Step 7	**configure crypto pki trustpoint***trustpoint-name* **delete** **Example:** `Device# configure crypto pki trustpoint ca-server-US delete`	(Optional) Deletes a trustpoint.

	Command or Action	Purpose
Step 8	**show crypto pki trustpoint** **Example:** `Device# show crypto pki trustpoint`	(Optional) Displays the trustpoint summary.
Step 9	**show crypto pki trustpoint***trustpoint-name* **certificate** **Example:** `Device# show crypto pki trustpoint ca-server-US certificate`	(Optional) Displays the content of the certificates that are created for a trustpoint.
Step 10	**show crypto pki timers** **Example:** `Device# show crypto pki timers`	(Optional) Displays the PKI timer information.

Configuring Manual Certificate Enrolment Using TFTP Server (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure crypto pki trustpoint** *ca-server-name* **enrollment tftp** *addr/file-name* **Example:** `Device# configure crypto pki trustpoint ca-server-US enrollment tftp://10.8.0.6/all_cert.txt`	Specifies the enrolment method to retrieve the CA certificate and client certificate for a trustpoint in WGB.
Step 2	**configure crypto pki trustpoint** *ca-server-name* **authenticate** **Example:** `Device# configure crypto pki trustpoint ca-server-US authenticate`	Retrieves the CA certificate and authenticates it from the specified TFTP server. If the file specification is included, the wgb will append the extension ".ca" to the specified filename.
Step 3	**configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* **Example:** `Device# configure crypto pki trustpoint ca-server-Us key-size 60`	Configures a private key size.
Step 4	**configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* [*2ltr-country-code* |*state-name* |*locality* |*org-name* |*org-unit* |*email*]	Configures the subject name.

	Command or Action	Purpose

	Example:
	`Device# configure crypto pki trustpoint`
	
	`ca-server-US subject-name test US CA abc cisco AP test@cisco.com`	

Step 5	**configure crypto pki trustpoint** *ca-server-name* **enrol**
	Example:
	`Device# configure crypto pki trustpoint`
	
	`ca-server-US enroll`
		Generate a private key and Certificate Signing Request (CSR) and writes the request out to the TFTP server. The filename to be written is appended with the extension ".req".

Step 6	**configure crypto pki trustpoint** *ca-server-name* **import certificate**
	Example:
	`Device# configure crypto pki trustpoint`
	
	`ca-server-US import certificate`
		Import the signed certificate in WGB using TFTP at the console terminal, which retrieves the granted certificate.
		The WGB will attempt to retrieve the granted certificate using TFTP using the same filename and the file name append with ".crt" extension.

Step 7	**show crypto pki trustpoint** **Example:** `Device# show crypto pki trustpoint`	(Optional) Displays the trustpoint summary.
Step 8	**show crypto pki trustpoint** *trustpoint-name* **certificate** **Example:** `Device# show crypto pki trustpoint ca-server-US certificate`	(Optional) Displays the content of the certificates that are created for a trustpoint.

Importing the PKCS12 Format Certificates from the TFTP Server (CLI)

Procedure

	Command or Action	Purpose

Step 1	**configure crypto pki trustpoint** *ca-server-name* **import pkcs12 tftp** *addr/file-name* **password** *pwd*
	Example:
	`Device# configure crypto pki trustpoint`
	
	`ca-server-US enrollment tftp://10.8.0.6/all_cert.txt password ******`
		Imports PKCS12 format certificate from the TFTP server.

Step 2	**show crypto pki trustpoint** **Example:**	(Optional) Displays the trustpoint summary.

	Command or Action	Purpose
	`Device# show crypto pki trustpoint`	
Step 3	**show crypto pki trustpoint** *trustpoint-name* **certificate** **Example:** `Device# show crypto pki trustpoint ca-server-US certificate`	(Optional) Displays the content of the certificates that are created for a trustpoint.

Configuring Radio Interface for Workgroup Bridges (CLI)

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.

Procedure

	Command or Action	Purpose
Step 1	**configure dot11radio** *radio-int* **mode root-ap** **Example:** `Device# configure dot11Radio 0/3/0 mode root-ap`	Maps a radio interface as 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.
Step 2	**configure dot11Radio <0|1> beacon-period** *beacon-interval* **Example:** `Device# configure dot11radio 1 beacon-period 120`	Configures the periodic beacon interval in milli-seconds. The value range is between 2 and 2000 milli-seconds.
Step 3	**configure dot11Radio** *radio-int* **mode wgb ssid-profile** *ssid-profile-name* **Example:** `Device# configure dot11Radio 0/3/0 mode wgb ssid-profile bgl18`	Maps a radio interface to a WGB SSID profile.
Step 4	**configure dot11Radio** *radio-int* **mode uwgb** *mac-addr* **ssid-profile** *ssid-profile-name* **Example:** `Device# configure dot11Radio 0/3/0 mode uwgb 0042.5AB6.0EF0 ssid-profile bgl18`	Maps a radio interface to a WGB SSID profile.
Step 5	**configure dot11Radio** *radio-int* {**enable**| **disable**} **Example:** `Device# configure dot11Radio 0/3/0 mode enable`	Configures a radio interface. **Note** After configuring the uplink to the SSID profile, we recommend that you disable and enable the radio for the changes to be active.

	Command or Action	Purpose
Step 6	**configure dot11Radio** *radio-int* **antenna** {**a-antenna** | **ab-antenna** | **abc-antenna** | **abcd-antenna**} **Example:** `Device# configure dot11Radio 0/3/0 antenna a-antenna`	Configures a radio antenna.

Step 7	**configure dot11Radio** *radio-int* **encryption mode ciphers aes-ccm** {
	Example:
	`Device# configure dot11Radio radio-int encryption mode ciphers aes-ccm`
		Configures the radio interface.

Step 8	**configure wgb mobile rate** {**basic 6 9 18 24 36 48 54** | **mcs** *mcs-rate*} **Example:** `Device# configure wgb mobile rate basic 6 9 18 24 36 48 54`	Configures the device channel rate.
Step 9	**configure wgb mobile period** *secondsthres-signal* **Example:** `Device# configure wgb mobile period 30 –50`	Configure the threshold duration and signal strength to trigger scanning.
Step 10	**configure wgb mobile station interface dot11Radio** *radio-int* **scan** *channel-number* **add** **Example:** `Device# configure wgb mobile station interface dot11Radio 0/3/0 scan 2 add`	Configures the static roaming channel.
Step 11	**configure wgb mobile station interface dot11Radio** *radio-int* **scan** *channel-number* **delete** **Example:** `Device# configure wgb mobile station interface dot11Radio 0/3/0 scan 2 delete`	(Optional) Delete the mobile channel.
Step 12	**configure wgb mobile station interface dot11Radio** *radio-int* **scan disable** **Example:** `Device# configure wgb mobile station interface dot11Radio 0/3/0 scan disable`	(Optional) Disable the mobile channel.

	Command or Action	Purpose
Step 13	**configure wgb beacon miss-count** *value* **Example:** `Device# configure wgb beacon miss-count 12`	(Optional) Configure the beacon miss-count. By default, this 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.
Step 14	**show wgb wifi** *wifi-interface* **stats** **Example:** `Device# show wgb wifi 0/3/0 stats`	(Optional) Displays the Wi-Fi station statistics.
Step 15	**show controllers dot11Radio** *radio-interface* **antenna** **Example:** `Device# show controllers dot11Radio 0/3/0 antenna`	(Optional) Displays the radio antenna statistics.
Step 16	**show wgb mobile scan channel** **Example:** `Device# show wgb mobile scan channel`	(Optional) Displays the mobile station channels scan configuration.
Step 17	**show configuration** **Example:** `Device# show configuration`	(Optional) Displays the configuration that is stored in the NV memory.
Step 18	**show running-config** **Example:** `Device# show running-config`	(Optional) Displays the running configuration in the device.

Configuring Workgroup Bridge Timeouts (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure wgb association response timeout** *response-millisecs* **Example:** `Device# configure wgb association response timeout 4000`	Configures the WGB association response timeout. The default value is 5000 milliseconds. The valid range is between 300 and 5000 milliseconds.
Step 2	**configure wgb authentication response timeout** *response-millisecs*	Configures the WGB authentication response timeout. The default value is 5000 milliseconds.

	Command or Action	Purpose
	Example: `Device# configure wgb authentication response timeout 4000`	The valid range is between 300 and 5000 milliseconds.
Step 3	**configure wgb uclient timeout** *timeout-secs* **Example:** `Device# configure wgb uclient timeout 70`	Configure the Universal WGB client response timeout. The default timeout value is 60 seconds. The valid range is between 1 and 65535 seconds..
Step 4	**configure wgb eap timeout** *timeout-secs* **Example:** `Device# configure wgb eap timeout 20`	Configures the WGB EAP timeout. The default timeout value is 3 seconds. The valid range is between 2 and 60 seconds.
Step 5	**configure wgb channel scan timeout** {**fast**| **medium** | **slow**} **Example:** `Device# configure wgb channel scan timeout slow`	Configures the WGB channel scan timeout.
Step 6	**configure wgb dhcp response timeout** *timeout-secs* **Example:** `Device# configure wgb dhcp response timeout 70`	Configures the WGB DHCP response timeout. The default value is 60 seconds. The valid range is between 1000 and 60000 milliseconds.
Step 7	**show wgb dot11 association** **Example:** `Device# show wgb dot11 association`	Displays the WGB association summary.

Configuring Bridge Forwarding for Workgroup Bridge (CLI)

Before you begin

The Cisco Wave 2 APs 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 need to retain the client entry in the WGB table for a longer duration, we recommend you increase the client WGB bridge timeout duration.

Procedure

	Command or Action	Purpose
Step 1	**configure wgb bridge client add** *mac-address* **Example:** `Device# configure wgb bridge client add F866.F267.7DFB-`	Adds a WGB client using the MAC address.
Step 2	**configure wgb bridge client timeout** *timeout-secs* **Example:** `Device# configure wgb bridge client timeout 400`	Configures the WGB bridge client timeout. Default timeout value is 300 seconds. The valid range is between 10 and 1000000 seconds.
Step 3	**show wgb bridge** **Example:** `Device# show wgb bridge`	Displays the WGB wired clients over the bridge.
Step 4	**show wgb bridge wired gigabitEthernet** *interface* **Example:** `Device# show wgb bridge wired gigabitEthernet 0/1`	Displays the WGB Gigabit wired clients over the bridge.
Step 5	**show wgb bridge dot11Radio** *interface-number* **Example:** `Device# show wgb bridge dot11Radio 0/3/1`	Displays the WGB bridge radio interface summary.

CHAPTER 115

Peer-to-Peer Client Support

- Information About Peer-to-Peer Client Support, on page 1155
- Configure Peer-to-Peer Client Support, on page 1155

Information About Peer-to-Peer Client Support

Peer-to-peer client support can be applied to individual WLANs, with each client inheriting the peer-to-peer blocking setting of the WLAN to which it is associated. The peer-to-Peer Client Support feature provides a granular control over how traffic is directed. For example, you can choose to have traffic bridged locally within a device, dropped by a device, or forwarded to the upstream VLAN.

Peer-to-peer blocking is supported for clients that are associated with local and central switching WLANs.

Restrictions

- Peer-to-peer blocking does not apply to multicast traffic.
- Peer-to-peer blocking is not enabled by default.
- In FlexConnect, peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all the FlexConnect APs that broadcast the SSID.
- FlexConnect central switching clients supports peer-to-peer upstream-forward. However, this is not supported in the FlexConnect local switching. This is treated as peer-to-peer drop and client packets are dropped.

  FlexConnect central switching clients supports peer-to-peer blocking for clients associated with different APs. However, for FlexConnect local switching, this solution targets only clients connected to the same AP. FlexConnect ACLs can be used as a workaround for this limitation.

Configure Peer-to-Peer Client Support

Follow the procedure given below to configure Peer-to-Peer Client Support:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan wlan1`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**peer-blocking** [**drop** | **forward-upstream**] **Example:** `Device(config-wlan)# peer-blocking drop`	Configures peer to peer blocking parameters. The keywords are as follows: • **drop**—Enables peer-to-peer blocking on the drop action. • **forward-upstream**—No action is taken and forwards packets to the upstream. **Note** The **forward-upstream** option is not supported for Flex local switching. Traffic is dropped even if this option is configured. Also, peer to peer blocking for local switching SSIDs are available only for the clients on the same AP.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 5	**show wlan id** *wlan-id* **Example:** `Device# show wlan id 12`	Displays the details of the selected WLAN.

CHAPTER 116

Wireless Guest Access

- Wireless Guest Access, on page 1157
- Load Balancing Among Multiple Guest Controllers, on page 1160
- Guidelines and Limitations for Wireless Guest Access, on page 1161
- Configure Mobility Tunnel for Guest Access (GUI), on page 1161
- Configure Mobility Tunnel for Guest Access (CLI), on page 1161
- Configuring Guest Access Policy (GUI), on page 1162
- Configuring Guest Access Policy (CLI), on page 1162
- Viewing Guest Access Debug Information (CLI), on page 1164
- Configure Guest Access Using Different Security Methods, on page 1165

Wireless Guest Access

The Wireless Guest Access feature addresses the need to provide internet access to guests in a secure and accountable manner. The implementation of a wireless guest network uses the enterprise's existing wireless and wired infrastructure to the maximum extent. This reduces the cost and complexity of building a physical overlay network. Wireless Guest Access solution comprises of two controllers - a Guest Foreign and a Guest Anchor. An administrator can limit bandwidth and shape the guest traffic to avoid impacting the performance of the internal network.

Note

- When a client joins through a capwap tunnel from an AP, the RADIUS NAS-Port-Type is set as "wireless 802.11". Here, Point of Attachment (PoA) and Point of Presence (PoP) is the same.
- When a client joins through a mobility tunnel, the RADIUS NAS-Port-Type is set as "virtual". Here, PoA is the Foreign controller and PoP is the Anchor controller as the client is anchored. For information on the standard types, see the following link:

  https://www.iana.org/assignments/radius-types/radius-types.xhtml#radius-types-13

Wireless Guest Access feature comprises the following functions:

- Guest Anchor controller is the point of presence for a client.
- Guest Anchor Controller provides internal security by forwarding the traffic from a guest client to a Cisco Wireless Controller in the demilitarized zone (DMZ) network through the anchor controller.

- Guest Foreign controller is the point of attachment of the client.
- Guest Foreign Controller is a dedicated guest WLAN or SSID and is implemented throughout the campus wireless network wherever guest access is required. A WLAN with mobility anchor (guest controller) configured on it identifies the guest WLAN.
- Guest traffic segregation implements Layer 2 or Layer 3 techniques across the campus network to restrict the locations where guests are allowed.
- Guest user-level QoS is used for rate limiting and shaping, although it is widely implemented to restrict the bandwidth usage for a guest user.
- Access control involves using embedded access control functionality within the campus network, or implementing an external platform to control guest access to the Internet from the enterprise network.
- Authentication and authorization of guests that are based on variables, including date, duration, and bandwidth.
- An audit mechanism to track who is currently using, or has used, the network.
- A wider coverage is provided by including areas such as lobbies and other common areas that are otherwise not wired for network connectivity.
- The need for designated guest access areas or rooms is removed.

Note To use IRCM with AireOS in your network, contact Cisco TAC for assistance.

Table 55: Supported Controllers

Controller Name	Supported as Guest Anchor	Supported as Guest Foreign
Cisco Catalyst 9800-40 Wireless Controller	Yes	Yes
Cisco Catalyst 9800-80 Wireless Controller	Yes	Yes
Cisco Catalyst 9800-CL Wireless Controller	Yes	Yes
Cisco Catalyst 9800-L Wireless Controller	Yes	Yes
Cisco Catalyst 9800 Embedded Wireless Controller for Switch	No	No
Cisco Catalyst 9800 Embedded Wireless Controller on Cisco Catalyst 9100 Series APs	No	No

Following is a list of features supported by Cisco Guest Access:

Supported Features

- Sleeping Clients
- FQDN
- AVC (AP upstream and downstream)
- Native Profiling
- Open Authentication
- OpenDNS
- Supported Security Methods:
  - MAB Central Web Authentication (CWA)
  - Local Web Authentication (LWA)
  - LWA on MAB Failure
  - 802.1x + CWA
  - 802.1x
- SSID QoS Upstream and Downstream (Foreign)
- AP/ Client SSO
- Static IP Roaming
- Client IPv6
- Roaming across controllers
- RADIUS Accounting

Note In a guest access scenario, accounting is always performed at the foreign controller for all authentication methods.

- QoS: Client-Level Rate Limiting
- Guest Anchor Load Balancing
- Workgroup Bridges (WGB)

Note To enable the controller to support multiple VLANs from a WGB, use **wgb vlan** command.

Foreign Map Overview

Guest Access supports Foreign Map using Policy Profile and WLAN Profile configuration models in Cisco Catalyst 9800 Series Wireless Controller.

Foreign Map support in Cisco Catalyst 9800 Series Wireless Controller is achieved with the following policy profile and WLAN profile config model.

- Guest Foreign commands:
  - **Foreign1: wlanProf1 PolicyProf1**
  - **Foreign2: wlanProf2 PolicyProf2**
- Guest Anchor commands:
  - **wlanProf1, wlanProf2**
  - **PolicyProf1: Vlan100 - subnet1**
  - **PolicyProf2: Vlan200 - subnet2**

Foreign Map Roaming

Configure two different WLAN profiles on the two Guest Foreigns and seamless roaming is not allowed between them. This is expected configuration. However, seamless roaming is allowed if the same WLAN profile is configured on two Guest Foreigns, but it prevents Foreign Map feature from working.

Wireless Guest Access: Use Cases

The wireless guest access feature can be used to meet different requirements. Some of the possibilities are shared here.

Scenario One: Providing Secured Network Access During Company Merger

This feature can be configured to provide employees of **company A** who are visiting **company B** to access company A resources on company B network securedly.

Scenario Two: Shared Services over Existing Setup

Using this feature, you can provide multiple services using multiple vendors piggy backing on the existing network. A company can provide services on an SSID which is anchored on the existing controller. This is while the existing service continues to serve over the same controller and network.

Load Balancing Among Multiple Guest Controllers

- You can configure export anchors to load balance large guest client volumes. For a single export foreign guest WLAN configuration, up to 72 controllers are allowed. To configure mobility guest controllers, use **mobility anchor** *ip address*.
- You can specify primary anchors with priority (1,3) and choose another anchor as backup in case of failure.
- In a multi-anchor scenario, when the primary anchor goes down, the clients get disconnected from the primary anchor and joins the secondary anchor.

Guidelines and Limitations for Wireless Guest Access

- Match the security profiles under WLAN on both Guest Foreign, and Guest Anchor.
- Match the policy profile attributes such as NAC and AAA Override on both Guest Foreign, and Guest Anchor controllers.
- On Export Anchor, the WLAN profile name and Policy profile name is chosen when a client joins at runtime and the same should match with the Guest Foreign controller.

Troubleshooting IPv6

When a guest export client cannot get a routable IPv6 address through SLAAC or cannot pass traffic when the IPv6 address is learned through DHCPv6, you can use the following workarounds:

- On IPv6 Routers: You can work around the RA multicast to unicast conversion by modifying behaviour on the IPv6 gateway. Depending on the product, this may be the default behaviour or may require configuration.
  - On Cisco IPv6 Routers
    - Cisco Nexus platform: Has solicited unicast RA enabled by default to help with wireless deployment.
    - Cisco IOS-XE platform: Use the following configuration command to turn on unicast RA to help with wireless deployment:

      ipv6 nd ra solicited unicast

  - On non-Cisco IPv6 Routers: If non-Cisco network devices do not support configuration command to enable solicited unicast RA then a work around does not exist.

Configure Mobility Tunnel for Guest Access (GUI)

Procedure

Step 1 Choose **Configure** > **Tags and Profiles** > **WLANs**.

Step 2 In the **Wireless Networks** area, click the relevant WLAN or RLAN and click **Mobility Anchor**.

Step 3 In the **Wireless Network Details** section, choose a device from the **Switch IP Address** drop-down list.

Step 4 Click **Apply**.

Configure Mobility Tunnel for Guest Access (CLI)

Follow the procedure given below to configure a mobility tunnel.

Procedure

	Command or Action	Purpose
Step 1	**wireless mobility group name** *group name* **Example:** `Device(config)# wireless mobility group name mtunnelgrp`	Configures a mobility group.
Step 2	**wireless mobility mac-address** *mac address* **Example:** `Device(config)# wireless mobility mac-address 0d:4c:da:3a:f2:21`	Configures a mobility MAC address.
Step 3	**wireless mobility group member mac** *mac address* **ip** *ip address* **group** *group name* **Example:** `Device(config)# wireless mobility group member mac-address df:07:a1:a7:a8:55 ip 206.223.123.2 group mtgrp`	Configures a mobility peer.

Configuring Guest Access Policy (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** and enable the **Central Switching** toggle button.

Step 4 In the **Access Policies** tab, under the **VLAN** settings, choose the vlans from the **VLAN/VLAN Group** drop-down list.

Step 5 In the **Mobility** tab, under the **Mobility Anchors** settings, check the **Export Anchor** check box.

Step 6 In the **Advanced** tab, under the **WLAN Timeout** settings, enter the **Idle Timeout (sec)**.

Step 7 Click **Apply to Device**.

Configuring Guest Access Policy (CLI)

Follow the procedure given below to create and configure the guest access profile policy. Alternately, you may use the existing default policy profile after configuring the mobility anchor to that policy.

You can only configure anchors which are peers. Ensure that the IP address that is used is a mobility peer and is included in the mobility group. The system shows an invalid anchor IP address error message when any other IP address is used.

To delete the mobility group, ensure that the mobility peer which is also a mobility anchor is removed from the policy profile.

Note

- No payload is sent to Guest Foreign to display the VLAN.
- To avoid a client exclusion from occurring due to VLAN, Cisco Catalyst 9800 Series Controllers need to define VLAN along with the associated name being pushed from ISE.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan_policy_profile* **Example:** `Device(config)# wireless profile policy guest-test-policy`	Configures the policy profile and enters wireless profile configuration mode. **Note** • You can use the **default-policy-profile** to configure the profile policy.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Shuts down the policy if it exists before configuring the anchor.
Step 4	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	(Optional) Enables central switching.

Step 5	Choose the first option to configure the Guest Foreign or second option to configure the Guest Anchor:
	• **mobility anchor** *anchor-ip-address*
	• **mobility anchor**
	Example:
	For Guest Foreign:
	`Device(config-wireless-policy)# mobility anchor 19.0.2.1`
	For Guest Anchor:
	`Device(config-wireless-policy)# mobility anchor`
		Configures Guest Foreign or Guest Anchor.

	Command or Action	Purpose
Step 6	**idle-timeout** *timeout* **Example:** `Device (config-wireless-policy)# idle-timeout 1000`	(Optional) Configures duration of idle timeout, in seconds.
Step 7	**vlan** *vlan-id* **Example:** `Device(config-wireless-policy)# vlan 2`	Configures VLAN name or VLAN Id. **Note** VLAN is optional for a Guest Foreign controller.
Step 8	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables policy profile.
Step 9	**end** **Example:** `Device(config-wireless-policy)# end`	Exits the configuration mode and returns to privileged EXEC mode.
Step 10	**show wireless profile policy summary** **Example:** `Device# show wireless profile policy summary`	(Optional) Displays the configured profiles.
Step 11	**show wireless profile policy detailed** *policy-profile-name* **Example:** `Device# show wireless profile policy detailed guest-test-policy`	(Optional) Displays detailed information of a policy profile.

Viewing Guest Access Debug Information (CLI)

- To display client level detailed information about mobility state and the anchor IP address, use the following command:.

  show wireless client mac-add *mac-address* **detail**

- To display the client mobility statistics, use the following command:

  show wireless client mac-address *mac-address* **mobility statistics**

- To display client level roam history for an active client in sub-domain, use the following command:

  show wireless client mac-address *mac-address* **mobility history**

- To display detailed parameters of a given profile policy, use the following command:

  show wireless profile policy detailed *policy-name*

- To display the global level summary for all mobility messages, use the following command:

show wireless mobility summary

- To display the statistics for the Mobility manager, use the following command:

  show wireless stats mobility

Configure Guest Access Using Different Security Methods

The following sections provide information about the following:

Open Authentication

To configure the guest access with open authentication, follow the steps:

1. Configuring the WLAN Profile
2. Configuring Guest Access Policy (CLI), on page 1162

Note No tag is required unless AVC is enabled.

Configure a WLAN Profile for Guest Access with Open Authentication (GUI)

Procedure

Step 1	Choose **Configuration** > **Tags & Profiles** > **WLANs**.
Step 2	Click **Add**.
Step 3	In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**. Choose the radio policy from the **Radio Policy** drop-down list. Enable or disable the **Status** and **Broadcast SSID** toggle buttons.
Step 4	Choose **Security** > **Layer2** tab. Uncheck the **WPA Policy**, **WPA2 Policy**, **AES** and **802.1x** check boxes.
Step 5	Click **Apply to Device**.

Configure a WLAN Profile For Guest Access with Open Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id ssid-name*. **Example:**	Configures the WLAN and SSID.

	Command or Action	Purpose
	`Device(config)# wlan mywlan 34 mywlan-ssid`	
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 6	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 7	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Saves the configuration.

Configuring a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan-policy-profile* **Example:** `Device(config)# wireless profile policy open_it`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	Choose the first option to configure a Guest Foreign or second option to configure a Guest Anchor: • **mobility anchor** *anchor-ip-address* • **mobility anchor** **Example:**	Configures Guest Foreign or Guest Anchor.

	Command or Action	Purpose

	For Guest Foreign:
	`Device (config-wireless-policy)# mobility anchor 19.0.2.1`
	For Guest Anchor:
	`Device (config-wireless-policy)# mobility anchor`	

Step 4	**central switching**. **Example:** `Device(config-wireless-policy)# central switching`	Enables Central switching
Step 5	**vlan** *id* **Example:** `Device(config-wireless-policy)# vlan 16`	Configures a VLAN name or VLAN ID. **Note** VLAN is optional for a Guest Foreign controller.
Step 6	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the policy profile.

Local Web Authentication

To configure LWA, follow these steps:

1. Configure a Parameter Map (CLI)
2. Configure a WLAN Profile for Guest Access with Local Web Authentication (CLI)
3. Applying Policy Profile on a WLAN
4. Configure an AAA Server for Local Web Authentication (CLI)

Configure a Parameter Map (GUI)

Procedure

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

Step 2 Click **Add**.

Step 3 Enter the **Parameter-map name**, **Maximum HTTP connections**,**Init-State Timeout(secs)** and choose **webauth** in the **Type** drop-down list.

Step 4 Click **Apply to Device**.

Configure a Parameter Map (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth global** **Example:** `Device(config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 3	**type webauth** **Example:** `Device(config-params-parameter-map)#type webauth`	Configures the webauth type parameter.
Step 4	**timeout init-state sec** *timeout-seconds* **Example:** `Device(config-params-parameter-map)# timeout inti-state sec 3600`	Configures the WEBAUTH timeout in seconds. Valid range for the time in sec parameter is 60 to 3932100 seconds.
Step 5	**virtual-ip ipv4** *virtual_IP_address* **Example:** `Device(config-params-parameter-map)#virtual-ip ipv4 209.165.201.1`	Configures a VLAN name or VLAN ID.

Configure a WLAN Profile for Guest Access with Local Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.
Step 2 Click on the **WLAN** name.
Step 3 Choose **Security** > **Layer3**.
Step 4 Check the **Web Policy** check box.
Step 5 Choose a parameter map from the **Web Auth Parameter Map** drop-down list.
Step 6 Choose an authentication list from the **Authentication List** drop-down list.
Step 7 Click **Update & Apply to Device**.

Configure a WLAN Profile for Guest Access with Local Web Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-id ssid-name* **Example:** `Device# Device(config)# wlan mywlan 38 mywlan-ssid1`	Configures the WLAN and SSID.
Step 3	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables web authentication for a WLAN.
Step 4	**security web-auth parameter-map** *default* **Example:** `Device(config-wlan)# security web-auth parameter-map default`	Configure the default parameter map. **Note** When **security web-auth** is enabled, you get to map the **default authentication-list** and global **parameter-map**. This is applicable for authentication-list and parameter-map that are not explicitly mentioned.
Step 5	**security web-auth parameter-map** *global* **Example:** `Device(config-wlan)# security web-auth parameter-map global`	Configure the global parameter map.
Step 6	**security web-auth authentication-list** *LWA-AUTHENTICATION* **Example:** `Device(config-wlan)# security web-auth authentication-list LWA-AUTHENTICATION`	Sets the authentication list for IEEE 802.1x.

Configure an AAA Server for Local Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **AAA Advanced** > **Global Config**.

Step 2 Choose the options from the **Local Authentication**, **Authentication Method List**, **Local Authorization** and **Authorization Method List** drop-down lists.

Step 3 Enable or Disable the **Radius Server Load Balance** using toggle button.

Step 4 Check the **Interim Update** check box.

Step 5 Click **Apply**.

Configure an AAA Server for Local Web Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa authentication login** *LWA-AUTHENTICATION* **local** **Example:** `Device(config)#aaa authentication login lwa-authentication local`	Defines the authentication method at login.
Step 3	**aaa authorization network default local if-authenticated** **Example:** `Device(config)#aaa authorization network default local if-authenticated`	Sets the authorization method to local if the user has authenticated.

Global Configuration

Follow the procedure given below for global configuration:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**username** *name* **password 0** *clear-text-passowrd* **Example:** `Device(config)# #username base password 0 pass1`	Sets the clear text password for the user.
Step 3	**ip http server** **Example:** `Device(config)#ip http server`	Enables the HTTP server.

	Command or Action	Purpose
Step 4	**ip http authentication local** **Example:** `Device(config)#ip http authentication local`	Sets the HTTP server authentication method to local. **Note** You will get the admin access rights regardless of the user privilege, if the **ip http authentication local** is disabled and username is the same as enable password.

Central Web Authentication

To configure CWA, follow these steps:

1. Configure a WLAN Profile for Guest Access with Central Web Authentication (CLI)
2. Applying Policy Profile to a WLAN, on page 731
3. AAA Server Configuration (CLI)
4. Creating Redirect ACL, on page 588

Configure a WLAN Profile for Guest Access with Central Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.

Step 4 To enable the WLAN, set **Status** as **Enabled**.

Step 5 From the **Radio Policy** drop-down list, select the radio policy.

Step 6 To enable the **Broadcast SSID**, set the status as **Enabled**.

Step 7 Choose **Security** > **Layer2** tab. Uncheck the **WPA Policy**, **WPA2 Policy**, **AES** and **802.1x** check boxes.

Step 8 Check the **MAC Filtering** check box to enable the feature. With MAC Filtering enabled, choose the Authorization list from the **Authorization List** drop-down list.

Step 9 Click **Apply to Device**.

Configure a WLAN Profile for Guest Access with Central Web Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-id ssid-name* **Example:** `Device# Device(config)# wlan mywlan 38 mywlan-ssid1`	Configures the WLAN and SSID.
Step 3	**mac-filtering** *remote_authorization_list_name* **Example:** `Device(config-wlan)# mac-filtering auth-list`	Enables MAB authentication for the remote RADIUS server.
Step 4	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 7	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Saves the configuration.

AAA Server Configuration (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **Servers/Groups** > **RADIUS** > **Server Groups**.

Step 2 Click the RADIUS server group.

Step 3 From the **MAC-Delimiter** drop-down list, choose an option.

Step 4 From the **MAC-Filtering** drop-down list, choose an option.

Step 5 Enter the **Dead-Time (mins)**.

Step 6 From the **Available Servers** on the left, move the servers you need to **Assigned Servers** on the right.

Step 7 Click **Update & Apply to Device**.

Step 8 Choose **Configuration** > **Security** > **AAA** > **Servers/Groups** > **RADIUS** > **Servers**.

Step 9 Click the RADIUS server.

Step 10 Enter the **IPv4/IPv6 Server Address**, **Auth Port**, **Acct Port**, **Server Timeout (seconds)** and **Retry Count**.

Step 11 Check or uncheck the **PAC Key** checkbox and choose the Key Type from the **Key Type** drop-down list. Enter the **Key** and **Confirm Key**.

Step 12 Enable or disable the **Support for CoA** toggle button.

Step 13 Click **Update & Apply to Device**.

AAA Server Configuration (CLI)

Note Configure AAA server for Guest Foreign only.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa authorization network** *authorization-list***local group** *Server-group-name* **Example:** `Device(config)#aaa authorization network cwa local group ise`	Sets the authorization method to local.
Step 3	**aaa group server radius** *server-group-name* **Example:** `Device(config)#aaa group server radius ise`	Configures RADIUS server group definition.

	Command or Action	Purpose
Step 4	**server name** *radius-server-name* **Example:** `Device(config-sg-radius)#server name ise1`	Configures the RADIUS server name.
Step 5	**subscriber mac-filtering security-mode mac** **Example:** `Device(config-sg-radius)#$mac-filtering security-mode mac`	Sets the MAC address as the password.
Step 6	**mac-delimiter colon** **Example:** `Device(config-sg-radius)#mac-delimiter colon`	Sets the MAC address delimiter to colon.
Step 7	**end** **Example:** `Device(config-sg-radius)#end`	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.
Step 8	**radius server** *name* **Example:** `Device(config)#radius server ISE1`	Sets the RADIUS server name
Step 9	**address ipv4** *radius-server-ipaddress* **auth-port** *port-number* **acct-port** *port-number* **Example:** `Device(config-radius-server)#address ipv4 209.165.201.1 auth-port 1635 acct-port 33`	Configures the RADIUS server IP address authentication and accounting ports.

Configure Web Authentication on MAC Address Bypass failure (GUI)

Procedure

Step 1 Click **Configuration** > **Tags and Profiles** > **WLANs**.

Step 2 Click **Add** to add a new WLAN Profile or click the one you want to edit.

Step 3 In the **Edit WLAN** window, complete the following steps:

a) Choose **Security** > **Layer2** and check the **MAC Filtering** check box ot enable MAC filtering.
b) From the **Authorization List** drop-down list, select a value.
c) Choose the **Layer3** tab.
d) Click **Show Advanced Settings** and check the **On MAC Filter Failure** checkbox.

Configure Web Authentication on MAC Address Bypass Failure (CLI)

You can configure authentication to fall back to web authentication, if a client cannot authenticate using MAC filter (Local or RADIUS), while trying to connect to a WLAN. To enable this feature, configure both MAC filtering and Web Authentication on the device. This can also avoid disassociations that happen only because of MAC filter authentication failure. To configure this feature, follow the procedure:

Configure a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-name* **Example:** `Device(config)# wireless profile policy cwa`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Enables Central switching.

Step 4	Choose the first option to configure a Guest Foreign or second option to configure a Guest Anchor:
	• **mobility anchor** *anchor-ip-address*
	• **mobility anchor**
	Example:
	For Guests Foreign:
	`Device (config-wireless-policy)# mobility anchor 19.0.2.1`
	For Guest Anchor:
	`Device (config-wireless-policy)# mobility anchor`
		Configures Guest Foreign or Guest Anchor.

Step 5	**vlan** *name* **Example:** `Device(config-wireless-policy)# vlan 16`	Configures a VLAN name or VLAN ID. **Note** VLAN is optional for a Guest Foreign controller.
Step 6	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the policy profile.

Configure a WLAN Profile

Procedure

	Command or Action	Purpose
Step 1	**wlan** *guest-wlan-name wlan-id ssid* **Example:** `config# wlan test-wlan-guest 10 wlan-ssid`	Configures guest WLAN.
Step 2	**mac-filtering** *mac-auth-listname* **authorization-override** *override-auth-listname* **Example:** `config-wlan# mac-filtering mac-auth-listname authorization-override`	Configures MAC filtering support on WLAN.
Step 3	**security web-auth** **Example:** `config-wlan# security web-auth`	Enables web authentication.
Step 4	**security web-auth on-macfilter-failure** **Example:** `config-wlan# security web-auth on-macfilter-failure`	Enables web authentication if MAC filter authentication fails.

CHAPTER 117

802.11r BSS Fast Transition

- Information About 802.11r Fast Transition, on page 1177
- Restrictions for 802.11r Fast Transition, on page 1178
- Monitoring 802.11r Fast Transition (CLI), on page 1179
- Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI), on page 1180
- Configuring 802.11r Fast Transition in an Open WLAN (CLI), on page 1181
- Configuring 802.11r Fast Transition on a PSK Security–Enabled WLAN (CLI), on page 1183
- Disabling 802.11r Fast Transition (GUI), on page 1184
- Disabling 802.11r Fast Transition (CLI), on page 1184

Information About 802.11r Fast Transition

802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with a new AP is done even before the corresponding client roams to the target access point. This concept is called Fast Transition. The initial handshake allows a client and the access points to do the Pairwise Transient Key (PTK) calculation in advance. These PTK keys are applied to the client and the access points after the client responds to the reassociation request or responds to the exchange with new target AP.

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).

Client Roaming

For a client to move from its current AP to a target AP using the FT protocols, message exchanges are performed using one of the following methods:

- Over-the-Air—The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.
- Over-the-Distribution System (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 device.

Figure 29: Message Exchanges when Over–the–Air Client Roaming is Configured

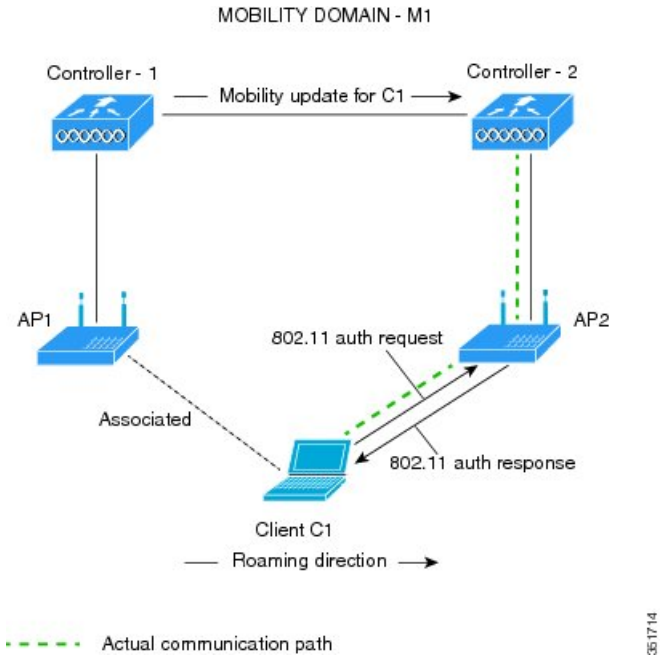
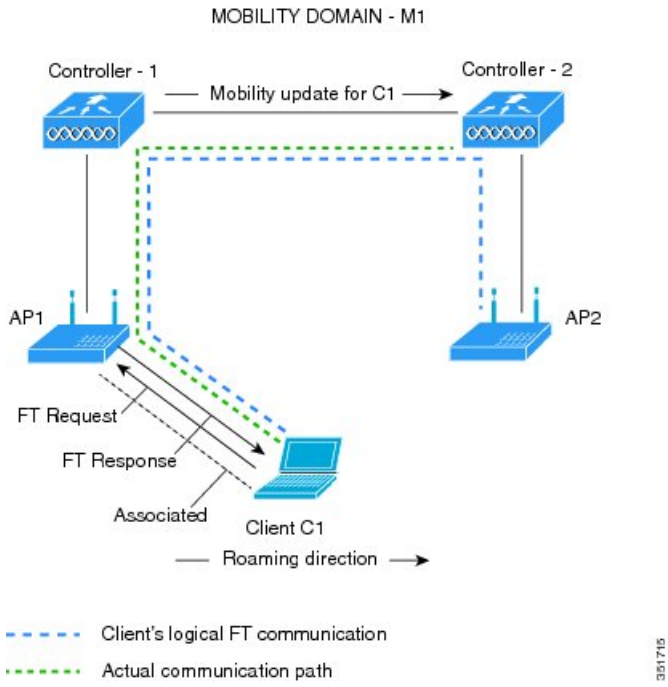


Figure 30: Message Exchanges when Over–the–DS Client Roaming is Configured



Restrictions for 802.11r Fast Transition

- EAP LEAP method is not supported.

- Traffic Specification (TSPEC) is not supported for 802.11r fast roaming. Therefore, RIC IE handling is not supported.
- If WAN link latency exists, fast roaming is also delayed. Voice or data maximum latency should be verified. The Cisco WLC handles 802.11r Fast Transition authentication requests during roaming for both Over-the-Air and Over-the-DS methods.
- Legacy clients cannot associate with a WLAN that has 802.11r enabled if the driver of the supplicant that is responsible for parsing the Robust Security Network Information Exchange (RSN IE) is old and not aware of the additional AKM suites in the IE. Due to this limitation, clients cannot send association requests to WLANs. These clients, however, can still associate with non-802.11r WLANs. Clients that are 802.11r-capable can associate as 802.11i clients on WLANs that have both 802.11i and 802.11r Authentication Key Management Suites enabled.

  The workaround is to enable or upgrade the driver of the legacy clients to work with the new 802.11r AKMs, after which the legacy clients can successfully associate with 802.11r-enabled WLANs.

  Another workaround is to have two SSIDs with the same name, but with different security settings (FT and non-FT).
- Fast Transition resource–request protocol is not supported because clients do not support this protocol. Also, the resource–request protocol is an optional protocol.
- To avoid any Denial of Service (DoS) attack, each Cisco WLC allows a maximum of three Fast Transition handshakes with different APs.
- Non-802.11r–capable devices will not be able to associate with FT-enabled WLAN.
- We do not recommend 802.11r FT + PMF.
- We recommend 802.11r FT Over-the-Air roaming for FlexConnect deployments.
- 802.11r ft-over-ds is enabled by default, when a WLAN is created in the controller . In Cisco Wave 2 APs, local switching local authentication with 802.11r is not supported. To make the local switching local authentication work with Cisco Wave 2 APs, explicitly disable 802.11r in WLAN. A sample configuration is given below:

```
wlan local-dot1x 24 local-dot1x
no security ft over-the-ds
no security ft adaptive
security dot1x authentication-list spwifi_dot1x
no shutdown
```

Monitoring 802.11r Fast Transition (CLI)

The following command can be used to monitor 802.11r Fast Transition:

Command	Description
show wlan name *wlan-name*	Displays a summary of the configured parameters on the WLAN.

Command	Description
show wireless client mac-address *mac-address*	Displays the summary of the 802.11r authentication key management configuration on a client. . . . . . . Client Capabilities CF Pollable : Not implemented CF Poll Request : Not implemented Short Preamble : Not implemented PBCC : Not implemented Channel Agility : Not implemented Listen Interval : 15 Fast BSS Transition : Implemented Fast BSS Transition Details : Client Statistics: Number of Bytes Received : 9019 Number of Bytes Sent : 3765 Number of Packets Received : 130 Number of Packets Sent : 36 Number of EAP Id Request Msg Timeouts : 0 Number of EAP Request Msg Timeouts : 0 Number of EAP Key Msg Timeouts : 0 Number of Data Retries : 1 Number of RTS Retries : 0 Number of Duplicate Received Packets : 1 Number of Decrypt Failed Packets : 0 Number of Mic Failured Packets : 0 Number of Mic Missing Packets : 0 Number of Policy Errors : 0 Radio Signal Strength Indicator : -48 dBm Signal to Noise Ratio : 40 dB . . . . . .

Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

	Command or Action	Purpose
Step 3	**client vlan** *vlan-name* **Example:** `Device(config-wlan)# client vlan 0120`	Associates the client VLAN to this WLAN.
Step 4	**local-auth** *local-auth-profile-eap* **Example:** `Device(config-wlan)# local-auth`	Enables the local auth EAP profile.
Step 5	**security dot1x authentication-list default** **Example:** `Device(config-wlan)# security dot1x authentication-list default`	Enables security authentication list for dot1x security. The configuration is similar for all dot1x security WLANs.
Step 6	**security ft** **Example:** `Device(config-wlan)# security ft`	Enables 802.11r Fast Transition on the WLAN.
Step 7	**security wpa akm ft dot1x** **Example:** `Device(config-wlan)# security wpa akm ft dot1x`	Enables 802.1x security on the WLAN.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 9	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode

Configuring 802.11r Fast Transition in an Open WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

	Command or Action	Purpose
Step 3	**client vlan** *vlan-id* **Example:** `Device(config-wlan)# client vlan 0120`	Associates the client VLAN to the WLAN.
Step 4	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA secuirty.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 7	**no wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 8	**security ft** **Example:** `Device(config-wlan)# security ft`	Specifies the 802.11r Fast Transition parameters.
Step 9	**no shutdown** **Example:** `Device(config-wlan)# shutdown`	Shuts down the WLAN.
Step 10	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode

Configuring 802.11r Fast Transition on a PSK Security–Enabled WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**client vlan** *vlan-name* **Example:** `Device(config-wlan)# client vlan 0120`	Associates the client VLAN to this WLAN.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**security wpa akm ft psk** **Example:** `Device(config-wlan)# security wpa akm ft psk`	Configures Fast Transition PSK support.
Step 6	**security wpa akm psk set-key** {**ascii** {**0** | **8**} | **hex** {**0** | **8**}} **Example:** `Device(config-wlan)# security wpa akm psk set-key ascii 0 test`	Configures PSK AKM shared key.
Step 7	**security ft** **Example:** `Device(config-wlan)# security ft`	Configures 802.11r Fast Transition.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

	Command or Action	Purpose
Step 9	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode

Disabling 802.11r Fast Transition (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **WLANs** page, click the WLAN name.

Step 3 In the **Edit WLAN** window, click the **Security** > **Layer2** tab.

Step 4 From the **Fast Transition** drop-down list, choose **Disabled**. Note that you cannot enable or disable Fast Transition, if you have configured an SSID with Open Authentication.

Step 5 Click **Update & Apply to Device**.

Disabling 802.11r Fast Transition (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**no security ft** [**over-the-ds** | **reassociation-timeout** *timeout-in-seconds*] **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables 802.11r Fast Transition on the WLAN.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

CHAPTER 118

Assisted Roaming

- 802.11k Neighbor List and Assisted Roaming, on page 1185
- Restrictions for Assisted Roaming, on page 1186
- How to Configure Assisted Roaming, on page 1186
- Verifying Assisted Roaming, on page 1188
- Configuration Examples for Assisted Roaming, on page 1188

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 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 device CLI.

How to Configure Assisted Roaming

Configuring Assisted Roaming (GUI)

Assisted roaming allows clients to request neighbor reports containing information about known neighbor access points that are candidates for a service set transition.

Before you begin

Ensure that you have configured an AP Join Profile prior to configuring the primary and backup controllers.

Procedure

Step 1 Choose **Configuration** > **Tags&Profiles** > **WLAN** and click **Add** to add a WLAN or select an existing WLAN.

Step 2 On the **Advanced** tab, go to the **Assisted Roaming (11K)** and select the **Prediction Optimization** checkbox 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 3 Select the **Neighbor List** checkbox to optimize roaming for 802.11K clients by generating a neighbor list for each client without sending an 802.11k neighbor list request. By default, the neighbor list contains only neighbors in the same band with which the client is associated. However, if you select the Dual Band Neighbor List checkbox, it allows 802.11k to return neigbors in both bands.

Step 4 Click **Apply to Device.** .

Configuring Assisted Roaming (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless assisted-roaming floor-bias** *dBm* **Example:** `Device(config)# wireless assisted-roaming floor-bias 20`	Configures neighbor floor label bias. The valid range is from 5 to 25 dBm, and the default value is 15 dBm.
Step 3	**wlan** *wlan-id* **Example:** `Device(config)# wlan wlan1`	Enters the WLAN configuration submode. The *wlan-name* is the profile name of the configured WLAN.
Step 4	**assisted-roaming neighbor-list** **Example:** `Device(wlan)# assisted-roaming neighbor-list`	Configures an 802.11k neighbor list for a WLAN. By default, assisted roaming is enabled on the neighbor list when you create a WLAN. The **no** form of the command disables assisted roaming neighbor list.
Step 5	**assisted-roaming dual-list** **Example:** `Device(wlan)# assisted-roaming dual-list`	Configures a dual-band 802.11k dual list for a WLAN. By default, assisted roaming is enabled on the dual list when you create a WLAN. The **no** form of the command disables assisted roaming dual list.
Step 6	**assisted-roaming prediction** **Example:** `Device(wlan)# assisted-roaming prediction`	Configures assisted roaming prediction list feature for a WLAN. By default, the assisted roaming prediction list is disabled. **Note** A warning message is displayed and load balancing is disabled for the WLAN if load balancing is already enabled for the WLAN.
Step 7	**wireless assisted-roaming prediction-minimum** *count* **Example:** `Device# wireless assisted-roaming prediction-minimum`	Configures the minimum number of predicted APs required for the prediction list feature to be activated. The default value is 3. **Note** If the number of the AP in the prediction assigned to the client is less than the number that you specify, the assisted roaming feature will not apply on this roam.

	Command or Action	Purpose
Step 8	**wireless assisted-roaming denial-maximum** *count* **Example:** `Device# wireless assisted-roaming denial-maximum 8`	Configures the maximum number of times a client can be denied association if the association request is sent to an AP does not match any AP on the prediction. The valid range is from 1 to 10, and the default value is 5.
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Assisted Roaming

The following command can be used to verify assisted roaming configured on a WLAN:

Command	Description
show wlan id *wlan-id*	Displays the WLAN parameters on the WLAN.

Configuration Examples for Assisted Roaming

This example shows how to configure the neighbor floor label bias:

```
Device# configure terminal
Device(config)# wireless assisted-roaming floor-bias 10
Device(config)# end
Device# show wlan id 23
```

This example shows how to disable neighbor list on a specific WLAN:

```
Device# configure terminal
Device(config)# wlan test1
Device(config (wlan)# no assisted-roaming neighbor-list
Device(config)(wlan)# end
Device# show wlan id 23
```

This example shows how to configure the prediction list on a specific WLAN:

```
Device# configure terminal
Device(config)# wlan test1
Device(config)(wlan)# assisted-roaming prediction
Device(config)(wlan)# end
Device# show wlan id 23
```

This example shows how to configure the prediction list based on assisted roaming prediction threshold and maximum denial count on a specific WLAN:

```
Device# configure terminal
Device(config)# wireless assisted-roaming prediction-minimum 4
```

```
Device(config)# wireless assisted-roaming denial-maximum 4
Device(config)(wlan)# end
Device# show wlan id 23
```

CHAPTER 119

802.11v

- Information About 802.11v, on page 1191
- Prerequisites for Configuring 802.11v, on page 1192
- Restrictions for 802.11v, on page 1192
- Enabling 802.11v BSS Transition Management, on page 1192
- Configuring 802.11v BSS Transition Management (GUI), on page 1193
- Configuring 802.11v BSS Transition Management (CLI), on page 1193

Information About 802.11v

The 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 the 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 delivers 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 is 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 that 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.

Prerequisites for Configuring 802.11v

- Applies for Apple clients like Apple iPad, iPhone, and so on, that run on Apple iOS version 7 or later.
- Supports local mode; also supports FlexConnect access points in central authentication modes only.

Restrictions for 802.11v

Client needs to support 802.11v BSS Transition.

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 if the client is not reassociated to another AP.

Configuring 802.11v BSS Transition Management (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add** to create WLANs.

The **Add WLAN** page is displayed.

Step 3 In the **Advanced** tab and **11v BSS Transition Support** section, select the **BSS Transition** check box to enable BSS transition per WLAN.

Step 4 Enable the **Dual Neighbor List** check box to include the neighbours of other radio slots of the same AP in the BSS transition response.

Note This is applicable only for 2.4 GHz and 5 GHz radio slots.

Step 5 Enable the **BSS Max Idle Service** check box to help clients and APs efficiently decide how long to remain associated when no traffic is being transmitted. The device uses this information to preserve device battery life.

Step 6 Enable the **BSS Max Idle Protected** check box to enable the AP to accept only authenticated frames (encrypted with Robust Security Network (RSN) information) from the client to reset the BSS Max Idle period counter. Without protected mode, any data or management frame (encrypted or unencrypted) sent by the client will reset the idle timer for the client.

Step 7 Enable the **Directed Multicast Service** check box to request the AP to send a multicast stream as unicast, to any DMS capable client on this WLAN.

Step 8 Click **Save & Apply to Device**.

Configuring 802.11v BSS Transition Management (CLI)

802.11v BSS Transtion is applied in the following three scenarios:

Procedure

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

	Command or Action	Purpose
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan test-wlan`	Configures WLAN profile and enters the WLAN profile configuration mode.
Step 3	**shut** **Example:** `Device(config-wlan)# shut`	Shutdown the WLAN profile.
Step 4	**bss-transition** **Example:** `Device(config-wlan)# bss-transition`	Configure BSS transition per WLAN.
Step 5	**bss-transition disassociation-imminent** **Example:** `Device(config-wlan)# bss-transition disassociation-imminent`	Configure BSS transition disassociation Imminent per WLAN.
Step 6	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN profile.
Step 7	**end** **Example:** `Device(config-wlan)# end`	Return to privilege EXEC mode. Alternatively, you can press **CTRL + Z** to exit global configuration mode.

CHAPTER 120

802.11w

- Information About 802.11w, on page 1195
- Prerequisites for 802.11w, on page 1198
- Restrictions for 802.11w, on page 1198
- How to Configure 802.11w, on page 1199
- Disabling 802.11w, on page 1200
- Monitoring 802.11w, on page 1201

Information About 802.11w

Wi-Fi is a broadcast medium that enables any device to eavesdrop and participate either as a legitimate or rogue device. Management frames such as authentication, de-authentication, association, dissociation, beacons, and probes are used by wireless clients to initiate and tear down sessions for network services. Unlike data traffic, which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients and therefore must be transmitted as open or unencrypted. While these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks. For example, an attacker could spoof management frames from an AP to attack a client associated with the AP.

The 802.11w protocol applies only to a set of robust management frames that are protected by the Protected Management Frames (PMF) service. These include Disassociation, De-authentication, 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:

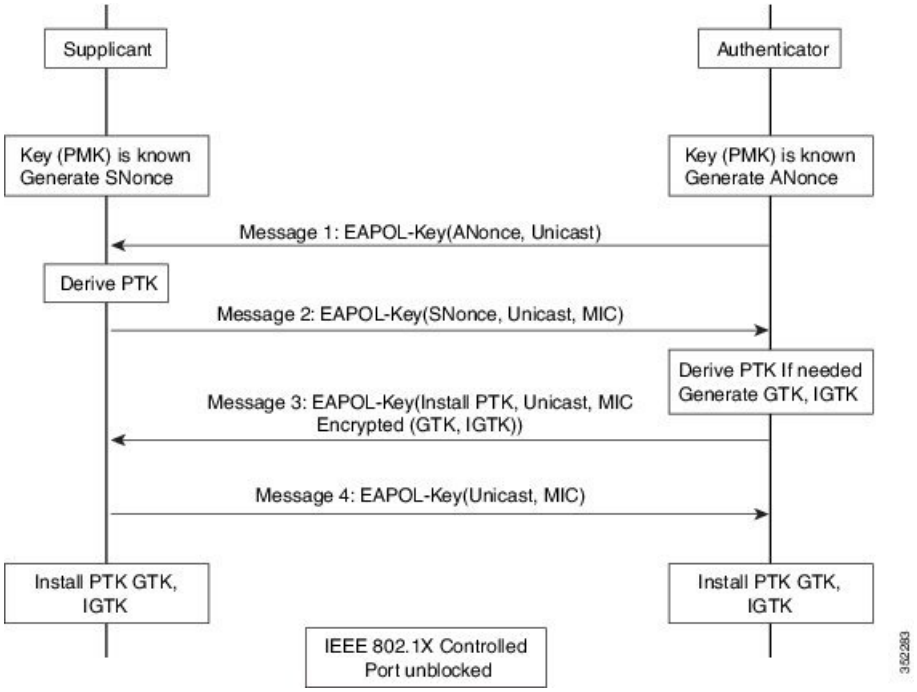
- Client protection is added by the AP adding cryptographic protection to de-authentication and dissociation frames preventing them from being spoofed in a DOS attack.
- Infrastructure protection is added by adding a Security Association (SA) tear down protection mechanism consisting of an Association Comeback Time and an SA-Query procedure preventing spoofed association request from disconnecting an already connected client.

802.11w has introduced a new IGTK Key, which is used to protect broadcast/multicast robust management frames:

- IGTK is a random value assigned by the authenticator STA (WLC) and used to protect MAC management protocol data units (MMPDUs) from that source STA.

When Management Frame Protection is negotiated, the AP encrypts the GTK and IGTK values in the EAPOL-Key frame, which is delivered in Message 3 of 4-way handshake.

Figure 31: IGTK Exchange in 4-way Handshake

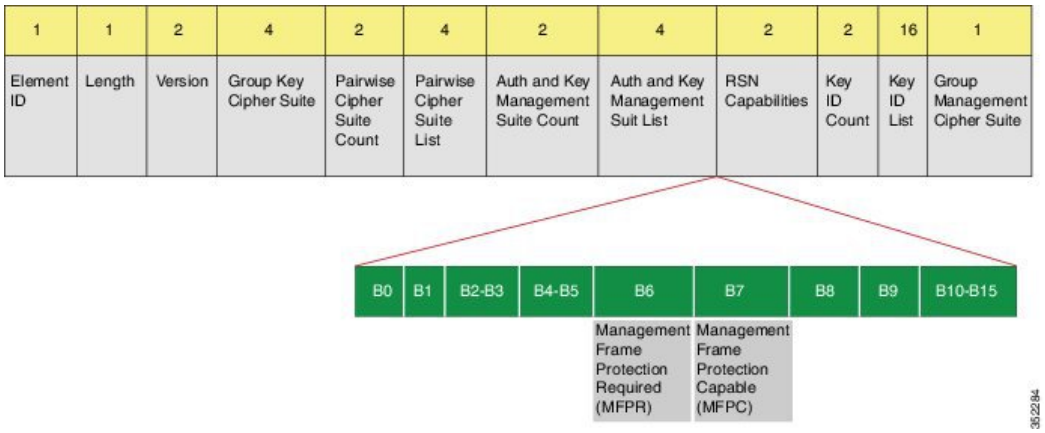


- If the AP later changes the GTK, it sends the new GTK and IGTK to the client using the Group Key Handshake .

802.11w defines a new Broadcast/Multicast Integrity Protocol (BIP) that provides data integrity and replay protection for broadcast/multicast robust management frames after successful establishment of an IGTKSA - It adds a MIC that is calculated using the shared IGTK key.

802.11w Information Elements (IEs)

Figure 32: 802.11w Information Elements

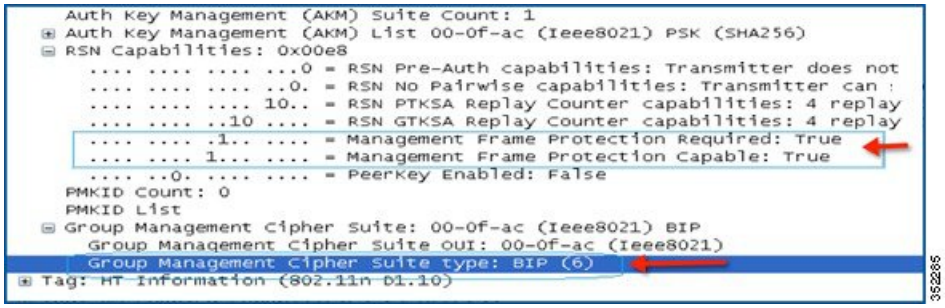


1. Modifications made in the RSN capabilities field of RSNIE.
   a. Bit 6: Management Frame Protection Required (MFPR)
   b. Bit 7: Management Frame Protection Capable (MFPC)
2. Two new AKM Suites, 5 and 6 are added for AKM Suite Selectors.
3. New Cipher Suite with type 6 is added to accommodate BIP.

The WLC adds this modified RSNIE in association and re-association responses and the APs add this modified RSNIE in beacons and probe responses.

The following Wireshark captures shows the RSNIE capabilities and the Group Management Cipher Suite elements.

Figure 33: 802.11w Information Elements



Security Association (SA) Teardown Protection

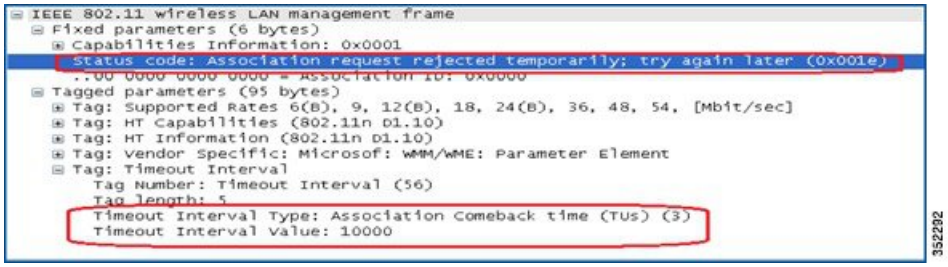
SA teardown protection is a mechanism to prevent replay attacks from tearing down the session of an existing client. It consists of an Association Comeback Time and an SA-Query procedure preventing spoofed association requests from disconnecting an already connected client.

If a client has a valid security association, and has negotiated 802.11w, the AP shall reject another Association Request with status code 30. This status code stands for "Association request rejected temporarily; Try again later". The AP should not tear down or otherwise modify the state of the existing association until the SA-Query

procedure determines that the original SA is invalid and shall include in the Association Response an Association Comeback Time information element, specifying a comeback time when the AP would be ready to accept an association with this client.

The following capture shows the Association Reject message with status code 0x1e (30) and the Association comeback time set to 10 seconds.

Figure 34: Association Reject with Comeback Time



Following this, if the AP is not already engaged in an SA Query with the client, the AP shall issue an SA Query until a matching SA Query response is received or the Association Comeback time expires. An AP may interpret reception of a valid protected frame as an indication of a successfully completed SA Query.

If a SA QUERY response with a matching transaction identifier within the time period, the AP shall allow the association process to be started without starting additional SA Query procedures.

Prerequisites for 802.11w

- To configure 802.11w feature for optional and mandatory, you must have WPA and AKM configured.

Note The RNS (Robust Secure Network) IE must be enabled with an AES Cipher.

Restrictions for 802.11w

- 802.11w cannot be applied on an open WLAN, WEP-encrypted WLAN, or a TKIP-encrypted WLAN.
- Cisco Catalyst 9800 Series Wireless Controller supports 802.11w + PMF combination for non-Apple clients. But Apple iOS version 11 and earlier require fix from the Apple iOS side to resolve the association issues.
- The controller will ignore disassociation or deauthentication frames sent by the clients if they are not using 802.11w PMF. The client entry will only get deleted immediately upon reception of such a frame if the client uses PMF. This is to avoid denial of service by malicious device since there is no security on those frames without PMF.

How to Configure 802.11w

Configuring 802.11w (GUI)

Before you begin

WPA and AKM must be configured.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add** to create WLANs.

The **Add WLAN** page is displayed.

Step 3 In the **Security** > **Layer2** tab, navigate to the **Protected Management Frame** section.

Step 4 Choose **PMF** as *Disabled*, *Optional*, or *Required*. By default, the PMF is *disabled*.

If you choose **PMF** as *Optional* or *Required*, you get to view the following fields:

- **Association Comeback Timer**—Enter a value between 1 and 10 seconds to configure 802.11w association comeback time.
- **SA Query Time**—Enter a value between 100 to 500 (milliseconds). This is required for clients to negotiate 802.11w PMF protection on a WLAN.

Step 5 Click **Save & Apply to Device**.

Configuring 802.11w (CLI)

Before you begin

WPA and AKM must be configured.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id ssid* **Example:** `Device(config)# wlan wlan-test 12 alpha`	Configures a WLAN and enters configuration mode.

	Command or Action	Purpose
Step 3	**security wpa akm dot1x-sha256** **Example:** `Device(config-wlan)#security wpa akm dot1x-sha256`	Configures 802.1x support.
Step 4	**security pmf association-comeback** *comeback-interval* **Example:** `Device(config-wlan)# security pmf association-comeback 10`	Configures the 802.11w association comeback time.
Step 5	**security pmf mandatory** **Example:** `Device(config-wlan)# security pmf mandatory`	Requires clients to negotiate 802.11w PMF protection on a WLAN.
Step 6	**security pmf saquery-retry-time** *timeout* **Example:** `Device(config-wlan)# security pmf saquery-retry-time 100`	Time interval identified in milliseconds before which the SA query response is expected. If the device does not get a response, another SQ query is tried.

Disabling 802.11w

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id ssid* **Example:** `Device(config)# wlan wlan-test 12 alpha`	Configures a WLAN and enters configuration mode.
Step 3	**no security wpa akm dot1x-sha256** **Example:** `Device(config-wlan)# no security wpa akm dot1x-sha256`	Disables 802.1x support.
Step 4	**no security pmf association-comeback** *comeback-interval* **Example:** `Device(config-wlan)# no security pmf association-comeback 10`	Disables the 802.11w association comeback time.

	Command or Action	Purpose
Step 5	**no security pmf mandatory** **Example:** `Device(config-wlan)# no security pmf mandatory`	Disables client negotiation of 802.11w PMF protection on a WLAN.
Step 6	**no security pmf saquery-retry-time** *timeout* **Example:** `Device(config-wlan)# no security pmf saquery-retry-time 100`	Disables SQ query retry.

Monitoring 802.11w

Use the following commands to monitor 802.11w.

Procedure

Step 1 **show wlan name** *wlan-name*

Displays the WLAN parameters on the WLAN. The PMF parameters are displayed.

```
. . . .
. . . .
Auth Key Management
            802.1x                          : Disabled
            PSK                             : Disabled
            CCKM                            : Disabled
            FT dot1x                        : Disabled
            FT PSK                          : Disabled
            FT SAE                          : Disabled
            Dot1x-SHA256                    : Enabled
            PSK-SHA256                      : Disabled
            SAE                             : Disabled
            OWE                             : Disabled
            SUITEB-1X                       : Disabled
            SUITEB192-1X                    : Disabled
    CCKM TSF Tolerance                      : 1000
    FT Support                              : Adaptive
        FT Reassociation Timeout            : 20
        FT Over-The-DS mode                 : Enabled
    PMF Support                             : Required
        PMF Association Comeback Timeout    : 1
        PMF SA Query Time                   : 500
. . . .
. . . .
```

Step 2 **show wireless client mac-address** *mac-address* **detail**

Displays the summary of the 802.11w authentication key management configuration on a client.

```
. . . .
. . . .
Policy Manager State: Run
```

```
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 497 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x-SHA256
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : Yes
EAP Type : LEAP
VLAN : 39
Multicast VLAN : 0
Access VLAN : 39
Anchor VLAN : 0
WFD capable : No
Manged WFD capable : No
. . . .
. . . .
```

CHAPTER 121

Ethernet over GRE

- Introduction to EoGRE, on page 1203
- Create a Tunnel Gateway, on page 1205
- Configuring a Tunnel Domain, on page 1206
- Configuring EoGRE Global Parameters, on page 1207
- Configuring a Tunnel Profile, on page 1207
- Associating WLAN to a Wireless Policy Profile, on page 1209
- Attaching a Policy Tag and a Site Tag to an AP, on page 1209
- Verifying the EoGRE Tunnel Configuration, on page 1210

Introduction to EoGRE

Ethernet over GRE (EoGRE) is an aggregation solution for grouping 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 Generic Routing Encapsulation (GRE) tunnel. When the IP GRE tunnels are terminated on a service provider's broadband network gateway, the end-host traffic is forwarded and subscriber sessions are initiated.

Client IPv6

Client IPv6 traffic is supported on IPv4 EoGRE tunnels. A maximum of eight different client IPv6 addresses are supported per client. Wireless controller s send all the client IPv6 addresses that they have learned to the accounting server using the accounting update message. All RADIUS or accounting messages exchanged between controller s and tunnel gateways or RADIUS servers are outside the EoGRE tunnel.

EoGRE for WLAN

To enable EoGRE for a WLAN, the wireless policy profile should be mapped to a tunnel profile, which may contain the following:

- AAA override: Allows you to bypass rule filtering for a client.
- Gateway RADIUS proxy: Allows forwarding of AAA requests to tunnel gateways.
- Tunnel rules: Defines the domain to use for each realm. They also define VLAN tagging for the client traffic towards tunnel gateways.
- DHCP option 82: Provides a set of predefined fields.

EoGRE Deployment with Multiple Tunnel Gateways

The wireless controller embedded wireless controller sends keepalive pings to the primary and secondary tunnel gateways and keeps track of the missed pings. When a certain threshold level is reached for the missed pings, switchover is performed and the secondary tunnel is marked as active. This switchover deauthenticates all the clients to enable them to rejoin the access points (APs). When the primary tunnel come back online, all the client traffic are reverted to the primary tunnel. However, this behavior depends on the type of redundancy.

Load Balancing in EtherChannels

Load balancing of tunneled traffic over Etherchannels works by hashing the source or destination IP addresses or mac addresses of the tunnel endpoint pair. Because the number of tunnels is very limited when compared to clients (each tunnel carries traffic for many clients), the spreading effect of hashing is highly reduced and optimal utilization of Etherchannel links can be hard to achieve.

Using the EoGRE configuration model, you can use the *tunnel source* option of each tunnel interface to adjust the load-balancing parameters and spread tunnels across multiple links.

You can use different source interfaces on each tunnel for load balancing based on the source or destination IP address. For that choose the source interface IP address in such a way that traffic flows take different links for each src-dest IP pair. The following is an example with four ports:

```
Client traffic on Tunnel1 – Src IP: 40.143.0.72  Dest IP: 40.253.0.2
Client traffic on Tunnel2 – Src IP: 40.146.0.94  Dest IP: 40.253.0.6
Client traffic on Tunnel3 – Src IP: 40.147.0.74  Dest IP: 40.253.0.10
```

Use the **show platform software port-channel link-select interface port-channel 4 ipv4** *src_ip dest_ip* command to determine the link that a particular flow will take.

EoGRE Configuration Overview

The EoGRE solution can be deployed in two different ways:

- Central-Switching: EoGRE tunnels connect the controller to the tunnel gateways.
- Flex or Local-Switching: EoGRE tunnels are initiated on the APs and terminated on the tunnel gateways.

To configure EoGRE, perform the following tasks:

1. Create a set of tunnel gateways.
2. Create a set of tunnel domains.
3. Create a tunnel profile with rules that define how to match clients to domains.
4. Create a policy profile and attach the tunnel profile to it.
5. Map the policy profile to WLANs using policy tags.

Note The EoGRE tunnel fallback to the secondary tunnel is triggered after the *max-skip-count* ping fails in the last measurement window. Based on the starting and ending instance of the measurement window, the fall-back may take more time than the duration that is configured.

Table 56: EoGRE Authentication Methods

Method Name	First Supported Release	Mode
PSK	17.2.1	Local/Flex (central authentication)
Open	16.12.1	Local/Flex (central authentication)
LWA	16.12.1	Local/Flex (central authentication)
Dot1x	16.12.1	Local/Flex (central authentication)
CWA	16.12.1	Local/Flex (central authentication)

Create a Tunnel Gateway

Note In the Cisco Catalyst 9800 Series Wireless Controller , a tunnel gateway is modeled as a tunnel interface.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface tunnel** *tunnel_number* **Example:** `Device(config)# interface tunnel 21`	Configures a tunnel interface and enters interface configuration mode.
Step 3	**tunnel source** *source_intf* **Example:** `Device(config-if)# tunnel source 22`	Sets the source address of the tunnel interface. The source interface can be VLAN, Gigabit Ethernet or loopback.
Step 4	**tunnel destination** *tunnel-address* **Example:** `Device(config-if)# tunnel destination 10.11.12.13`	Sets the destination address of the tunnel.
Step 5	**tunnel mode ethernet gre** {**ipv4** | **ipv6**} **p2p** **Example:** `Device(config-if)# tunnel mode ethernet gre ipv4 p2p`	Sets the encapsulation mode of the tunnel to Ethernet over GRE IPv4 or Ethernet over GRE IPv6.

Configuring a Tunnel Domain

Note Tunnel domains are a redundancy grouping of tunnels. The following configuration procedure specifies a primary and a secondary tunnel, along with a redundancy model.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**tunnel eogre domain** *domain* **Example:** `Device(config)# tunnel eogre domain dom1`	Configures EoGRE redundancy domain.
Step 3	**primary tunnel** *primary-tunnel_intf* **Example:** `Device(config-eogre-domain)# primary tunnel 21`	Configures the primary tunnel.
Step 4	**secondary tunnel** *secondary-tunnel_intf* **Example:** `Device(config-eogre-domain)# secondary tunnel 22`	Configures the secondary tunnel.
Step 5	**redundancy revertive** **Example:** `Device(config-eogre-domain)# redundancy revertive`	Sets the redundancy model as revertive. When redundancy is set to revertive and the primary tunnel goes down, a switchover to secondary tunnel is performed. When the primary tunnel comes back up, a switchover to the primary tunnel is performed, because the primary tunnel has priority over the secondary tunnel. When redundancy is not set to revertive, tunnels will have the same priority, and a switchover to the primary tunnel is not performed if the active tunnel is the secondary tunnel and the primary tunnel comes back up.

Configuring EoGRE Global Parameters

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**tunnel eogre heartbeat interval** *interval-value* **Example:** `Device(config)# tunnel eogre heartbeat interval 600`	Sets EoGRE tunnel heartbeat periodic interval.
Step 3	**tunnel eogre heartbeat max-skip-count** *skip-count* **Example:** `Device(config)# tunnel eogre heartbeat max-skip-count 7`	Sets the maximum number of tolerable dropped heartbeats. After reaching the maximum number of heartbeats that can be dropped, the tunnel is declared as down and a switchover is performed.
Step 4	**tunnel eogre source loopback** *tunnel_source* **Example:** `Device(config)# tunnel eogre source loopback 12`	Sets the tunnel EoGRE source interface.
Step 5	**tunnel eogre interface tunnel** *tunnel-intf* **aaa proxy key** *key key-name* **Example:** `Device(config)# tunnel eogre interface tunnel 21 aaa proxy key 0 mykey`	(Optional) Configures AAA proxy RADIUS key for the AAA proxy setup. **Note** When the tunnel gateway is behaving as the AAA proxy server, only this step is required for the configuration.

Configuring a Tunnel Profile

Before you begin

Ensure that you define the destination VLAN on the controller. If you do not define the VLAN, clients will not be able to connect.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy-name* **Example:** `Device(config)# wireless profile policy eogre_policy`	Configures a WLAN policy profile.
Step 3	**tunnel-profile** *tunnel-profile-name* **Example:** `Device(config-wireless-policy)# tunnel-profile tunnel1`	Creates a tunnel profile.
Step 4	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.
Step 5	**wireless profile tunnel** *tunnel-profile-name* **Example:** `Device(config)# wireless profile tunnel wl-tunnel-1`	Configures a wireless tunnel profile.
Step 6	**dhcp-opt82 enable** **Example:** `Device(config-tunnel-profile)# dhcp-opt82 enable`	Activates DHCP Option 82 for the tunneled clients.
Step 7	**dhcp-opt82 remote-id** *remote-id* **Example:** `Device(config-tunnel-profile)# dhcp-opt82 remote-id vlan`	Configures Remote ID options. Choose from the comma-separated list of options such as **ap-mac**, **ap-ethmac**, **ap-name**, **ap-group-name**, **flex-group-name**, **ap-location**, **vlan**, **ssid-name**, **ssid-type**, and **client-mac**.
Step 8	**aaa-override** **Example:** `Device(config-tunnel-profile)# aaa-override`	Enables AAA policy override.
Step 9	**gateway-radius-proxy** **Example:** `Device(config-tunnel-profile)# gateway-radius-proxy`	Enables the gateway RADIUS proxy.

	Command or Action	Purpose
Step 10	**gateway-accounting-radius-proxy** **Example:** `Device(config-tunnel-profile)# gateway-accounting-radius-proxy`	Enables the gateway accounting RADIUS proxy.
Step 11	**rule** *priority* **realm-filter** *realm* **domain** *domain-name* **vlan** *vlan-id* **Example:** `Device(config-tunnel-profile)# rule 12 realm-filter realm domain dom1 vlan 5`	Creates a rule to choose a domain, using the realm filter, for client Network Access Identifier (NAI), tunneling domain name, and destination VLAN.

Associating WLAN to a Wireless Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config)# wireless tag policy eogre_tag`	Configures a policy tag and enters policy tag configuration mode.
Step 3	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan eogre_open_eogre policy eogre_policy`	Maps an EoGRE policy profile to a WLAN profile.
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.

Attaching a Policy Tag and a Site Tag to an AP

Procedure

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

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap 80E8.6FD4.0BB0`	Configures an AP and enters AP profile configuration mode.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag eogre_tag`	Maps the EoGRE policy tag to the AP.
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag sp-flex-site`	Maps a site tag to the AP.
Step 5	**end** **Example:** `Device(config-ap-tag)# end`	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.

Verifying the EoGRE Tunnel Configuration

The `show tunnel eogre` command displays the EoGRE clients, domains, gateways, global-configuration, and manager information in the local mode.

To display the EoGRE domain summary in the local mode, use the following command:

```
Device# show tunnel eogre domain summary

Domain Name          Primary GW   Secondary GW      Active GW      Redundancy
-------------------------------------------------------------------------------
domain1              Tunnel1      Tunnel2           Tunnel1        Non-Revertive
eogre_domain         Tunnel1      Tunnel2           Tunnel1        Non-Revertive
```

To display the details of an EoGRE domain in the local mode, use the following command:

```
Device# show tunnel eogre domain detailed domain-name

Domain Name    : eogre_domain
 Primary GW    : Tunnel1
 Secondary GW  : Tunnel2
 Active GW     : Tunnel1
 Redundancy    : Non-Revertive
```

To view the EoGRE tunnel gateway summary and statistics in the local mode, use the following command:

```
Device# show tunnel eogre gateway summary

Name              Type  Address                                 AdminState  State  Clients
-------------------------------------------------------------------------------------------
Tunnel1            IPv4  9.51.1.11                               Up          Up     0
```

```
Tunnel2            IPv4  9.51.1.12                          Up          Down   0

Tunnel10           IPv6  fd09:9:8:21::90                    Down        Down   0

Tunnel11           IPv4  9.51.1.11                          Up          Up     0

Tunnel12           IPv6  fd09:9:8:21::90                    Up          Down   0

Tunnel100          IPv4  9.51.1.100                         Up          Down   0
```

To view the details of an EoGRE tunnel gateway in the local mode, use the following command:

```
Device# show tunnel eogre gateway detailed gateway-name

Gateway : Tunnel1
 Mode   : IPv4
 IP     : 9.51.1.11
 Source : Vlan51 / 9.51.1.1
 State  : Up
 SLA ID : 56
 MTU    : 1480
 Up Time: 4 minutes 45 seconds

 Clients
  Total Number of Wireless Clients      : 0
 Traffic
  Total Number of Received Packets      : 0
  Total Number of Received Bytes        : 0
  Total Number of Transmitted Packets   : 0
  Total Number of Transmitted Bytes     : 0
 Keepalives
  Total Number of Lost Keepalives       : 0
  Total Number of Received Keepalives   : 5
  Total Number of Transmitted Keepalives: 5
  Windows                               : 1
  Transmitted Keepalives in last window : 2
  Received Keepalives in last window    : 2
```

To view the client summary of EoGRE in the local mode, use the following command:

```
Device# show tunnel eogre client summary

Client MAC      AP MAC          Domain                              Tunnel        VLAN  Local
-------------------------------------------------------------------------------------------
74da.3828.88b0  80e8.6fd4.9520  eogre_domain                         N/A           2121   No
```

To view the details of an EoGRE global configuration in the local mode, use the following command:

```
Device# show tunnel eogre global-configuration

Heartbeat interval       : 60
Max Heartbeat skip count : 3
Source Interface         : (none)
```

To view the details of the global tunnel manager statistics in the local mode, use the following command:

```
Device# show tunnel eogre manager stats global

Tunnel Global Statistics
Last Updated                    : 02/18/2019 23:50:35
EoGRE Objects
```

```
  Gateways                       : 6
  Domains                        : 2

EoGRE Flex Objects
  AP Gateways                    : 2
  AP Domains                     : 1
  AP Gateways HA inconsistencies : 0
  AP Domains HA inconsistencies  : 0

Config events
  IOS Tunnel updates             : 806
  IOS Domain updates             : 88
  Global updates                 : 48
  Tunnel Profile updates         : 120
  Tunnel Rule updates            : 16
  AAA proxy key updates          : 0

AP events
  Flex AP Join                   : 1
  Flex AP Leave                  : 0
  Local AP Join                  : 0
  Local AP leave                 : 0
  Tunnel status (rx)             : 4
  Domain status (rx)             : 1
  IAPP stats msg (rx)            : 3
  Client count (rx)              : 6
  VAP Payload msg (tx)           : 4
  Domain config (tx)             : 1
  Global config (tx)             : 1
  Client delete (tx)             : 1
  Client delete per domain (tx)  : 3
  DHCP option 82 (tx)            : 4

Client events
  Add-mobile                     : 2
  Run-State                      : 3
  Delete                         : 1
  Cleanup                        : 0
  Join                           : 2
  Plumb                          : 0
  Join Errors                    : 0
  HandOff                        : 0
  MsPayload                      : 2
  FT Recover                     : 0
  Zombie GW counter increase     : 0
  Zombie GW counter decrease     : 0
  Tunnel Profile reset           : 88
  Client deauth                  : 0
  HA reconciliation              : 0

Client Join Events
  Generic Error                  : 0
  MSPayload Fail                 : 0
  Invalid VLAN                   : 0
  Invalid Domain                 : 0
  No GWs in Domain               : 0
  Domain Shut                    : 0
  Invalid GWs                    : 0
  GWs Down                       : 0
  Rule Match Error               : 0
  AAA-override                   : 0
  Flex No Active GW              : 0
  Open Auth join attempt         : 2
  Dot1x join attempt             : 2
```

```
  Mobility join attempt          : 0
  Tunnel Profile not valid       : 2
  Tunnel Profile valid           : 2
  No rule match                  : 0
  Rule match                     : 2
  AAA proxy                      : 0
  AAA proxy accounting           : 0
  AAA eogre attributes           : 0
  Has aaa override               : 0
  Error in handoff payload       : 0
  Handoff AAA override           : 0
  Handoff no AAA override        : 0
  Handoff payload received       : 0
  Handoff payload sent           : 0

SNMP Traps
  Client                         : 0
  Tunnel                         : 2
  Domain                         : 0

IPC
  IOSd TX messages               : 0

Zombie Client
  Entries                        : 0
```

To view the tunnel manager statistics of a specific process instance in the local mode, use the following command:

```
Device# show tunnel eogre manager stats instance instance-number

Tunnel Manager statistics for process instance : 0
Last Updated                     : 02/18/2019 23:50:35
EoGRE Objects
  Gateways                       : 6
  Domains                        : 2

EoGRE Flex Objects
  AP Gateways                    : 2
  AP Domains                     : 1
  AP Gateways HA inconsistencies : 0
  AP Domains HA inconsistencies  : 0

Config events
  IOS Tunnel updates             : 102
  IOS Domain updates             : 11
  Global updates                 : 6
  Tunnel Profile updates         : 15
  Tunnel Rule updates            : 2
  AAA proxy key updates          : 0

AP events
  Flex AP Join                   : 1
  Flex AP Leave                  : 0
  Local AP Join                  : 0
  Local AP leave                 : 0
  Tunnel status (rx)             : 4
  Domain status (rx)             : 1
  IAPP stats msg (rx)            : 3
  Client count (rx)              : 6
  VAP Payload msg (tx)           : 4
  Domain config (tx)             : 1
  Global config (tx)             : 1
```

```
  Client delete (tx)              : 1
  Client delete per domain (tx)   : 3
  DHCP option 82 (tx)             : 4

Client events
  Add-mobile                      : 2
  Run-State                       : 3
  Delete                          : 1
  Cleanup                         : 0
  Join                            : 2
  Plumb                           : 0
  Join Errors                     : 0
  HandOff                         : 0
  MsPayload                       : 2
  FT Recover                      : 0
  Zombie GW counter increase      : 0
  Zombie GW counter decrease      : 0
  Tunnel Profile reset            : 11
  Client deauth                   : 0
  HA reconciliation               : 0

Client Join Events
  Generic Error                   : 0
  MSPayload Fail                  : 0
  Invalid VLAN                    : 0
  Invalid Domain                  : 0
  No GWs in Domain                : 0
  Domain Shut                     : 0
  Invalid GWs                     : 0
  GWs Down                        : 0
  Rule Match Error                : 0
  AAA-override                    : 0
  Flex No Active GW               : 0
  Open Auth join attempt          : 2
  Dot1x join attempt              : 2
  Mobility join attempt           : 0
  Tunnel Profile not valid        : 2
  Tunnel Profile valid            : 2
  No rule match                   : 0
  Rule match                      : 2
  AAA proxy                       : 0
  AAA proxy accounting            : 0
  AAA eogre attributes            : 0
  Has aaa override                : 0
  Error in handoff payload        : 0
  Handoff AAA override            : 0
  Handoff no AAA override         : 0
  Handoff payload received        : 0
  Handoff payload sent            : 0

SNMP Traps
  Client                          : 0
  Tunnel                          : 2
  Domain                          : 0

IPC
  IOSd TX messages                : 0

Zombie Client
  Entries                         : 0
```

The `show ap tunnel eogre` command displays the tunnel domain information, EoGRE events, and the tunnel gateway status on the APs, in the flex mode.

To view the summary information of an EoGRE tunnel gateway in the flex mode, use the following command:

```
Device# show ap tunnel eogre domain summary

AP MAC          Domain                          Active Gateway
-----------------------------------------------------------------------------
80e8.6fd4.9520  eogre_domain                    Tunnel1
```

To view the wireless tunnel profile summary, use the following command:

```
Device# show wireless profile tunnel summary

Profile Name                    AAA-Override AAA-Proxy DHCP Opt82 Enabled
------------------------------- ------------ --------- ---------- ---------
eogre_tunnel                             No        No        Yes       Yes
eogre_tunnel_set                         No        No        Yes        No
eogre_tunnel_snmp                        No        No         No        No
```

To view a wireless tunnel profile's details, use the following command:

```
Device# show wireless profile tunnel detailed profile-name

Profile Name : eogre_tunnel
Status : Enabled
 AAA-Proxy/Accounting-Proxy: Disabled / Disabled
 AAA-Override : Disabled
 DHCP Option82 : Enabled
  Circuit-ID : ap-mac,ap-ethmac,ap-location,vlan
  Remote-ID : ssid-name,ssid-type,client-mac,ap-name

Tunnel Rules

Priority Realm                Vlan Domain (Status/Primary GW/Secondary GW)
-------- -------------------- ---- ---------------------------------------
1        *                    2121 eogre_domain (Enabled/Tunnel1/Tunnel2)
```

To view detailed information about an EoGRE tunnel domain's status, use the following command:

```
Device# show ap tunnel eogre domain detailed

Domain     : eogre_domain
AP MAC     : 80e8.6fd4.9520
Active GW  : Tunnel1
```

To view the EoGRE events on an AP, use the following command:

```
Device# show ap tunnel eogre events

AP 80e8.6fd4.9520  Event history
Timestamp               #Times   Event                RC Context
----------------------- -------- -------------------- --
----------------------------------------
02/18/2019 23:50:26.341 6        IAPP_STATS           0 GW Tunnel2 uptime:0s

02/18/2019 23:49:40.222 2        CLIENT_JOIN          0 74da.3828.88b0, (eogre_domain/2121)

02/18/2019 23:48:43.549 1        CLIENT_LEAVE         0 74da.3828.88b0, (eogre_domain/2121)

02/18/2019 23:47:33.127 1        DOMAIN_STATUS        0 eogre_domain Active GW: Tunnel1

02/18/2019 23:47:33.124 4        AP_TUNNEL_STATUS     0 Tunnel2 Dn
```

```
02/18/2019 23:47:33.124 1        MSG_CLIENT_DEL       0 GW Tunnel2 (IP: 9.51.1.12)

02/18/2019 23:47:33.124 2        TUNNEL_ADD           0 GW Tunnel2

02/18/2019 23:47:33.120 3        MSG_CLIENT_DEL_PD    0 GW Tunnel1 (IP: 9.51.1.11)

02/18/2019 23:47:31.763 2        AP_DOMAIN_PUSH       0 Delete:eogre_domain_set, 0 GWs

02/18/2019 23:47:31.753 4        AP_VAP_PUSH          0 profile:'eogre_tunnel',
wlan:pyats_eogre
```

To view the summary information of the EoGRE tunnel gateway, use the following command:

```
Device# show ap tunnel eogre gateway summary

AP MAC          Gateway         Type  IP                                        State  Clients
-----------------------------------------------------------------------------------------------
80e8.6fd4.9520  Tunnel1          IPv4  9.51.1.11                                   Up     1

80e8.6fd4.9520  Tunnel2          IPv4  9.51.1.12                                   Down   0
```

To view detailed information about an EoGRE tunnel gateway, use the following command:

```
Device# show ap tunnel eogre gateway detailed gateway-name

Gateway : Tunnel1
 Mode   : IPv4
 IP     : 9.51.1.11
 State  : Up
 MTU    : 1476
 Up Time: 14 hours 25 minutes 2 seconds
 AP MAC : 80e8.6fd4.9520

 Clients
  Total Number of Wireless Clients      : 1
 Traffic
  Total Number of Received Packets      : 6
  Total Number of Received Bytes        : 2643
  Total Number of Transmitted Packets   : 94
  Total Number of Transmitted Bytes     : 20629
  Total Number of Lost Keepalive        : 3
```

To view summary information about the EoGRE tunnel gateway status, use the following command:

```
Device# show ap tunnel eogre domain summary

AP MAC          Domain                          Active Gateway
-------------------------------------------------------------------------------
80e8.6fd4.9520  eogre_domain                    Tunnel1
```

To view information about EoGRE events on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre events

AP 80e8.6fd4.9520  Event history
Timestamp               #Times   Event               RC Context
----------------------- -------- ------------------- --
----------------------------------------
02/18/2019 23:50:26.341 6        IAPP_STATS           0 GW Tunnel2 uptime:0s

02/18/2019 23:49:40.222 2        CLIENT_JOIN         0 74da.3828.88b0, (eogre_domain/2121)

02/18/2019 23:48:43.549 1        CLIENT_LEAVE        0 74da.3828.88b0, (eogre_domain/2121)
```

```
02/18/2019 23:47:33.127 1        DOMAIN_STATUS        0 eogre_domain Active GW: Tunnel1

02/18/2019 23:47:33.124 4        AP_TUNNEL_STATUS     0 Tunnel2 Dn

02/18/2019 23:47:33.124 1        MSG_CLIENT_DEL       0 GW Tunnel2 (IP: 9.51.1.12)

02/18/2019 23:47:33.124 2        TUNNEL_ADD           0 GW Tunnel2

02/18/2019 23:47:33.120 3        MSG_CLIENT_DEL_PD    0 GW Tunnel1 (IP: 9.51.1.11)

02/18/2019 23:47:31.763 2        AP_DOMAIN_PUSH       0 Delete:eogre_domain_set, 0 GWs

02/18/2019 23:47:31.753 4        AP_VAP_PUSH          0 profile:'eogre_tunnel',
wlan:pyats_eogre
```

To view the summary information about EoGRE tunnel domain's status on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre domain summary
```

```
AP MAC          Domain                            Active Gateway
-------------------------------------------------------------------------------
80e8.6fd4.9520  eogre_domain
```

To view the detailed information about EoGRE tunnel domain on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre domain detailed
```

```
Domain Name    : eogre_domain
 Primary GW    : Tunnel1
 Secondary GW  : Tunnel2
 Active GW     : Tunnel1
 Redundancy    : Non-Revertive
 AdminState    : Up
```

To view the summary information about EoGRE tunnel gateways on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre gateway summary
```

```
AP MAC          Gateway          Type  IP                                      State  Clients
-------------------------------------------------------------------------------------------
80e8.6fd4.9520  Tunnel1          IPv4  9.51.1.11                                 Up     1

80e8.6fd4.9520  Tunnel2          IPv4  9.51.1.12                                 Down   0
```

To view detailed information about an EoGRE tunnel gateway's status on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre gateway detailed gateway-name
```

```
Gateway : Tunnel2
 Mode   : IPv4
 IP     : 9.51.1.12
 State  : Down
 MTU    : 0
 AP MAC : 80e8.6fd4.9520

 Clients
  Total Number of Wireless Clients      : 0
 Traffic
  Total Number of Received Packets      : 0
  Total Number of Received Bytes        : 0
  Total Number of Transmitted Packets   : 0
```

```
Total Number of Transmitted Bytes     : 0
Total Number of Lost Keepalive        : 151
```

PART XVII

Multicast Domain Name System

- Multicast Domain Name System, on page 1221

CHAPTER 122

Multicast Domain Name System

- Introduction to mDNS Gateway, on page 1221
- Enabling mDNS Gateway (GUI), on page 1222
- Enabling or Disabling mDNS Gateway (GUI), on page 1223
- Enabling or Disabling mDNS Gateway (CLI), on page 1223
- Creating Default Service Policy, on page 1224
- Creating Custom Service Definition (GUI), on page 1225
- Creating Custom Service Definition, on page 1225
- Creating Service List (GUI), on page 1226
- Creating Service List, on page 1226
- Creating Service Policy (GUI), on page 1228
- Creating Service Policy, on page 1228
- Configuring an mDNS Flex Profile (GUI), on page 1229
- Configuring an mDNS Flex Profile (CLI), on page 1230
- Applying an mDNS Flex Profile to a Wireless Flex Connect Profile (GUI), on page 1231
- Applying an mDNS Flex Profile to a Wireless Flex Connect Profile (CLI), on page 1231
- Associating mDNS Service Policy with Wireless Profile Policy (GUI), on page 1232
- Associating mDNS Service Policy with Wireless Profile Policy, on page 1232
- Enabling or Disabling mDNS Gateway for WLAN (GUI), on page 1234
- Enabling or Disabling mDNS Gateway for WLAN, on page 1234
- mDNS Gateway with Guest Anchor Support and mDNS Bridging, on page 1235
- Configuring mDNS Gateway on Guest Anchor, on page 1236
- Configuring mDNS Gateway on Guest Foreign (Guest WLAN), on page 1236
- Verifying mDNS Gateway Configurations, on page 1237

Introduction to mDNS Gateway

Multicast Domain Name System (mDNS) is an Apple service discovery protocol which locates devices and services on a local network with the use of mDNS service records.

The Bonjour protocol operates on service announcements and queries. Each query or advertisement is sent to the Bonjour multicast address ipv4 224.0.0.251 (ipv6 FF02::FB). This protocol uses mDNS on UDP port 5353.

The address used by the Bonjour protocol is link-local multicast address and therefore is only forwarded to the local L2 network. As, multicast DNS is limited to an L2 domain for a client to discover a service it has to be part of the same L2 domain, This is not always possible in any large scale deployment or enterprise.

In order to address this issue, the Cisco Catalyst 9800 Series Wireless Controller acts as a Bonjour Gateway. The controller then listens for Bonjour services, caches these Bonjour advertisements (AirPlay, AirPrint, and so on) from the source or host. For example, Apple TV responds back to Bonjour clients when asked or requested for a service. This way you can have sources and clients in different subnets.

By default, the mDNS gateway is disabled on the controller. To enable mDNS gateway functionality, you must explicitly configure mDNS gateway using CLI or Web UI.

Prerequisite

Since the Cisco Catalyst 9800 Series Wireless Controller will respond and advertise for services cached when acting as a Bonjour Gateway, it must have an SVI interface with a valid IP address on every VLAN where mDNS is allowed or used. This will be the source IP address of those mDNS packets that are coming out from the controller acting as mDNS Gateway.

Enabling mDNS Gateway (GUI)

Procedure

Step 1 Choose **Configuration > Services > mDNS**.

Step 2 In the **Global** section, toggle the slider to enable or disable the **mDNS Gateway**.

Step 3 From the **Transport** drop-down list, choose one of the following types:

- **ipv4**
- **ipv6**
- **both**

Step 4 Enter an appropriate timer value in **Active-Query Timer**. The valid range is between 15 to 120 minutes. The default is 30 minutes.

Step 5 From the **mDNS-AP Service Policy** drop-down list, choose an mDNS service policy.

Note Service policy is optional only if mDNS-AP is configured. If mDNS-AP is not configured, the system uses default-service-policy.

Step 6 Click **Apply**.

Enabling or Disabling mDNS Gateway (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **mDNS** > **Global**.

Step 2 Enable or disable the **mDNS Gateway** toggle button.

Step 3 Choose **ipv4** or **ipv6** or **both** from the **Transport** drop-down list.

Step 4 Enter the **Active-Query Timer**.

Step 5 Click **Apply**.

Enabling or Disabling mDNS Gateway (CLI)

Note

- mDNS gateway is disabled by default globally on the controller.
- You need both global and WLAN configurations to enable mDNS gateway.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged **EXEC** mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd gateway** **Example:** `Device(config)# mdns-sd gateway`	Enables mDNS gateway.
Step 4	**transport** {**ipv4** | **ipv6** | **both**} **Example:** `Device(config-mdns-sd)# transport ipv4`	Processes mDNS message on a specific transport. Here, **ipv4** signifies that the IPv4 mDNS message processing is enabled. This is the default value.

	Command or Action	Purpose
		ipv6 signifies that the IPv6 mDNS message processing is enabled. **both** signifies that the IPv4 and IPv6 mDNS message is enabled for each network.
Step 5	**active-query timer** *active-query-periodicity* **Example:** `Device(config-mdns-sd)# active-query timer 15`	Changes the periodicity of mDNS multicast active query. **Note** An active query is a periodic mDNS query to refresh dynamic cache. Here, *active-query-periodicity* refers to the active query periodicity in Minutes. The valid range is from 15 to 120 minutes. Active query runs with a default periodicity of 30 minutes.
Step 6	**exit** **Example:** `Device(config-mdns-sd)# exit`	Returns to global configuration mode.

Creating Default Service Policy

When the mdns gateway is enabled on any of the WLANs by default, mdns-default-service-policy is associated with it. Default service policy consists of default-service-list and their details are explained in this section. You can override the default service policy with a custom service policy.

Procedure

Step 1 Create a service-definition if the service is not listed in the preconfigured services.

Step 2 Create a service list for IN and OUT by using the service-definitions.

Step 3 Use the existing service list to create a new service. For more information, refer to *Creating Service Policy* section.

Step 4 Attach the mdns-service-policy to the profile or VLAN that needs to be enforced.

Step 5 To check the default-mdns-service list, use the following command:

show mdns-sd default-service-list

Creating Custom Service Definition (GUI)

Procedure

Step 1 Choose **Configuration > Services > mDNS**.

Step 2 In the **Service Definition** section, click **Add**.

Step 3 In the **Quick Setup: Service Definition** page that is displayed, enter a name and description for the service definition.

Step 4 Enter a service type and click **+** to add the service type.

Step 5 Click **Apply to Device**.

Creating Custom Service Definition

Service definition is a construct that provides an admin friendly name to one or more mDNS service types or A pointer (PTR) Resource Record Name.

By default, few built-in service definitions are already predefined and available for admin to use.

In addition to built-in service definitions, admin can also define custom service definitions.

You can execute the following command to view the list of all the service definitions (built-in and custom):

```
Device# show mdns-sd master-service-list
```

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged **EXEC** mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-definition** *service-definition-name* **Example:** `Device(config)# mdns-sd service-definition CUSTOM1`	Configures mDNS service definition. **Note** • All the created custom service definitions are added to the primary service list. • Primary service list comprises of a list of custom and built-in service definitions.

	Command or Action	Purpose
Step 4	**service-type** *string* **Example:** `Device(config-mdns-ser-def)# service-type _custom1._tcp.local`	Configures mDNS service type.
Step 5	**exit** **Example:** `Device(config-mdns-ser-def)# exit`	Returns to global configuration mode.

Creating Service List (GUI)

Procedure

Step 1 Choose **Configuration > Services > mDNS**.

Step 2 In the **Service List** section, click **Add**.

Step 3 In the **Quick Setup: Service List** page that is displayed, enter a name for the service list.

Step 4 From the **Direction** drop-down list, choose **IN** for inbound filtering or **OUT** for outbound filtering.

Step 5 From the **Available Services** drop-down list, choose a service type to match the service list.

Note To allow all services, choose the **all** option.

Step 6 Click **Add Services**.

Step 7 From the **Message Type** drop-down list, choose the message type to match from the following options:

- **any**—To allow all messages.
- **announcement**—To allow only service advertisements or announcements for the device.
- **query**—To allow only a query from the client for a service in the network.

Step 8 Click **Save** to add services.

Step 9 Click **Apply to Device**.

Creating Service List

mDNS service list is a collection of service definitions.

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged **EXEC** mode.

	Command or Action	Purpose
	Example: `Device> enable`	Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**mdns-sd service-list** *service-list-name* {**IN** | **OUT**}
	Example:
	`Device(config)# mdns-sd service-list Basic-In IN`
	`Device(config)# mdns-sd service-list Basic-Out OUT`
		Configures mDNS service list.
		• **IN**: Provides inbound filtering.
		• **Out**: Provides outbound filtering.

Step 4	**match** *service-definition-name* **message-type** {**announcement** | **any** | **query**} **Example:** `Device(config-mdns-sl-in)# match CUSTOM1 message-type query`	Matches the service to the message type. Here, *service-definition-name* refers to the names of services, such as, airplay, airserver, airtunes, and so on. **Note** To add a service, the service name must be part of the primary service list. If the mDNS service list is set to IN, you get to view the following command: **match service-definition-name message-type {announcement | any | query}**. If the mDNS service list is set to Out, you get to view the following command: **match service-definition-name**.
Step 5	**show mdns-sd service-list {direction | name }**	Displays inbound or outbound direction list of the configured service-list to classify matching service-types for service-policy. The list can be filtered by name or specific direction.
Step 6	**exit** **Example:** `Device(config-mdns-sl-in)# exit`	Returns to global configuration mode.

Creating Service Policy (GUI)

Procedure

Step 1 Choose **Configuration > Services > mDNS**.

Step 2 In the **Service Policy** section, click **Add**.

Step 3 In the **Quick Setup: Service Policy** page that is displayed, enter a name for the service policy.

Step 4 From the **Service List Input** drop-down list, choose one of the types.

Step 5 From the **Service List Output** drop-down list, choose one of the types.

Step 6 From the **Location** drop-down list, choose the location you want to associate with the service list.

Step 7 Click **Apply to Device**.

Creating Service Policy

mDNS service policy is used for service filtering while learning services or responding to queries.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged **EXEC** mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy mdns-policy1`	Enables mDNS service policy.
Step 4	**location** {**lss** | **site-tag**} **Example:**	Filters mDNS service types based on LSS or site-tag.

	Command or Action	Purpose
	`Device(config-mdns-ser-pol)# location lss`	**Note** In Location Specific Services (LSS) based filtering, the mDNS gateway responds with the service instances learnt from the neighboring APs of the querying client AP. Other service instances for the rest of APs are filtered. In Site tag based filtering, the mDNS gateway responds with the service instances that belong to the same site-tag as that of querying client. The mDNS gateway responds back with wired services even if the location based filtering is configured.
Step 5	**service-list** *service-list-name* {**IN** | **OUT**} **Example:** `Device(config-mdns-ser-pol)# service-list VLAN100-list IN`	Configures various service-list names for IN and OUT directions. **Note** If an administrator decides to create or use a custom service policy, then the custom service policy must be configured with service-lists for both directions (IN and OUT); otherwise, the mDNS Gateway will not work (will not learn services if there is no IN service-list, or will not reply or announce services learned if there is no OUT service-list).
Step 6	**exit** **Example:** `Device(config-mdns-ser-pol)# exit`	Returns to global configuration mode.

Configuring an mDNS Flex Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **mDNS**.

Step 2 In the **mDNS Flex Profile** section, click **Add**.
The **Add mDNS Flex Profile** window is displayed.

Step 3 In the **Profile Name** field, enter the flex mDNS profile name.

Step 4 In the **Service Cache Update Timer** field, specify the service cache update time. The default value is 1 minute. The valid range is from 1 to 100 minutes.

Step 5 In the **Statistics Update Timer** field, specify the statistics update timer. The default value is 1 minute. The valid range is from 1 to 100 minutes.

Step 6 In the **VLANs** field, specify the VLAN ID. You can enter multiple VLAN IDs separated by commas, or enter a range of VLAN IDs. Maximum number of VLANs allowed is 16.

Step 7 Click **Apply to Device**.

Configuring an mDNS Flex Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**mdns-sd flex-profile** *mdns-flex-profile-name* **Example:** `Device(config)# mdns-sd flex-profile mdns-flex-profile-name`	Enters the mDNS Flex Profile mode.
Step 3	**update-timer service-cache** *service-cache timer-value <1-100>* **Example:** `Device(config-mdns-flex-profile)# update-timer service-cache 60`	Configures the mDNS update service cache timer for the flex profile. The default value is 1 minute. Value range is between 1 minute and 100 minutes.
Step 4	**update-timer statistics** *statistics timer-value <1-100>* **Example:** `Device(config-mdns-flex-profile)# update-timer statistics 65`	Configures the mDNS update statistics timer for the flex profile. The default value is 1 minute. The valid range is from 1 to 100 minutes.
Step 5	**wired-vlan-range** *wired-vlan-range value* **Example:** `Device(config-mdns-flex-profile)# wired-vlan-range 10 - 20`	Configures the mDNS wired VLAN range for the flex profile. The default value is 1 minute. The valid range is from 1 minute to 100 minutes.

Applying an mDNS Flex Profile to a Wireless Flex Connect Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 Click **Add**.
The **Add Flex Profile** window is displayed.

Step 3 Under the **General** tab, from the **mDNS Flex Profile** drop-down list, choose a flex profile name from the list.

Step 4 Click **Apply to Device**.

Applying an mDNS Flex Profile to a Wireless Flex Connect Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *wireless-flex-profile-name* **Example:** `Device# wireless profile flex wireless-flex-profile-name`	Enters wireless flex profile configuration mode.
Step 3	**mdns-sd** *mdns-flex-profile* **Example:** `Device(config-wireless-flex-profile)# mdns-sd mdns-flex-profile-name`	Enables the mDNS features for all the APs in the profile

Associating mDNS Service Policy with Wireless Profile Policy (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the **policy profile** name.

Step 3 In the **Advanced** tab, choose the mDNS service policy from the **mDNS Service Policy** drop-down list.

Step 4 Click **Update & Apply to Device**.

Associating mDNS Service Policy with Wireless Profile Policy

Note You must globally configure the mDNS service policy before associating it with the wireless profile policy.

A default mDNS service policy is already attached once the wireless profile policy is created. You can use the following commands to override the default mDNS service policy with any of your service policy:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures wireless profile policy. Here, *profile-policy* refers to the name of the WLAN policy profile.
Step 3	**mdns-sd service-policy** *custom-mdns-service-policy* **Example:** `Device(config-wireless-policy)# mdns-sd service-policy custom-mdns-service-policy`	Associates an mDNS service policy with the wireless profile policy. The default mDNS service policy name is **default-mdns-service-policy**.

	Command or Action	Purpose
		Note The **default-mdns-profile-policy** uses **default-mdns-service-list** configuration for filtering mDNS service announcement and queries. In wireless network, the mDNS packets are consumed by the mDNS gateway and clients or device is deprived of learning this service. To share the service with the device and provide ease of configuration to the administrator, a list of few standard service types are shared by default on the wireless network. The list of such standard service types is termed as default service policy that comprises a set of service types. The table covers a sample service list in the default service policy. ***Table 57: Default Name and mDNS Service Type*** **Default Name** / **mDNS Service Type** Apple HomeSharing / _home-sharing._tcp.local Printer-IPPS / _ipps._tcp.local Google-chromecast / _googlecast._tcp.local **Note** • Location would be disabled on mDNS default service policy. • You cannot change the contents of the mDNS default service policy. However, you can create separate mDNS service policies and associate them under the wireless policy profile.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.

Enabling or Disabling mDNS Gateway for WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click on the WLAN.

Step 3 In the **Advanced** tab, choose the mode in **mDNS Mode** drop-down list.

Step 4 Click **Update & Apply to Device**.

Enabling or Disabling mDNS Gateway for WLAN

Note Bridging is the default behaviour. This means that the mDNS packets are always bridged.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id ssid-name* **Example:** `Device(config)# wlan test 24 ssid1`	Specifies the WLAN name and ID. • *profile-name* is the WLAN name which can contain 32 alphanumeric characters • *wlan-id* is the wireless LAN identifier. The valid range is from 1 to 512. • *ssid-name* is the SSID which can contain 32 alphanumeric characters. **Note** Global configuration must be in place for mDNS gateway to work.

	Command or Action	Purpose

Step 3	**mdns-sd-interface** {**gateway** | **drop**}
	Example:
	`Device(config-wlan)# mdns-sd gateway`
	`Device(config-wlan)# mdns-sd drop`
		Enables or disables mDNS gateway and bridge functions on WLAN.

Step 4	**exit** **Example:** `Device(config-wlan)# exit`	Returns to global configuration mode.
Step 5	**show wlan name** *wlan-name* | **show wlan all** **Example:** `Device# show wlan name test | show wlan all`	Verifies the status of mDNS on WLAN.
Step 6	**show wireless profile policy** **Example:** `Device# show wireless profile policy`	Verifies the service policy configured in WLAN.

mDNS Gateway with Guest Anchor Support and mDNS Bridging

When mDNS Gateway is enabled on both Anchor and Foreign controller, the mDNS gateway functionality is supported in guest anchor deployment where clients on guest LAN or WLAN with guest anchor enabled will be responded with any services or cache from export foreign controller itself. All advertisements received on Guest LAN or WLAN on export foreign are learnt on the export foreign itself. All queries received on guest LAN or WLAN are responded by the export foreign itself.

When mDNS Gateway is enabled on Anchor and Disabled on Foreign controller [Bridging Mode], the mDNS gateway functionality is supported in guest anchor deployment where clients on guest LAN or WLAN with guest anchor enabled will be responded with any services or cache from export Anchor even though the clients are connected on Foreign. All advertisements received on guest LAN or WLAN on export foreign is forwarded to Anchor and the cache is stored on the Anchor itself. All queries received on guest LAN or WLAN are responded by the export Anchor itself.

Note

- You must configure the guest-LAN to a wireless profile policy which is configured with the required mDNS service-policy.
- To configure non guest LAN mDNS gateway, see the Introduction to mDNS Gateway chapter.

Configuring mDNS Gateway on Guest Anchor

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**guest-wlan profile-name** *guest-lan-profile-name guest-wlan-id* **Example:** `Device(config)# guest-wlan profile-name g-lanpro 2`	Configures the guest WLAN profile with a wired VLAN.
Step 3	**mdns-sd gateway** **Example:** `Device(config-guest-wlan)# mdns-sd gateway`	Enables mDNS gateway on the guest WLAN.

Configuring mDNS Gateway on Guest Foreign (Guest WLAN)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**guest-wlan profile-name** *guest-lan-profile-name guest-wlan-id* **wired-vlan** *vlan-id* **Example:** `Device(config)# guest-wlan profile-name g-lanpro 2 wired-vlan 230`	Configures guest WLAN profile with a wired VLAN. **Note** Configure the wired VLAN only for the Guest Foreign controller.
Step 3	**mdns-sd gateway** **Example:** `Device(config-guest-wlan)# mdns-sd gateway`	Enables mDNS gateway on the guest WLAN.
Step 4	**exit** **Example:**	Returns to global configuration mode.

	Command or Action	Purpose
	Device(config-wireless-policy)# exit	

Verifying mDNS Gateway Configurations

To verify the mDNS summary, use the following command:

```
Device# show mdns-sd summary
mDNS Gateway: Enabled
Active Query: Enabled
  Periodicity (in minutes): 30
Transport Type: IPv4
```

To verify the mDNS cache, use the following command:

```
Device# show mdns-sd cache
------------------------------------------------------------ PTR Records
----------------------------------------
RECORD-NAME                      TTL      WLAN   CLIENT-MAC       RR-RECORD-DATA

-------------------------------------------------------------------------------------------------------------
_airplay._tcp.local              4500     30     07c5.a4f2.dc01   CUST1._airplay._tcp.local

_ipp._tcp.local                  4500     30     04c5.a4f2.dc01   CUST3._ipp._tcp.local2

_ipp._tcp.local                  4500     15     04c5.a4f2.dc01   CUST3._ipp._tcp.local4

_ipp._tcp.local                  4500     10     04c5.a4f2.dc01   CUST3._ipp._tcp.local6

_veer_custom._tcp.local          4500     10     05c5.a4f2.dc01
CUST2._veer_custom._tcp.local8
```

To verify the mDNS cache from wired service provider, use the following command:

```
Device# show mdns-sd cache wired
------------------------------------------------------------ PTR Records
----------------------------------------
RECORD-NAME                              TTL      VLAN      CLIENT-MAC       RR-RECORD-DATA

-------------------------------------------------------------------------------------------------------------
_airplay._tcp.local                        4500     16        0866.98ec.97af
wiredapple._airplay._tcp.local
_raop._tcp.local                           4500     16        0866.98ec.97af
086698EC97AF@wiredapple._raop._tcp.local

------------------------------------------------------------ SRV Records
----------------------------------------
RECORD-NAME                              TTL      VLAN      CLIENT-MAC       RR-RECORD-DATA

-------------------------------------------------------------------------------------------------------------
wiredapple._airplay._tcp.local             4500     16        0866.98ec.97af   0 0 7000
wiredapple.local
086698EC97AF@wiredapple._raop._tcp.local   4500     16        0866.98ec.97af   0 0 7000
wiredapple.local

------------------------------------------------------------ A/AAAA Records
----------------------------------------
RECORD-NAME                              TTL      VLAN      CLIENT-MAC       RR-RECORD-DATA

-------------------------------------------------------------------------------------------------------------
```

```
wiredapple.local                              4500     16        0866.98ec.97af
2001:8:16:16:e5:c446:3218:7437

------------------------------------------------------------ TXT Records
-----------------------------------------
RECORD-NAME                                TTL      VLAN      CLIENT-MAC       RR-RECORD-DATA

-------------------------------------------------------------------------------------------------------------------
wiredapple._airplay._tcp.local             4500     16        0866.98ec.97af
[343]'acl=0''deviceid=08:66:98:EC:97:AF''features=
086698EC97AF@wiredapple._raop._tcp.local   4500     16        0866.98ec.97af
[193]'cn=0,1,2,3''da=true''et=0,3,5''ft=0x5A7FFFF7
```

To verify the mdns-sd type PTR, use the following command:

```
Device# show mdns-sd cache type {PTR | SRV | A-AAA | TXT}
RECORD-NAME                                   TTL      WLAN      CLIENT-MAC
RR-Record-Data
-------------------------------------------------------------------------------------------------------------------
_custom1._tcp.local                           4500     2         c869.cda8.77d6
service_t1._custom1._tcp.local
_custom1._tcp.local                           4500     2         c869.cda8.77d6
vk11._custom1._tcp.local
_ipp._tcp.local                               4500     2         c869.cda8.77d6
service-4._ipp._tcp.local
```

To verify the mdns-sd cache for a client MAC, use the following command:

```
Device# show mdns-sd cache {ap-mac <ap-mac> | client-mac <client-mac> | wlan-id <wlan-id>
| wired}
RECORD-NAME                                   TTL      WLAN      CLIENT-MAC
RR-Record-Data
-------------------------------------------------------------------------------------------------------------------
_custom1._tcp.local                           4500     2         c869.cda8.77d6
service_t1._custom1._tcp.local
_custom1._tcp.local                           4500     2         c869.cda8.77d6
vk11._custom1._tcp.local
_ipp._tcp.local                               4500     2         c869.cda8.77d6
service-4._ipp._tcp.local

------------------------------------------------------------ SRV Records
-----------------------------------------------------------------
RECORD-NAME                                   TTL      WLAN      CLIENT-MAC
RR-Record-Data
-------------------------------------------------------------------------------------------------------------------
service-4._ipp._tcp.local                    4500     2         c869.cda8.77d6   0 0 1212
 mDNS-Client1s-275.local
vk11._custom1._tcp.local                      4500     2         c869.cda8.77d6   0 0 987
 mDNS-Client1s-275.local
service_t1._custom1._tcp.local                4500     2         c869.cda8.77d6   0 0 197
 mDNS-Client1s-275.local

------------------------------------------------------------ A/AAAA Records
-------------------------------------------------------------
RECORD-NAME                                   TTL      WLAN      CLIENT-MAC
RR-Record-Data
-------------------------------------------------------------------------------------------------------------------
mDNS-Client1s-275.local                      4500     2         c869.cda8.77d6   120.1.1.33


------------------------------------------------------------ TXT Records
-------------------------------------------------------------
RECORD-NAME                                   TTL      WLAN      CLIENT-MAC
RR-Record-Data
-------------------------------------------------------------------------------------------------------------------
```

```
service-4._ipp._tcp.local                       4500     2         c869.cda8.77d6   'CLient1'

vk11._custom1._tcp.local                         4500     2          c869.cda8.77d6
'txtvers=11'
service_t1._custom1._tcp.local                   4500     2          c869.cda8.77d6
'txtvers=12'
```

To verify the mdns-sd cache in detail, use the following command:

```
Device# show mdns-sd cache detail

Name: _custom1._tcp.local
  Type: PTR
  TTL: 4500
  WLAN: 2
  WLAN Name: mdns120
  VLAN: 120
  Client MAC: c869.cda8.77d6
  AP Ethernet MAC: 7069.5ab8.33d0
  Expiry-Time: 09/09/18 21:50:47
  Site-Tag: default-site-tag
  Rdata: service_t1._custom1._tcp.local
```

To verify the mdns-sd statistics, use the following command:

```
Device# show mdns-sd statistics

-----------------------------------------------------
Consolidated mDNS Packet Statistics
-----------------------------------------------------
mDNS stats last reset time: 03/11/19 04:17:35
mDNS packets sent: 61045
  IPv4 sent: 30790
    IPv4 advertisements sent: 234
    IPv4 queries sent: 30556
  IPv6 sent: 30255
    IPv6 advertisements sent: 17
    IPv6 queries sent: 30238
  Multicast sent: 57558
    IPv4 sent: 28938
    IPv6 sent: 28620
mDNS packets received: 72796
  advertisements received: 13604
  queries received: 59192
  IPv4 received: 40600
    IPv4 advertisements received: 6542
    IPv4 queries received: 34058
  IPv6 received: 32196
    IPv6 advertisements received: 7062
    IPv6 queries received: 25134
mDNS packets dropped: 87

-----------------------------------------------------
Wired mDNS Packet Statistics
-----------------------------------------------------
mDNS stats last reset time: 03/11/19 04:17:35
mDNS packets sent: 61033
  IPv4 sent: 30778
    IPv4 advertisements sent: 222
    IPv4 queries sent: 30556
  IPv6 sent: 30255
    IPv6 advertisements sent: 17
    IPv6 queries sent: 30238
  Multicast sent: 57558
    IPv4 sent: 28938
```

```
    IPv6 sent: 28620
mDNS packets received: 52623
  advertisements received: 1247
  queries received: 51376
  IPv4 received: 32276
    IPv4 advertisements received: 727
    IPv4 queries received: 31549
  IPv6 received: 20347
    IPv6 advertisements received: 520
    IPv6 queries received: 19827
mDNS packets dropped: 63

-----------------------------------------------------
mDNS Packet Statistics, for WLAN: 2
-----------------------------------------------------
mDNS stats last reset time: 03/11/19 04:17:35
mDNS packets sent: 12
  IPv4 sent: 12
    IPv4 advertisements sent: 12
    IPv4 queries sent: 0
  IPv6 sent: 0
    IPv6 advertisements sent: 0
    IPv6 queries sent: 0
  Multicast sent: 0
    IPv4 sent: 0
    IPv6 sent: 0
mDNS packets received: 20173
  advertisements received: 12357
  queries received: 7816
  IPv4 received: 8324
    IPv4 advertisements received: 5815
    IPv4 queries received: 2509
  IPv6 received: 11849
    IPv6 advertisements received: 6542
    IPv6 queries received: 5307
mDNS packets dropped: 24
```

To verify the default service list details, use the following command:

```
Device# show mdns-sd default-service-list

-----------------------------------------
        mDNS Default Service List
-----------------------------------------

Service Definition: airplay
Service Names: _airplay._tcp.local

Service Definition: airtunes
Service Names: _raop._tcp.local

Service Definition: homesharing
Service Names: _home-sharing._tcp.local

Service Definition: printer-ipp
Service Names: _ipp._tcp.local

Service Definition: printer-lpd
Service Names: _printer._tcp.local

Service Definition: printer-ipps
Service Names: _ipps._tcp.local

Service Definition: printer-socket
Service Names: _pdl-datastream._tcp.local
```

```
Service Definition: google-chromecast
Service Names: _googlecast._tcp.local

Service Definition: itune-wireless-devicesharing2
Service Names: _apple-mobdev2._tcp.local
```

To verify the primary service list details, use the following command:

```
Device# show mdns-sd master-service-list

-----------------------------------------
        mDNS Master Service List
-----------------------------------------

Service Definition: fax
Service Names: _fax-ipp._tcp.local

Service Definition: roku
Service Names: _rsp._tcp.local

Service Definition: airplay
Service Names: _airplay._tcp.local

Service Definition: scanner
Service Names: _scanner._tcp.local

Service Definition: spotify
Service Names: _spotify-connect._tcp.local

Service Definition: airtunes
Service Names: _raop._tcp.local

Service Definition: airserver
Service Names: _airplay._tcp.local
               _airserver._tcp.local

.
.
.

Service Definition: itune-wireless-devicesharing2
Service Names: _apple-mobdev2._tcp.local
```

To verify the mDNS-AP configured on the controller and VLAN(s) associated with it, use the following command:

```
Device# show mdns-sd ap

Number of mDNS APs.............................. 1

AP Name   Ethernet MAC   Number of Vlans   Vlanidentifiers
-------------------------------------------------------------------------------------------------------
AP3600-1   7069.5ab8.33d0          1      300
```

Further Debug

To debug mDNS further, use the following procedure:

1. Run this command at the controller:

   ```
   set platform software trace wncd <0-7> chassis active R0 mdns debug
   ```

2. Reproduce the issue.

3. Run this command to gather the traces enabled:

```
show wireless loadbalance ap affinity wncd 0

AP MAC   Discovery Timestamp  Join Timestamp               Tag    Vlanidentifiers
-------------------------------------------------------------------------------------
0cd0.f894.0600      06/30/21 12:39:48    06/30/21 12:40:021 default-site-tag     300
```