CONTENTS

PREFACE

Preface  lix
  Document Conventions  lix
  Related Documentation  lxii
  Obtaining Documentation and Submitting a Service Request  lxii

CHAPTER 1

Overview of the Cisco Catalyst 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)  9
  Configuring a Wireless Profile Policy (CLI)  10
  Setting a Flex Profile  11
  Configuring an AP Profile (GUI)  12
  Configuring an AP Profile (CLI)  16
  Configuring an RF Profile (GUI)  17
  Configuring an RF Profile (CLI)  17
  Configuring a Site Tag (GUI)  18
  Configuring a Site Tag (CLI)  19
  Configuring Policy Tag (GUI)  20
  Configuring a Policy Tag (CLI)  20
  Configuring Wireless RF Tag (GUI)  21
CHAPTER 5

Smart Licensing

Information About Cisco Smart Licensing 43
Creating a Smart Account 45
Using Smart Licensing 46
Using Specified License Reservation (SLR) 46
Enabling Specified License Reservation in CSSM 47
Enabling Smart Software Licensing 47
Enabling Smart Call Home Reporting 48
Configuring AIR License Level (GUI) 48
Configuring AIR License Level (CLI) 49
Configuring AIR Network Essentials License Level 49
Configuring AIR Network Advantage License Level 50
Verifying Smart Licensing Configurations 50

CHAPTER 6

Best Practices

Infrastructure 53
Disable Aironet IE 53
Disable Management over Wireless 54
HTTPs for Management 54
Load Balancing 55
NTP 55
Virtual Gateway IP 56
Local Profiling 56
VRF and Routing Protocol 56
Site Tag 56
Security 57
WLAN with WPA2 or 802.1X 57
Client Exclusion 57
User Login Policies 58
RF Management 58
Auto Coverage Hole Detection 58
Auto Dynamic Channel Assignment 59
PART II Lightweight Access Points 69

CHAPTER 7 Country Codes 71

Information About Country Codes 71
Prerequisites for Configuring Country Codes 71
Configuring Country Codes (GUI) 72
How to Configure Country Codes 72
Configuration Examples for Configuring Country Codes 74
Displaying Channel List for Country Codes: Example 74

CHAPTER 8 Sniffer Mode 77

Information about Sniffer 77
Prerequisites for Sniffer 77
Restrictions on Sniffer 77
How to Configure Sniffer 78
Configuring an Access Point as Sniffer (GUI) 78
Configuring an Access Point as Sniffer (CLI) 78
Enabling or Disabling Sniffing on the Access Point (GUI) 79
Enabling or Disabling Sniffing on the Access Point (CLI) 79
Verifying Sniffer Configurations 80
Examples for Sniffer Configurations and Monitoring 80

CHAPTER 9
Monitor Mode 81
Introduction to Monitor Mode 81
Enable Monitor Mode (GUI) 81
Enable Monitor Mode (CLI) 82

CHAPTER 10
Sensor Mode 83
Introduction to Sensor Mode 83
Enabling Sensor Mode 83
Verifying Sensor Mode Configuration 87

CHAPTER 11
AP Priority 89
Failover Priority for Access Points 89
Setting AP Priority 89

CHAPTER 12
FlexConnect 91
Information About FlexConnect 91
FlexConnect Authentication Process 93
Restrictions for FlexConnect 96
Configuring a Site Tag 98
Configuring a Policy Tag (CLI) 99
Attaching a Policy Tag and a Site Tag to an AP (GUI) 99
Attaching Policy Tag and Site Tag to an AP (CLI) 100
Applying ACLs on FlexConnect 101
Configuring FlexConnect 102
Configuring a Switch at a Remote Site 102
Configuring the Controller for FlexConnect 103
Configuring Local Switching in FlexConnect Mode (GUI) 103
Configuring Local Switching in FlexConnect Mode (CLI) 104
Example: Displaying Access Point Crash File Information 141

AP MAC Authorization 142
  Configuring AP MAC Authorization (CLI) 142

Ethernet VLAN Tagging on Access Points 143
  Information About Ethernet VLAN Tagging on Access Points 143
  Configuring Ethernet VLAN Tagging on Access Points (GUI) 143
  Configuring Ethernet VLAN Tagging on Access Points (CLI) 143

CHAPTER 15  
AP Crash File Upload 145
  AP Crash File Upload 145
  Configuring AP Crash File Upload (CLI) 147

CHAPTER 16  
Rogue per AP 149
  Rogue per AP 149
  Enabling Rogue Detection 150
    Configuring an AP Profile (GUI) 150
    Configure an AP Profile 154
    Define a Wireless Site Tag and Assign an AP Profile (GUI) 156
    Define a Wireless Site Tag and Assign an AP Profile (CLI) 156
    Associating Wireless Tag to an AP (GUI) 156
    Associate Wireless Tag to an AP (CLI) 157
  Rogue Detection Security Level 157
  Setting Rogue Detection Security-level 159
  Wireless Service Assurance Rogue Events 159
    Monitoring Wireless Service Assurance Rogue Events 160

CHAPTER 17  
Access Point Plug-n-Play 163
  Overview of Access Point Plug-n-Play 163
  Provisioning AP from PnP Server 163
  Verifying AP Tag Configuration 164

CHAPTER 18  
802.11 Parameters for Cisco Access Points 165
  2.4-GHz Radio Support 165
    Configuring 2.4-GHz Radio Support for the Specified Slot Number 165
5-GHz Radio Support 167
  Configuring 5-GHz Radio Support for the Specified Slot Number 167
Information About Dual-Band Radio Support 169
Configuring Default XOR Radio Support 169
Configuring XOR Radio Support for the Specified Slot Number (GUI) 171
Configuring XOR Radio Support for the Specified Slot Number 172
Receiver Only Dual-Band Radio Support 173
  Information About Receiver Only Dual-Band Radio Support 173
Configuring Receiver Only Dual-Band Parameters for Access Points 174
  Enabling CleanAir with Receiver Only Dual-Band Radio on a Cisco Access Point 174
  Disabling Receiver Only Dual-Band Radio on a Cisco Access Point 174
Configuring Client Steering (CLI) 174
Verifying Cisco Access Points with Dual-Band Radios 176

CHAPTER 19  802.1x Support 177
  Introduction to the 802.1x Authentication 177
    EAP-FAST Protocol 177
    EAP-TLS/EAP-PEAP Protocol 178
  Limitations of the 802.1x Authentication 178
  Topology - Overview 178
Configuring 802.1x Authentication Type and LSC AP Authentication Type (GUI) 179
Configuring 802.1x Authentication Type and LSC AP Authentication Type 179
  Configuring the 802.1x Username and Password (GUI) 180
  Configuring the 802.1x Username and Password (CLI) 181
Enabling 802.1x on the Switch Port 182
Verifying 802.1x on the Switch Port 183
Verifying the Authentication Type 184

CHAPTER 20  Configuring CAPWAP Link Aggregation Support 185
  Information About Link Aggregation 185
  Information About CAPWAP LAG Support 185
  Restrictions for CAPWAP LAG Support 186
Enabling CAPWAP LAG Support on Controller 186
Enabling CAPWAP LAG Globally on Controller 186
Disabling CAPWAP LAG Globally on Controller 187
Enabling CAPWAP LAG for an AP Profile 187
Disabling CAPWAP LAG for an AP Profile 188
Disabling CAPWAP LAG Support on Controller 188
Verifying CAPWAP LAG Support Configurations 189

CHAPTER 21

Configuring DHCP and NAT Functionality on Root Access Point 191
Information About DHCP and NAT Functionality on Root AP (RAP) 191
Configuring DHCP Server on Root Access Point (RAP) 192
Verifying DHCP Server for Root AP Configuration 192

CHAPTER 22

OFDMA Support for 11ax Access Points 193
Information About OFDMA Support for 11ax Access Points 193
Supported Modes on 11ax Access Points 193
Configuring 11AX (GUI) 194
Configuring Channel Width 194
Configuring 802.11ax Radio Parameters (CLI) 195
Setting up the 802.11ax Radio Parameters 195
Configuring OFDMA on a WLAN 196
Verifying Channel Width 197
Verifying Client Details 198
Verifying Radio Configuration 199

PART III

Radio Resource Management 203

CHAPTER 23

Radio Resource Management 205
Information About Radio Resource Management 205
Radio Resource Monitoring 206
Information About RF Groups 206
RF Group Leader 207
RF Group Name 208
Rogue Access Point Detection in RF Groups 208
Transmit Power Control 209
Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings 209
Contents

Dynamic Channel Assignment 209
Dynamic Bandwidth Selection 211
Coverage Hole Detection and Correction 211
Restrictions for Radio Resource Management 212
How to Configure RRM 212
Configuring Neighbor Discovery Type (GUI) 212
Configuring Neighbor Discovery Type (CLI) 212
Configuring RF Groups 213
  Configuring RF Group Selection Mode (GUI) 213
  Configuring RF Group Selection Mode (CLI) 214
  Configuring an RF Group Name (CLI) 214
  Configuring Members in an 802.11 Static RF Group (GUI) 215
  Configuring Members in an 802.11 Static RF Group (CLI) 215
Configuring Transmit Power Control 216
  Configuring Transmit Power (GUI) 216
  Configuring the Tx-Power Control Threshold (CLI) 216
  Configuring the Tx-Power Level (CLI) 217
Configuring 802.11 RRM Parameters 218
  Configuring Advanced 802.11 Channel Assignment Parameters (GUI) 218
  Configuring Advanced 802.11 Channel Assignment Parameters (CLI) 219
  Configuring 802.11 Coverage Hole Detection (GUI) 221
  Configuring 802.11 Coverage Hole Detection (CLI) 222
  Configuring 802.11 Event Logging (CLI) 223
  Configuring 802.11 Statistics Monitoring (GUI) 224
  Configuring 802.11 Statistics Monitoring (CLI) 224
  Configuring the 802.11 Performance Profile (GUI) 225
  Configuring the 802.11 Performance Profile (CLI) 226
Configuring Advanced 802.11 RRM 227
  Enabling Channel Assignment (GUI) 227
  Enabling Channel Assignment (CLI) 227
Restarting DCA Operation 228
  Updating Power Assignment Parameters (GUI) 228
  Updating Power Assignment Parameters (CLI) 228
Configuring Rogue Access Point Detection in RF Groups 229
Configuring Rogue Access Point Detection in RF Groups (CLI)  229  
Monitoring RRM Parameters and RF Group Status  230  
  Monitoring RRM Parameters  230  
  Verifying RF Group Status (CLI)  231  
Examples: RF Group Configuration  231  
Information About ED-RRM  231  
  Configuring ED-RRM on the Cisco Wireless LAN Controller (CLI)  232  

CHAPTER 24  
Coverage Hole Detection  235  
  Coverage Hole Detection and Correction  235  
  Configuring Coverage Hole Detection (GUI)  235  
  Configuring Coverage Hole Detection (CLI)  236  
  Configuring CHD for RF Tag Profile (GUI)  237  
  Configuring CHD for RF Tag Profile (CLI)  238  

CHAPTER 25  
Optimized Roaming  241  
  Optimized Roaming  241  
  Restrictions for Optimized Roaming  241  
  Configuring Optimized Roaming (GUI)  242  
  Configuring Optimized Roaming (CLI)  242  

CHAPTER 26  
Cisco Flexible Radio Assignment  245  
  Information About Flexible Radio Assignment  245  
    Benefits of the FRA Feature  246  
    Configuring an FRA Radio (CLI)  246  
    Configuring an FRA Radio (GUI)  248  

CHAPTER 27  
XOR Radio Support  249  
  Information About Dual-Band Radio Support  249  
  Configuring Default XOR Radio Support  249  
  Configuring XOR Radio Support for the Specified Slot Number (GUI)  252  
  Configuring XOR Radio Support for the Specified Slot Number  252  

CHAPTER 28  
Cisco Receiver Start of Packet  255
<table>
<thead>
<tr>
<th>Chapter 29</th>
<th>Client Limit</th>
<th>257</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information About Client Limit</td>
<td>257</td>
<td></td>
</tr>
<tr>
<td>Configuring Client Limit (CLI)</td>
<td>257</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 30</th>
<th>IP Theft</th>
<th>259</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to IP Theft</td>
<td>259</td>
<td></td>
</tr>
<tr>
<td>Configuring IP Theft</td>
<td>260</td>
<td></td>
</tr>
<tr>
<td>Configuring the IP Theft Exclusion Timer</td>
<td>260</td>
<td></td>
</tr>
<tr>
<td>Adding Static Entries for Wired Hosts</td>
<td>260</td>
<td></td>
</tr>
<tr>
<td>Verifying IP Theft Configuration</td>
<td>261</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 31</th>
<th>Unscheduled Automatic Power Save Delivery</th>
<th>263</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information About Unscheduled Automatic Power Save Delivery</td>
<td>263</td>
<td></td>
</tr>
<tr>
<td>Configuring Unscheduled Automatic Power Save Delivery (CLI)</td>
<td>263</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 32</th>
<th>USB Power Support</th>
<th>265</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring an AP Profile</td>
<td>265</td>
<td></td>
</tr>
<tr>
<td>Enabling or Disabling USB for a Cisco AP Profile</td>
<td>265</td>
<td></td>
</tr>
<tr>
<td>Enabling or disabling USB Port to Override for Each Access Point</td>
<td>266</td>
<td></td>
</tr>
<tr>
<td>Enabling or disabling USB Port on an Access Point</td>
<td>266</td>
<td></td>
</tr>
<tr>
<td>Verifying USB for Cisco Access Point Configurations</td>
<td>267</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 33</th>
<th>Dynamic Frequency Selection</th>
<th>269</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information About Dynamic Frequency Selection</td>
<td>269</td>
<td></td>
</tr>
<tr>
<td>Configuring Dynamic Frequency Selection</td>
<td>269</td>
<td></td>
</tr>
<tr>
<td>Verifying DFS</td>
<td>270</td>
<td></td>
</tr>
</tbody>
</table>

| Part IV | Network Management | 271 |
Contents

CHAPTER 34  AP Packet Capture  273
  Introduction to AP Client Packet Capture  273
  Enabling Packet Capture (GUI)  273
  Enabling Packet Capture (CLI)  274
  Create AP Packet Capture Profile and Map to an AP Join Profile (GUI)  274
  Create AP Packet Capture Profile and Map to an AP Join Profile  274
  Start or Stop Packet Capture  275

CHAPTER 35  DHCP Option82  277
  Information About DHCP Option 82  277
  Configuring DHCP Option 82 Global Interface  278
    Configuring Globally Through Server Override (CLI)  278
    Configuring Globally Through Different SVIs (GUI)  278
    Configuring Globally Through Different SVIs (CLI)  279
  Configuring DHCP Option 82 Through Profile Policy  279
    Configuring DHCP Option 82 with the ap_ethmac Command (CLI)  279
    Configuring DHCP Option 82 with the ap_location Command (CLI)  281
    Configuring DHCP Option 82 with the apmac Command (CLI)  282
    Configuring DHCP Option 82 with the apname Command (CLI)  284
    Configuring DHCP Option 82 with a Policy Tag Command (CLI)  285
    Configuring DHCP Option 82 with the SSID Command (CLI)  287
    Configuring DHCP Option 82 with ap_ethmac and SSID Commands (CLI)  288
    Configuring DHCP Option 82 with the ap_mac and vlan_id Commands (CLI)  290
    Configuring DHCP Option 82 with the ap_name Command and a VLAN ID (CLI)  291
    Configuring DHCP Option 82 with the ap_ethmac Command and server override enabled (CLI)  293
  Configuring DHCP Option82 Through a VLAN Interface  294
    Configuring DHCP Option 82 Through Option-Insert Command (CLI)  294
    Configuring DHCP Option 82 Through the server-ID-override Command (CLI)  295
    Configuring DHCP Option 82 Through a Subscriber-ID (CLI)  296
    Configuring DHCP Option 82 Through server-ID-overide and subscriber-ID Commands (CLI)  297
    Configuring DHCP Option 82 Through Different SVIs (CLI)  298
CHAPTER 36  RADIUS Realm  301
  Information About RADIUS Realm  301
  Enabling RADIUS Realm  302
  Configuring Realm to Match the RADIUS Server for Authentication and Accounting  302
  Configuring the AAA Policy for a WLAN  303
  Verifying the RADIUS-Realm Configuration  305

CHAPTER 37  Introduction to Accounting of AP Events  309
  Configuring Accounting Method-List for an AP Profile  309
  Verifying the AP Accounting Information  310

CHAPTER 38  Cisco StadiumVision  311
  Cisco StadiumVision Overview  311
  Configure Wireless Controller Parameters for Cisco StadiumVision (GUI)  312
  Configure Wireless Controller Parameters for Cisco StadiumVision (CLI)  312
  Verify StadiumVision Configurations  313

CHAPTER 39  Persistent SSID Broadcast  315
  Persistent SSID Broadcast  315
  Configuring Persistent SSID Broadcast  315
  Verifying Persistent SSID Broadcast  316

CHAPTER 40  Network Monitoring  317
  Network Monitoring  317
  Status Information Received Synchronously - Configuration Examples  317
  Alarm and Event Information Received Asynchronously - Configuration Examples  319

CHAPTER 41  Creating a Lobby Ambassador Account  321
  Information About Lobby Ambassador Account  321
  Creating a Lobby Ambassador Account (GUI)  321
  Creating a User Account  322
  Logging In Using the Lobby Account  322
### Creating a Lobby Ambassador Account (CLI) 322

#### CHAPTER 42 Configuring Guest User Accounts 325

Information About Creating Guest User Accounts 325  
Creating a Guest User Account (GUI) 325  
Creating a Guest User Account (CLI) 326  
Verifying Guest User Account 327

#### PART V System Management 329

#### CHAPTER 43 Network Mobility Services Protocol 331

Information About Network Mobility Services Protocol 331  
Radioactive Tracing for NMSP 332  
Enabling NMSP on Premises Services 332  
Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues 333  
Modifying the NMSP Notification Threshold for Clients, RFID Tags, and Rogues 333  
Configuring NMSP Strong Cipher 334  
Verifying NMSP Settings 334  
Examples: NMSP Settings Configuration 336  
NMSP by AP Groups with Subscription List from CMX 337  
Verifying NMSP by AP Groups with Subscription List from CMX 337  
Probe RSSI Location 339  
Configuring Probe RSSI 339  
RFID Tag Support 340  
Configuring RFID Tag Support 341  
Verifying RFID Tag Support 341

#### CHAPTER 44 Application Visibility and Control 345

Information About Application Visibility and Control 345  
Prerequisites for Application Visibility and Control 347  
Restrictions for Application Visibility and Control 347  
AVC Configuration Overview 347  
Create a Flow Monitor 348  
Create a Flow Record 349
Contents

CHAPTER 45
Cisco Hyperlocation 367
  Information About Cisco Hyperlocation 367
  Restrictions on Cisco Hyperlocation 369
  Support for IPv6 in Cisco Hyperlocation or BLE Configuration 370
  Configuring Cisco Hyperlocation (GUI) 370
  Configuring Cisco Hyperlocation (CLI) 371
  Verifying Cisco Hyperlocation 372
  Configuring Hyperlocation BLE Beacon Parameters for AP (GUI) 375
  Configuring Hyperlocation BLE Beacon Parameters (CLI) 375
  Verifying Hyperlocation BLE Beacon Configuration 376
  Configuring Hyperlocation BLE Beacon Parameters for AP (CLI) 376
  Verifying Hyperlocation BLE Beacon Configuration for AP 377

CHAPTER 46
FastLocate for Cisco Catalyst Series Access Points 379
  Information About FastLocate 379
CHAPTER 47
BLE Beacons in CiscoWave 2 Access Points 383
Managing BLE Beacons in Cisco Wave 2 and 802.11ax Access Points 383
Monitoring BLE Management 385

CHAPTER 48
Cisco DNA Spaces 389
Configuring Cisco DNA Spaces 389
Verifying Cisco DNA Spaces Configuration 390

CHAPTER 49
EDCA Parameters 393
Enhanced Distributed Channel Access Parameters 393
Configuring EDCA Parameters (GUI) 393
Configuring EDCA Parameters (CLI) 394

CHAPTER 50
802.11 parameters and Band Selection 397
Restrictions for Band Selection, 802.11 Bands, and Parameters 397
Information About Configuring Band Selection, 802.11 Bands, and Parameters 398
Band Selection 398
802.11 Bands 399
802.11n Parameters 399
802.11h Parameters 399
How to Configure 802.11 Bands and Parameters 400
Configuring Band Selection (GUI) 400
Configuring Band Selection (CLI) 400
Configuring the 802.11 Bands (GUI) 402
Configuring the 802.11 Bands (CLI) 402
Configuring a Band-Select RF Profile (GUI) 405
Configuring a Band-Select RF Profile (CLI) 405
Configuring 802.11n Parameters (GUI) 406
Configuring 802.11n Parameters (CLI) 406
Configuring 802.11h Parameters (CLI)  409

Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters  409

Verifying Configuration Settings Using Band Selection and 802.11 Bands Commands  409

Example: Viewing the Configuration Settings for the 5-GHz Band  410

Example: Viewing the Configuration Settings for the 24-GHz Band  410

Example: Viewing the status of 802.11h Parameters  413

Example: Verifying the Band-Selection Settings  413

Configuration Examples for Band Selection, 802.11 Bands, and Parameters  415

Examples: Band Selection Configuration  415

Examples: 802.11 Bands Configuration  416

Examples: 802.11n Configuration  416

Examples: 802.11h Configuration  417

---

CHAPTER 51

Predownloading an Image to an Access Point  419

Information About Predownloading an Image to an Access Point  419

Restrictions for Predownloading an Image to an Access Point  419

How to Predownload an Image to an Access Point  420

Predownloading an Image to Access Points (CLI)  420

Monitoring the Access Point Predownload Process  421

---

CHAPTER 52

Efficient Image Upgrade  423

Efficient Image Upgrade  423

Enable Pre-Download (GUI)  423

Enable Pre-Download (CLI)  424

Configuring a Site Tag (CLI)  424

Attaching Policy Tag and Site Tag to an AP (CLI)  425

Trigger Predownload to a Site Tag  426

---

CHAPTER 53

Hitless Upgrade  429

N+1 Hitless Rolling AP Upgrade  429

Configuring Hitless Upgrade  430

Verifying Hitless Upgrade  431

---

CHAPTER 54

Wireless Sub-Package for Switch  433
IPv6 Multicast-over-Multicast 474
Configuring IPv6 Multicast-over-Multicast 475
Verifying IPv6 Multicast-over-Multicast 475

Directed Multicast Service 476
Directed Multicast Service 476
Configuring Directed Multicast Service (GUI) 476
Configuring Directed Multicast Service 476
Verifying the Directed Multicast Service Configuration 477

Wireless Broadcast, Non-IP Multicast and Multicast VLAN 478
Configuring Non-IP Wireless Multicast 478
Configuring Wireless Broadcast (GUI) 479
Configuring Wireless Broadcast 480
Configuring Multicast-over-Multicast for All the AP Multicast Groups (CLI) 481
Verifying Wireless Multicast 481
Multicast Optimization 482
Configuring IP Multicast VLAN for WLAN 482
Verifying the Multicast VLAN Configuration 483

CHAPTER 61

Map-Server Per-Site Support 485
Information About Map Server Per Site Support 485
Configuring the Default Map Server (GUI) 486
Configuring the Default Map Server (CLI) 486
Configuring a Map Server Per Site (GUI) 487
Configuring a Map Server Per Site (CLI) 487
Creating a Map Server for Each VNID (GUI) 488
Creating a Map Server for Each VNID 488
Creating a Fabric Profile and Associating a Tag and VNID (GUI) 489
Creating a Fabric Profile and Associating a Tag and VNID (CLI) 489
Verifying the Map Server Configuration 490

CHAPTER 62

Volume Metering 493
Configuring Volume Metering 493

CHAPTER 63

Enabling Syslog Messages in Access Points and Controller for Syslog Server 495
Contents

Configuring ISE for Central Web Authentication 569
  Creating Authorization Profiles 569
  Mapping Authorization Profiles to Authentication Rule 569
  Mapping Authorization Profiles to Authorization Rule 570
Viewing DNS-Based Access Control Lists 570
Configuration Examples for DNS-Based Access Control Lists 571
Verifying DNS Snoop Agent (DSA) 572
Information About Flex Client IPv6 Support with WebAuth Pre and Post ACL 573
Enabling Pre-Authentication ACL for LWA and EWA 574
Enabling Post-Authentication ACL for LWA and EWA 576
Enabling DNS ACL for LWA and EWA 576
Verifying Flex Client IPv6 Support with WebAuth Pre and Post ACL 577

CHAPTER 70

Whitelisting of Specific URLs 579
  Whitelisting of Specific URLs 579
  Configuring URL Whitelisting 579
  Verifying URL Whitelisting on the Controller 580

CHAPTER 71

Configuring Policy Enforcement and Usage Monitoring 581
  Policy Enforcement and Usage Monitoring 581
  Configuring Policy Enforcement and Usage Monitoring (CLI) 581
  Example: Configuring Policy Enforcement and Usage Monitoring 582
  Verifying Policy Usage and Enforcement 583

CHAPTER 72

Web-Based Authentication 585
  Local Web Authentication Overview 585
    Device Roles 586
    Authentication Process 587
    Local Web Authentication Banner 587
    Customized Local Web Authentication 590
      Guidelines 590
      Redirection URL for Successful Login Guidelines 591
  How to Configure Local Web Authentication 591
    Configuring Default Local Web Authentication 591
Information About Central Web Authentication 613
Prerequisites for Central Web Authentication 613
How to Configure ISE 613
Creating an Authorization Profile 614
Creating an Authentication Rule 614
Creating an Authorization Rule 615
How to Configure Central Web Authentication on a Network Device 616
Configuring WLAN (GUI) 616
Configuring WLAN (CLI) 617
Configuring Policy Profile (CLI) 618
Configuring a Policy Profile (GUI) 619
Creating Redirect ACL 620
Configuring AAA for Central Web Authentication 621
Configuring Redirect ACL in Flex Profile (GUI) 621
Configuring Redirect ACL in Flex Profile (CLI) 622
Authentication for Sleeping Clients 623
Information About Authenticating Sleeping Clients 623
Restrictions on Authenticating Sleeping Clients 623
Configuring Authentication for Sleeping Clients (GUI) 624
Configuring Authentication for Sleeping Clients (CLI) 624
Sleeping Clients with Multiple Authentications 625
Mobility Support for Sleeping Clients 625
Supported Combinations of Multiple Authentications 625
Configuring Sleeping Clients with Multiple Authentications 626
Configuring WLAN for Dot1x and Local Web Authentication 626
Configuring WLAN for MAC Authentication Bypass and Local Web Authentication 627
Configuring WLAN for Local Web Authentication and MAC Filtering 628
Configuring a PSK + LWA in a WLAN 629
Configuring Sleeping Clients 630
Verifying Sleeping Clients Configuration 631

ISE Simplification and Enhancements 633
Utilities for Configuring Security 633
Configuring Multiple Radius Servers 634
Verifying AAA and Radius Server Configurations 634
Configuring Captive Portal Bypassing for Local and Central Web Authentication 635
  Information About Captive Bypassing 635
  Configuring Captive Bypassing for WLAN in LWA and CWA (GUI) 636
  Configuring Captive Bypassing for WLAN in LWA and CWA (CLI) 636
Sending DHCP Options 55 and 77 to ISE 637
  Information about DHCP Option 55 and 77 637
  Configuration to Send DHCP Options 55 and 77 to ISE (GUI) 638
  Configuration to Send DHCP Options 55 and 77 to ISE (CLI) 638
  Configuring EAP Request Timeout (GUI) 639
  Configuring EAP Request Timeout 639
Captive Portal 640
  Captive Portal Configuration 640
  Configuring Captive Portal 640
  Captive Portal Configuration - Example 643

CHAPTER 75 Authentication and Authorization Between Multiple RADIUS Servers 645
  Information About Authentication and Authorization Between Multiple RADIUS Servers 645
  Configuring 802.1X Security for WLAN with Split Authentication and Authorization Servers 646
    Configuring Explicit Authentication and Authorization Server List (GUI) 646
    Configuring Explicit Authentication Server List (CLI) 647
    Configuring Explicit Authorization Server List (CLI) 648
    Configuring Authentication and Authorization List for 802.1X Security 649
  Configuring Web Authentication for WLAN with Split Authentication and Authorization Servers 650
    Configuring Authentication and Authorization List for Web Authentication 650
  Verifying Split Authentication and Authorization Configuration 651
  Configuration Examples 652

CHAPTER 76 Secure LDAP (SLDAP) 653
  Information About SLDAP 653
  Prerequisite for Configuring SLDAP 655
  Restrictions for Configuring SLDAP 655
  Configuring SLDAP 655
  Configuring an AAA Server Group (GUI) 656
Contents

Configuring a AAA Server Group  657
Configuring Search and Bind Operations for an Authentication Request  658
Configuring a Dynamic Attribute Map on an LDAP Server  659
Verifying the LDAP Configuration  659

CHAPTER 77

RADIUS DTLS  661
Information About RADIUS DTLS  661
Prerequisites  663
Configuring RADIUS DTLS Server  663
  Configuring RADIUS DTLS Connection Timeout  664
  Configuring RADIUS DTLS Idle Timeout  664
  Configuring Source Interface for RADIUS DTLS Server  665
  Configuring RADIUS DTLS Port Number  666
  Configuring RADIUS DTLS Connection Retries  666
  Configuring RADIUS DTLS Trustpoint  667
Configuring DTLS Dynamic Author  668
Enabling DTLS for Client  668
  Configuring Client Trustpoint for DTLS  669
  Configuring DTLS Idle Timeout  670
  Configuring Server Trustpoint for DTLS  670
Verifying the RADIUS DTLS Server Configuration  671
Clearing RADIUS DTLS Specific Statistics  671

CHAPTER 78

MAC Authentication Bypass  673
MAC Authentication Bypass  673
  MAB Configuration Guidelines  673
Configuring 802.11 Security for WLAN (GUI)  674
Configuring 802.11 Security for WLAN (CLI)  675
Configuring AAA for External Authentication  676
Configuring AAA for Local Authentication (GUI)  677
Configuring AAA for Local Authentication (CLI)  678
Configuring MAB for Local Authentication  679
Configuring MAB for External Authentication (GUI)  680
Configuring MAB for External Authentication (CLI)  680
CHAPTER 79  IP Source Guard  683
  Information About IP Source Guard  683
  Configuring IP Source Guard  683

CHAPTER 80  Managing Rogue Devices  685
  Rogue Devices  685
    How to Configure Rogue Location Discovery Protocol (RLDP)  688
      Configuring an RLDP for Generating Alarms (GUI)  688
      Configuring an RLDP for Generating Alarms (CLI)  689
      Configuring an RLDP for Auto-Contain (GUI)  690
      Configuring an RLDP for Auto-Contain (CLI)  690
      Configuring a Schedule for RLDP (GUI)  690
      Configuring a Schedule for RLDP (CLI)  691
      Configuring RLDP Retry Times on Rogue Access Points (GUI)  692
      Configuring RLDP Retry Times on Rogue Access Points (CLI)  692
    How to Configure Rogue Detection  692
      Configuring Rogue Detection (CLI)  692
    Verifying Rogue Detection  694
  Examples: Rogue Detection Configuration  695

CHAPTER 81  Classifying Rogue Access Points  697
  Information About Classifying Rogue Access Points  697
  Guidelines and Restrictions for Classifying Rogue Access Points  699
  How to Classify Rogue Access Points  699
    Classifying Rogue Access Points and Clients Manually (GUI)  699
    Classifying Rogue Access Points and Clients Manually (CLI)  699
    Configuring Rogue Classification Rules (GUI)  701
    Configuring Rogue Classification Rules (CLI)  702
  Monitoring Rogue Classification Rules  704
  Examples: Classifying Rogue Access Points  704

CHAPTER 82  Configuring Secure Shell  707
  Information About Configuring Secure Shell  707
## Contents

**SSH and Device Access** 707  
**SSH Servers, Integrated Clients, and Supported Versions** 707  
**SSH Configuration Guidelines** 708  
**Secure Copy Protocol Overview** 708  
**Secure Copy Protocol** 709  
**SFTP Support** 709  
**Prerequisites for Configuring Secure Shell** 709  
**Restrictions for Configuring Secure Shell** 710  
**How to Configure SSH** 710  
  - Setting Up the Device to Run SSH 710  
  - Configuring the SSH Server 712  
**Monitoring the SSH Configuration and Status** 714

---

### Chapter 83

**Private PSK** 715  
- Information About Private Preshared Key 715  
- Configuring a PSK in a WLAN (CLI) 716  
- Configuring a PSK in a WLAN (GUI) 717  
- Applying a Policy Profile to a WLAN (GUI) 717  
- Applying a Policy Profile to a WLAN (CLI) 718  
- Verifying a Private PSK 718

---

### Chapter 84

**Multi-Preshared Key** 723  
- Information About Multi-Preshared Key 723  
- Restrictions on Multi-PSK 724  
- Configuring Multi-Preshared Key (GUI) 724  
- Configuring Multi-Preshared Key (CLI) 726  
- Verifying Multi-PSK Configurations 727

---

### Chapter 85

**Multiple Authentications for a Client** 731  
- Information About Multiple Authentications for a Client 731  
- Information About Supported Combination of Authentications for a Given Client 731  
- Configuring Multiple Authentication for a Client 732  
  - Configuring WLAN for 802.1X and Local Web Authentication 732  
  - Configuring WLAN for Preshared Key (PSK) and Local Web Authentication 733
Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication 734

Configuring WLAN 734
Applying Policy Profile to a WLAN 735

Verifying Multiple Authentication Configurations 736

CHAPTER 86 Configuring Cisco TrustSec 739
Information about Cisco TrustSec 739
Cisco TrustSec Features 740
Security Group Access Control List 742
Inline Tagging 743
Policy Enforcement 744
Enabling SGACL on the AP 744
Configuring SGACL, Inline Tagging, and SGT in Local Mode 746
Configuring ISE for TrustSec 746
Verifying Cisco TrustSec Configuration 748

CHAPTER 87 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 88 Locally Significant Certificates 757
Information About Locally Significant Certificates (LSC) 757
Certificate Provisioning on Controllers 758
Device Certificate Enrollment Operation 758
Certificate Provisioning on Lightweight Access Point 758
Provisioning Locally Significant Certificates 759
Configuring RSA Key for PKI Trustpoint 759
Configuring PKI TrustPoint Parameters 760
Authenticating and Enrolling the PKI TrustPoint with CA Server (GUI) 761
Guidelines and Restrictions for FIPS  784
FIPS Self-Tests  784
Configuring FIPS  784
Verifying FIPS Configuration  785

CHAPTER 91  Device Ecosystem  787
Device Analytics  787
  Information About Device Analytics  787
  Restrictions for Device Analytics  787
  Configuring Device Analytics (GUI)  787
  Configuring Device Analytics (CLI)  788
  Verifying Multiple Device Analytics Configurations  789
Adaptive 802.11r  790
  Information About Adaptive 802.11r  790
  Configuring Adaptive 802.11r (GUI)  790
  Verifying Adaptive 802.11r  790

CHAPTER 92  Adaptive WIPS  793
  Information About Adaptive WIPS  793
  aWIPS in a Cisco Catalyst Wireless Controller environment  793
  Supported Modes and Platforms  794
  Prerequisites for Adaptive WIPS  794
  Configuring Adaptive WIPS (GUI)  795
  Viewing Adaptive WIPS Alarms (GUI)  795
  Enabling Adaptive WIPS  795
  Verifying Adaptive WIPS  796

CHAPTER 93  Wi-Fi Protected Access 3  797
  Simultaneous Authentication of Equals  797
  Opportunistic Wireless Encryption  797
  Configuring WPA3 SAE  798
  Configuring SAE (WPA3+WPA2 Mixed Mode)  799
  Configuring WPA3 Enterprise  801
  Configuring the WPA3 OWE  802
Information About High Availability 841
Prerequisites for High Availability 843
Restrictions on High Availability 844
Configuring Boot Variables Manually on the Controller 845
Configuring High Availability (GUI) 845
Configuring High Availability 846
Verifying High Availability Configurations 847
Verifying AP or Client SSO Statistics 848
Verifying High Availability 850
Deleting High Availability 850
Configuring SNMP in High Availability 851
  Prerequisites 851
  Configuring SNMP in High Availability 852
    ENTITY-MIB 852
    ENTITY-STATE-MIB 852

CHAPTER 98

Redundancy Management Interface (RMI) 855
  Information About Redundancy Management Interface (RMI) 855
  Prerequisite for RMI 857
  Configuring Redundancy Management Interface (GUI) 858
  Configuring a Redundancy Management Interface IP Address (CLI) 858
  Configuring Gateway Monitoring (CLI) 860
  Verifying the Gateway-Monitoring Configuration 860
  Verifying the Redundancy Management Interface Configuration 861

PART IX

Quality of Service 863

CHAPTER 99

Quality of Service 865
  Information about Wireless QoS 865
    Wireless QoS Overview 865
    Wireless QoS Targets 865
    SSID Policies 865
    Client Policies 866
    Supported QoS Features on Wireless Targets 866
Creating a Parameter Map  889
Creating a Policy Map (GUI)  889
Creating a Policy Map (CLI)  890
Configuring Native Profiling in Local Mode  892
Verifying Native Profile Configuration  895

CHAPTER 102  Air Time Fairness  897
Information About Air Time Fairness  897
Restrictions on Cisco Air Time Fairness  899
Cisco Air Time Fairness (ATF) Use Cases  899
Configuring Cisco Air Time Fairness (ATF)  900
Creating Cisco ATF Policy  900
Attaching Cisco ATF Policy to a Policy Profile in an AP (GUI)  901
Attaching Cisco ATF Policy to a Policy Profile in an AP  901
Enabling ATF in RF Profile Associated to an AP  902
Verifying Cisco ATF Configurations  902
Verifying Cisco ATF Statistics  903

PART X  IPv6  905

CHAPTER 103  IPv6 Client IP Address Learning  907
Information About IPv6 Client Address Learning  907
SLAAC Address Assignment  908
Stateful DHCPv6 Address Assignment  909
Static IP Address Assignment  909
Router Solicitation  909
Router Advertisement  909
Neighbor Discovery  910
Neighbor Discovery Suppression  910
RA Guard  910
RA Throttling  910
Prerequisites for IPv6 Client Address Learning  910
Configuring RA Throttle Policy (CLI)  911
Applying RA Throttle Policy on VLAN (GUI)  911
CHAPTER 104

Configuring IPv6 ACL 923

Information About IPv6 ACL 923

Understanding IPv6 ACLs 923

Types of ACL 923

Per User IPv6 ACL 923

Filter ID IPv6 ACL 924

Downloadable IPv6 ACL 924

Prerequisites for Configuring IPv6 ACL 924

Restrictions for Configuring IPv6 ACL 924

Configuring IPv6 ACLs 925

Default IPv6 ACL Configuration 925

Interaction with Other Features and Switches 925

How To Configure an IPv6 ACL 926

Creating an IPv6 ACL 926

Creating WLAN IPv6 ACL 929

Verifying IPv6 ACL 930

Displaying IPv6 ACLs 930

Configuration Examples for IPv6 ACL 930

Example: Creating an IPv6 ACL 930
Example: Applying an IPv6 ACL to a Policy Profile in a Wireless Environment 931
Example: Displaying IPv6 ACLs 931
Example: Configuring RA Throttling 932

CHAPTER 105 IPv6 Client Mobility 935
Information About IPv6 Client Mobility 935
Using Router Advertisement 936
RA Throttling 936
IPv6 Address Learning 937
Handling Multiple IP Addresses 937
IPv6 Configuration 937
Prerequisites for IPv6 Client Mobility 937
Monitoring IPv6 Client Mobility 938

CHAPTER 106 IPv6 Support on Flex and Mesh 939
IPv6 Support on Flex + Mesh Deployment 939
Configuring IPv6 Support for Flex + Mesh 939
Configuring Preferred IP Address as IPv6 940
Verifying IPv6 on Flex+Mesh 941

CHAPTER 107 IPv6 CAPWAP UDP Lite Support 943
Information About UDP Lite 943
Enabling UDP Lite Support 943
Verifying UDP Lite Support Configuration 944

PART XI CleanAir 945

CHAPTER 108 Cisco CleanAir 947
Information About Cisco CleanAir 947
Cisco CleanAir-Related Terms 948
Cisco CleanAir Components 948
Interference Types that Cisco CleanAir can Detect 949
EDRRM and AQR Update Mode 950
Prerequisites for CleanAir 950
Restrictions for CleanAir 951

How to Configure CleanAir 951

   Enabling CleanAir for the 2.4-GHz Band (GUI) 951
   Enabling CleanAir for the 2.4-GHz Band (CLI) 951
   Configuring Interference Reporting for a 2.4-GHz Device (GUI) 952
   Configuring Interference Reporting for a 2.4-GHz Device (CLI) 953
   Enabling CleanAir for the 5-GHz Band (GUI) 954
   Enabling CleanAir for the 5-GHz Band (CLI) 955
   Configuring Interference Reporting for a 5-GHz Device (GUI) 955
   Configuring Interference Reporting for a 5-GHz Device (CLI) 956
   Configuring Event Driven RRM for a CleanAir Event (GUI) 957
   Configuring EDRRM for a CleanAir Event (CLI) 957

Verifying CleanAir Parameters 958

   Monitoring Interference Devices 960

Configuration Examples for CleanAir 961

CleanAir FAQs 961

__CHAPTER 109__

Bluetooth Low Energy 963

   Information About Bluetooth Low Energy 963
   Enabling Bluetooth Low Energy Beacon 964

__CHAPTER 110__

Persistent Device Avoidance 967

   Persistent Device Avoidance 967
   Configuring Persistent Device Avoidance (CLI) 968
   Verifying Persistent Device Avoidance 968

__CHAPTER 111__

Spectrum Intelligence 971

   Spectrum Intelligence 971
   Configuring Spectrum Intelligence 972
   Verifying Spectrum Intelligence Information 972

__PART XII__

Mesh Access Points 975

__CHAPTER 112__

Mesh Access Points 977
Configuring Wireless Backhaul Data Rate  994
Configuring Dynamic Frequency Selection  995
Configuring the Intrusion Detection System  995
Configuring Ethernet Bridging  996
Configuring Multicast over Mesh  997
Configuring RRM on Mesh Backhaul  997
Selecting a Preferred Parent  998
Changing an AP's Role  998
Configuring the Mesh Leaf Node  999
Configuring Subset-Channel Synchronization  999
Provisioning LSC for Bridge-Mode and Mesh APs  1000
Specifying the Backhaul Slot for the Root AP  1001
Using a Link Test on Mesh Backhaul  1001
Configuring Battery State for Mesh AP  1002
Configuring Mesh CAC  1002
Configuring ATF on Mesh  1003
Create an ATF Policy for a MAP  1003
Creating an ATF Policy (GUI)  1004
Adding an ATF to a Policy Profile (GUI)  1004
Enabling ATF Mode in an RF Profile (GUI)  1004
Verifying ATF Configuration on Mesh  1005
Verifying Mesh Configuration  1006

PART XIII  VideoStream  1009
CHAPTER 113  VideoStream  1011

  Information about Media Stream  1011
  Prerequisites for Media Stream  1011
  How to Configure Media Stream  1012
    Configuring Multicast-Direct Globally for Media Stream  1012
    Configuring Media Stream for 802.11 Bands  1013
    Configuring a WLAN to Stream Video(GUI)  1015
    Configuring a WLAN to Stream Video (CLI)  1015
    Deleting a Media Stream (GUI)  1016

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x
PART XIV

Software-Defined Access Wireless 1025

CHAPTER 114

Software-Defined Access Wireless 1027

Information to Software-Defined Access Wireless 1027

Configuring SD-Access Wireless 1030

Configuring Default Map Server (GUI) 1030

Configuring Default Map Server (CLI) 1031

Configuring SD-Access Wireless Profile (GUI) 1031

Configuring SD-Access Wireless Profile (CLI) 1032

Configuring Map Server in Site Tag (GUI) 1032

Configuring Map Server in Site Tag (CLI) 1033

Configuring Map Server per L2-VNID (GUI) 1033

Configuring Map Server per L2-VNID (CLI) 1034

Verifying SD-Access Wireless 1034

CHAPTER 115

Configuring Passive Client on Software Defined Access [SDA-Wireless] 1037

Information About Passive Clients 1037

Enabling Passive Client on WLAN Policy Profile (GUI) 1038

Enabling Passive Client on WLAN Policy Profile (CLI) 1038

Enabling ARP Broadcast on VLAN (GUI) 1039

Enabling ARP Broadcast on VLAN (CLI) 1039

Configuring Passive Client in Fabric Deployment 1039

Enabling Broadcast Underlay on VLAN 1039
Contents

CHAPTER 120  Remote LANs 1099
Information About Remote LANs 1099
Configuring Remote LANs (RLANs) 1100
   Enabling or Disabling all RLANs 1100
   Creating RLAN Profile 1101
   Configuring RLAN Profile Parameters (GUI) 1101
   Configuring RLAN Profile Parameters 1102
   Creating RLAN Policy Profile 1103
   Configuring RLAN Policy Profile Parameters (GUI) 1103
   Configuring RLAN Policy Profile Parameters 1105
   Configuring Policy Tag and Mapping an RLAN Policy Profile to an RLAN Profile 1107
   Configuring LAN Port 1107
   Attaching Policy Tag to an Access Point (GUI) 1108
   Attaching Policy Tag to an Access Point (CLI) 1108
   Verifying RLAN Configuration 1108

CHAPTER 121  Network Access Server Identifier 1113
Information About Network Access Server Identifier 1113
Creating a NAS ID Policy(GUI) 1114
Creating a NAS ID Policy 1114
Contents

Attaching a Policy to a Tag (GUI) 1115
Attaching a Policy to a Tag (CLI) 1115
Verifying the NAS ID Configuration 1116

CHAPTER 122

DHCP for WLANs 1117
Information about Dynamic Host Configuration Protocol 1117
  Internal DHCP Servers 1117
  External DHCP Servers 1118
  DHCP Assignments 1118
  DHCP Option 82 1119
Restrictions for Configuring DHCP for WLANs 1120
How to Configure DHCP for WLANs 1120
  Configuring DHCP Scopes (GUI) 1120
  Configuring DHCP Scopes (CLI) 1121
Configuring Internal DHCP Server 1122
  Configuring Internal DHCP Server Under Client VLAN SVI 1122
  Configuring the Internal DHCP Server Under a Wireless Policy Profile 1125
  Configuring the Internal DHCP Server Globally 1127
Verifying Internal DHCP Configuration 1130

CHAPTER 123

WLAN Security 1133
Information About WPA1 and WPA2 1133
Information About AAA Override 1134
  Configuring AAA Override 1134
Information About VLAN Override 1135
  Configuring Override VLAN for Central Switching 1135
  Configuring Override VLAN for Local Switching 1136
  VLAN Override on Layer 3 Web Authentication 1136
Verifying VLAN Override on Layer 3 Web Authentication 1137
Prerequisites for Layer 2 Security 1137
How to Configure WLAN Security 1138
  Configuring Static WEP Layer 2 Security Parameters (GUI) 1138
  Configuring Static WEP Layer 2 Security Parameters (CLI) 1138
  Configuring WPA + WPA2 Layer 2 Security Parameters (GUI) 1140
Configuring WPA + WPA2 Layer 2 Security Parameters (CLI) 1140

CHAPTER 124
Workgroup Bridges 1145
- Information About Cisco Workgroup Bridges 1145
- Configuring Workgroup Bridge on a WLAN 1146
- Verifying the Status of a Workgroup Bridge 1147

CHAPTER 125
Peer-to-Peer Client Support 1149
- Information About Peer-to-Peer Client Support 1149
- Configure Peer-to-Peer Client Support 1149

CHAPTER 126
Wireless Guest Access 1151
- Wireless Guest Access 1151
- Load Balancing Among Multiple Guest Controllers 1153
- Guidelines and Limitations for Wireless Guest Access 1154
  - IPv6 Limitations 1154
- Configure Mobility Tunnel for Guest Access (GUI) 1154
- Configure Mobility Tunnel for Guest Access 1155
- Configuring Guest Access Policy 1155
- Viewing Guest Access Debug Information (CLI) 1157
- Configuring Site Tag 1158
- Configuring Policy Tag 1158
- Associating Policy Tag to an AP 1159
- Attaching Site Tag and Policy Tag to an AP 1160
- Configure Guest Access Using Different Security Methods 1161
  - Open Authentication 1161
    - Configure WLAN Profile For Guest Access with Open Authentication 1162
    - Configuring the Policy Profile 1162
  - Local Web Authentication 1163
    - Configure the Parameter Map 1164
    - Configure WLAN Profile for Guest Access with Local Web Authentication 1164
    - Configure AAA Server for Local Web Authentication 1165
  - Global Configuration 1165
  - Central Web Authentication 1166
Restrictions for 802.11w 1222
How to Configure 802.11w 1223
   Configuring 802.11w (GUI) 1223
   Configuring 802.11w (CLI) 1223
Disabling 802.11w 1224
Monitoring 802.11w 1225

CHAPTER 133
Management Frame Protection 1227
   Information About Management Frame Protection 1227
   Restrictions for Management Frame Protection 1228
   Configuring Management Frame Protection (CLI) 1229
   Verifying Management Frame Protection Settings 1229

CHAPTER 134
Deny Wireless Client Session Establishment Using Calendar Profiles 1231
   Information About Denial of Wireless Client Session Establishment 1231
   Configuring Daily Calendar Profile 1232
   Configuring Weekly Calendar Profile 1233
   Configuring Monthly Calendar Profile 1234
   Mapping a Daily Calendar Profile to a Policy Profile 1235
   Mapping a Weekly Calendar Profile to a Policy Profile 1236
   Mapping a Monthly Calendar Profile to a Policy Profile 1237
   Verifying Calendar Profile Configuration 1238
   Verifying Policy Profile Configuration 1238

CHAPTER 135
Ethernet over GRE 1241
   Introduction to EoGRE 1241
      EoGRE Configuration Overview 1242
   Create a Tunnel Gateway 1243
   Configuring the Tunnel Gateway (GUI) 1243
   Configuring a Tunnel Domain 1244
   Configuring Tunnel Domain (GUI) 1245
   Configuring EoGRE Global Parameters 1245
   Configuring EoGRE Global Parameters (GUI) 1246
   Configuring a Tunnel Profile 1247
### Link Aggregation Control Protocol and Port Aggregation Protocol

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information About LACP</td>
<td>1259</td>
</tr>
<tr>
<td>Information About Port Aggregation Protocol</td>
<td>1259</td>
</tr>
<tr>
<td>Configuring LACP and PAgP</td>
<td>1260</td>
</tr>
<tr>
<td>Restrictions for LACP and PAgP</td>
<td>1261</td>
</tr>
<tr>
<td>Create a Port-Channel Interface</td>
<td>1262</td>
</tr>
<tr>
<td>Add an Interface to a Port Channel (LACP)</td>
<td>1262</td>
</tr>
<tr>
<td>Adding VLANs Under a LAG</td>
<td>1263</td>
</tr>
<tr>
<td>Adding an Interface to a Port Channel (PAgP)</td>
<td>1263</td>
</tr>
<tr>
<td>Removing a Port Channel Group from a Physical Port</td>
<td>1264</td>
</tr>
<tr>
<td>Verifying the Configuration</td>
<td>1264</td>
</tr>
</tbody>
</table>

### Hotspot 2.0

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to Hotspot</td>
<td>1267</td>
</tr>
<tr>
<td>Configuring Hotspot 2.0</td>
<td>1268</td>
</tr>
<tr>
<td>Configuring an Access Network Query Protocol Server</td>
<td>1268</td>
</tr>
<tr>
<td>Configuring the WAN Metrics</td>
<td>1270</td>
</tr>
<tr>
<td>Configuring an Online Sign-up Provider</td>
<td>1272</td>
</tr>
<tr>
<td>Configuring Hotspot 2.0 WLAN</td>
<td>1273</td>
</tr>
<tr>
<td>Configuring an Online Subscription with Encryption WLAN</td>
<td>1273</td>
</tr>
<tr>
<td>Attaching an ANQP Server to a Policy Profile</td>
<td>1274</td>
</tr>
<tr>
<td>Configuring Interworking for Hotspot</td>
<td>1275</td>
</tr>
<tr>
<td>Configuring Custom QoS Mapping</td>
<td>1275</td>
</tr>
<tr>
<td>Configuring DSCP-to-User Priority Mapping Exception</td>
<td>1276</td>
</tr>
<tr>
<td>Configuring Trust Upstream DSCP Value</td>
<td>1278</td>
</tr>
<tr>
<td>Configuring Generic Advertisement Service Rate Limit</td>
<td>1278</td>
</tr>
<tr>
<td>Verifying Hotspot 2.0 Configuration</td>
<td>1279</td>
</tr>
</tbody>
</table>

### Express Wi-Fi by Facebook

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Express Wi-Fi by Facebook</td>
<td>1281</td>
</tr>
</tbody>
</table>
Information About Express Wi-Fi by Facebook  1281
Restrictions for Express Wi-Fi by Facebook  1282
Enabling Express Wi-Fi by Facebook NAC for Policy Profile (GUI)  1282
Enabling Accounting RADIUS Server for Flex Profile (GUI)  1282
Configuring Captive Portal for Express Wi-Fi by Facebook (GUI)  1283
Configuring Captive Portal for Express Wi-Fi by Facebook (CLI)  1283
Configuring Express Wi-Fi by Facebook Policy on Controller (CLI)  1284
Configuring RADIUS Server for Accounting and Authentication in FlexConnect Profile (CLI)  1286
Verifying Express Wi-Fi by Facebook Configurations on Controller  1287
Verifying Express Wi-Fi by Facebook Configurations on the AP  1287

PART XVII

Multicast Domain Name System  1291

CHAPTER 139

Multicast Domain Name System  1293

Introduction to mDNS Gateway  1293
Enabling mDNS Gateway (GUI)  1294
Enabling or Disabling mDNS Gateway (CLI)  1294
Creating Custom Service Definition (GUI)  1295
Creating Custom Service Definition  1296
Creating Service List (GUI)  1297
Creating Service List  1297
Creating Service Policy (GUI)  1298
Creating Service Policy  1299
Configuring a Local or Native Profile for an mDNS Policy  1300
Enabling the mDNS Gateway on the VLAN Interface  1301
Location-Based Service Filtering  1301
  Prerequisite for Location-Based Service Filtering  1301
  Configuring mDNS Location-Based Filtering Using SSID  1302
  Configuring mDNS Location-Based Filtering Using AP Name  1302
  Configuring mDNS Location-Based Filtering Using AP Location  1303
  Configuring mDNS Location-Based Filtering Using Regular Expression  1303
Configuring an mDNS AP  1304
Enabling mDNS Gateway on the RLAN Interface  1305
Enabling mDNS Gateway on Guest LAN Interface  1307
Contents

Associating mDNS Service Policy with Wireless Profile Policy  1308
Enabling or Disabling mDNS Gateway for WLAN  1311
mDNS Gateway with Guest Anchor Support and mDNS Bridging  1312
Configuring mDNS Gateway on Guest Anchor (Guest LAN)  1312
Configuring mDNS Gateway on Guest Foreign (Guest LAN)  1313
Verifying mDNS Gateway Configurations  1313
Preface

- Document Conventions, on page lix
- Related Documentation, on page lxi
- Obtaining Documentation and Submitting a Service Request, on page lxi

Document Conventions

This document uses the following conventions:

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

| 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
  This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

  SAVE THESE INSTRUCTIONS
Related Documentation

Before installing or upgrading the device, refer to the device release notes at https://www.cisco.com/go/c9800.

- 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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
Overview of the Cisco Catalyst 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 controller is deployable in physical and virtual (private and public cloud) form factors and is manageable controller using Cisco DNA 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:

- Catalyst 9800 Series Wireless Controller Appliance
- Catalyst 9800 Series Wireless Controller for Cloud
- 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. This model provides a model to map access points (APs) to three types of tags. The clients and APs derive their configurations from profiles that are contained within tags.

- 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

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 define 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
   - Site
   - RF

2. Create the following tags:
   - Policy
   - Site
   - RF

3. Associate tags to an AP.
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.

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 33
- BIOS Protection, on page 41
- Smart Licensing, on page 43
- Best Practices, on page 53
Information About New Configuration Model

Cisco Catalyst 9800 Series Wireless Controller simplifies the configuration of the wireless controller 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 a specific target. The configuration targets are AP, radio, and WLAN. 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 new configuration model (flexconnect mode) helps the central controller to manage sites that are geo-distributed, for example, retail, campus, and so on, where the WLANs are the same. Only, the network and radio profiles have some changes based on the local deployment or topology.
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 master 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 IEEE 802.11a and IEEE 802.11b 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 a specific target. The configuration targets are AP, radio, and WLAN. 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 the attributes that are a part of the flex group. However, policy attributes are grouped with the policy profile. The flex profile also contains 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 the following parameters – 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.

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, 9115AXI, 9115AXE, 9117I, APVIRTUAL, 9120AXE, and 9120AXI.

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.

Static Association of APs

APs can only be configured statically using the policy-tag, site tag, and RF tag. The APs are identified by the Ethernet MAC address and the association to AP and tag is stored on the controller as a configuration.

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.
- **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
- Central Authentication
- Central DHCP
- Central Association Enable
- Flex NAT/PAT

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

---

### Configuring a Wireless Profile Policy (CLI)

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

---

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless profile policy <em>profile-policy</em></td>
<td>Configures WLAN policy profile and enters wireless policy configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# wireless profile policy rr-xyz-policy-1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> idle-timeout <em>timeout</em></td>
<td>(Optional) Configures the duration of idle timeout, in seconds.</td>
</tr>
<tr>
<td>Example: Device(config-wireless-policy)# idle-timeout 1000</td>
<td></td>
</tr>
</tbody>
</table>

---

**Note**

When a client moves from an old controller to a new controller (managed by 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.
### Setting a Flex Profile

Follow the procedure given below to set a flex profile:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>wireless profile flex flex-profile</code></td>
<td>Configures an RF profile and enters RF profile configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# wireless profile flex rr-wyz-flex-profile</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>description</code></td>
<td>(Optional) Enables default parameters for the RF profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-wireless-flex-profile)# description xyz-default-flex-profile</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>arp-caching</code></td>
<td>(Optional) Enables ARP caching.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

Note: (Optional) To view detailed information about a policy profile, use the `show wireless profile policy detailed policy-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 the following parameters – CAPWAP IPv4/IPv6, UDP Lite, High Availability, retransmit configuration parameters, global AP failover, Hyperlocation configuration parameters, Telnet/SSH, 11u parameters, and so on.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Device(config-wireless-flex-profile)# arp-caching</td>
<td>Saves the configuration and exits configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 5</strong> end</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-flex-profile)# end</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><strong>Step 6</strong> show wireless profile flex summary</td>
<td>(Optional) Displays the flex-profile parameters.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show wireless profile flex summary</td>
<td></td>
</tr>
</tbody>
</table>

**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 the following parameters – 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.

**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.

  **Note** Configure Fast Heartbeat Timeout to assist AP in sending primary discovery request periodically to the configured backup controllers along with the primary, secondary, and tertiary-base controllers.

  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.

- 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.
  
  c) From the **Power Injector Type** drop-down list, choose power injector type from the following options:
    - Installed—If you want the AP to examine and remember the MAC address of the currently connected switch port. (This selection assumes that a power injector is connected.)
    - Override—To enable the AP to operate in high-power mode without first verifying a matching MAC address.
  
  d) In the **Injector Switch MAC** field, enter the MAC address of the switch.
  
  e) Enter the relevant country code. The country code enables you to specify a particular country of operation (such as FR for France or ES for Spain).
  
  f) From the **EAP Type** drop-down list, choose the EAP type as **EAP-FAST**, **EAP-TLS**, or **EAP-PEAP**.
  
  g) From the **AP Authorization Type** drop-down list, choose the type as either **CAPWAP DTLS +** or **CAPWAP DTLS**.
  
  h) In the **Client Statistics Reporting Interval** section, enter the interval for 5 GHz and 2.4 GHz radios in seconds.
  
  i) Check the **Enable** check box to enable extended module.
  
  j) From the **Profile Name** drop-down list, choose a profile name for mesh.
  
  k) 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.
- 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.

- 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.
Configuring an AP Profile (CLI)

Follow the procedure given below to configure an AP profile:

**Before you begin**

When you modify an AP join profile in the controller, the NTP server IP is not pushed to the AP. This is because, the AP profile-specific NTP server IP is introduced to address the time sensitivity of the Hyperlocation feature and is pushed to the AP only when the operational status of Hyperlocation is Up. This behavior is applicable to all Hyperlocation-related TLVs (trigger threshold, reset threshold, and detection threshold) as well.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>ap profile ap-profile</code></td>
<td>Configures an AP profile and enters AP profile</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>configuration mode.</td>
</tr>
<tr>
<td>Device(config)# ap profile xyz-ap-profile</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When you delete a named profile, the APs</td>
</tr>
<tr>
<td></td>
<td>associated with that profile will not revert to</td>
</tr>
<tr>
<td></td>
<td>the default profile.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>description ap-profile-name</code></td>
<td>Adds a description for the ap profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring an RF Profile (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 > RF. |
| Step 2 | On the RF Profile page, click Add. |
| Step 3 | In the General tab, enter a name for the RF profile. |
| 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:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cdp</code></td>
<td>Enables CDP for all Cisco APs.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Saves the configuration and exits configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>show ap profile profile-name summary</code></td>
<td>(Optional) Displays the number of AP join profiles. Note: To view detailed information about an AP join profile, use the <code>show ap profile profile-name detailed</code> command.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ap dot11 24ghz rf-profile rf-profile</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap dot11 24ghz rf-profile rfprof24_1</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>default</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-rf-profile)# default</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>no shutdown</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-rf-profile)# no shutdown</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-rf-profile)# end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show ap rf-profile summary</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show ap rf-profile summary</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show ap rf-profile name rf-profile detail</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show ap rf-profile name rfprof24_1 detail</td>
</tr>
</tbody>
</table>

Configuring a Site Tag (GUI)

Procedure

**Step 1** Choose Configuration > Tags & Profiles > Tags.
### Configuring a Site Tag (CLI)

Follow the procedure given below to configure a site tag:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code>&lt;br&gt;Example: <code>Device# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>wireless tag site site-name</code>&lt;br&gt;Example: <code>Device(config)# wireless tag site rr-xyz-site</code></td>
<td>Configures a site tag and enters site tag configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>flex-profile flex-profile-name</code>&lt;br&gt;Example: <code>Device(config-site-tag)# flex-profile rr-xyz-flex-profile</code></td>
<td>Configures a flex profile.  &lt;br&gt;Note: You cannot remove the flex profile configuration from a site tag if local site is configured on the site tag.  &lt;br&gt;Note: The <code>no local-site</code> command needs to be used to configure the Site Tag as Flexconnect, otherwise the Flex profile config does not take effect.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>description site-tag-name</code>&lt;br&gt;Example: <code>Device(config-site-tag)# description &quot;default site tag&quot;</code></td>
<td>Adds a description for the site tag.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code>&lt;br&gt;Example: <code>Device(config-site-tag)# end</code></td>
<td>Saves the configuration and exits configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>show wireless tag site summary</code></td>
<td>(Optional) Displays the number of site tags.</td>
</tr>
</tbody>
</table>
### Configuring Policy Tag (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configuration</strong> &gt; <strong>Tags &amp; Profiles</strong> &gt; <strong>Tags</strong> &gt; <strong>Policy</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>Add</strong> to view the <strong>Add Policy Tag</strong> window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter a name and description for the policy tag.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Add</strong> to map WLAN and policy.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Save &amp; Apply to Device</strong>.</td>
</tr>
</tbody>
</table>

### Configuring a Policy Tag (CLI)

Follow the procedure given below to configure a policy tag:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>wireless tag policy policy-tag-name</code></td>
<td>Configures policy tag and enters policy tag configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-policy-tag)# wireless tag policy default-policy-tag</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Wireless RF Tag (GUI)

**Procedure**

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

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

3. **Step 3**  
   Enter a name and description for the RF tag.

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

5. **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 (IEEE 802.11a and IEEE 802.11b) in an RF tag.
- Ensure that you use the same AP tag name that you created when configuring the AP tag task too.
## Attaching a Policy Tag and Site Tag to an AP (GUI)

### Procedure

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

### 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**

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

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.

#### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> `ap tag-source-priority source-priority source {filter</td>
<td>pnp}`</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config)# ap tag-source-priority 2 source pnp</code></td>
<td><strong>Note</strong> It is not mandatory to configure AP filter. It comes with default priorities for Static, Filter, and PnP.</td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>end</code></td>
<td>Exits configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
Create an AP Filter

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.

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.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures an AP filter.</td>
</tr>
<tr>
<td>ap filter name <em>filter_name</em></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ap filter filter-1</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the AP filter based on regular expression.</td>
</tr>
<tr>
<td>ap name-regex <em>regular-expression</em></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-ap-filter)# ap name-regex testany</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures a policy tag for this filter.</td>
</tr>
<tr>
<td>tag policy <em>policy-tag</em></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-ap-filter)# tag policy pol-tag1</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures an RF tag for this filter.</td>
</tr>
<tr>
<td>tag rf <em>rf-tag</em></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-ap-filter)# tag rf rf-tag1</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Configures a site tag for this filter.</td>
</tr>
<tr>
<td>tag site <em>site-tag</em></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Set Up and Update Filter Priority

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

Procedure

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure AP filter priority.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>A filter without a priority is not active. Similarly, you cannot set a filter priority without a filter.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap filter priority 10 filter-name test1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Exits configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-ap)# end</td>
</tr>
</tbody>
</table>

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`

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>regex</th>
<th>Policy Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>first</td>
<td>abcd</td>
<td>pol-tag1</td>
</tr>
</tbody>
</table>
To view the list of active filters, use the following command:

```
Device# show ap filters active
```

<table>
<thead>
<tr>
<th>Priority</th>
<th>Filter Name</th>
<th>regex</th>
<th>Policy Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>test1</td>
<td>testany</td>
<td>sitel</td>
</tr>
</tbody>
</table>

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

```
Device# show ap tag summary
```

<table>
<thead>
<tr>
<th>AP Name</th>
<th>AP Mac</th>
<th>Site Tag Name</th>
<th>Policy Tag Name</th>
<th>RF Tag Name</th>
<th>Misconfigured Tag Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP002A.1034.CA78 002a.1034.ca78</td>
<td>named-site-tag</td>
<td>named-policy-tag</td>
<td>named-rf-tag</td>
<td>No Filter</td>
<td></td>
</tr>
<tr>
<td>AP00A2.891C.2480 00a2.891c.2480</td>
<td>named-site-tag</td>
<td>named-policy-tag</td>
<td>named-rf-tag</td>
<td>No Filter</td>
<td></td>
</tr>
<tr>
<td>AP58AC.78DE.9946 58ac.78de.9946</td>
<td>default-site-tag</td>
<td>default-policy-tag</td>
<td>default-rf-tag</td>
<td>No AP</td>
<td></td>
</tr>
<tr>
<td>AP0081.C4F4.1F34 0081.c4f4.1f34</td>
<td>default-site-tag</td>
<td>default-policy-tag</td>
<td>default-rf-tag</td>
<td>No Default</td>
<td></td>
</tr>
</tbody>
</table>

## 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)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configuration</strong> &gt; <strong>Wireless Setup</strong> &gt; <strong>Basic</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the <strong>Basic Wireless Setup</strong> page, click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>General</strong> tab, enter a name and description for the location.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Set the <strong>Location Type</strong> as either <strong>Local</strong> or <strong>Flex</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Use the slider to set <strong>Client Density</strong> as <strong>Low</strong>, <strong>Typical</strong> or <strong>High</strong>. This plug-in sets the RF characteristics of an AP.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

Configuring a Location for an Access Point (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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  
Device(config-ap-location)# tag rf rf_tag  
Device(config-ap-location)# tag site site_tag | Configures tags for the location. |
| **Step 4** | **location description**  
**Example:**  
Device(config-ap-location)# location description | Adds description to the location. |
Adding an Access Point to the Location (GUI)

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.

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>ap location name location_name</td>
<td>Configures a location for an access point.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# ap location name location1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>ap-eth-mac ap_ethernet_mac</td>
<td>Adds an access point to the location.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-ap-location)# ap-eth-mac 188b.9de.6ec</td>
<td></td>
</tr>
</tbody>
</table>
Step 4:  

Example:  

Device(config-ap-location)# end

**Purpose**

- 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

### Prerequisites for SNMP in Location Configuration

- The management port must be up and running.
- The management port must have a 10x network IP address to query SNMP commands because the IP Address from where you are issuing the SNMP getmany is in **10.x.x.x** network.

### 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**

<table>
<thead>
<tr>
<th>MIB Objects</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>cLApLocationName</td>
<td>Provides the name of the AP location.</td>
</tr>
<tr>
<td>cLApLocationPolicyTag</td>
<td>Provides the policy tag configured on the location.</td>
</tr>
<tr>
<td>cLApLocationSiteTag</td>
<td>Provides the site tag configured on the location.</td>
</tr>
<tr>
<td>cLApLocationRfTag</td>
<td>Provides the RF tag configured on the location.</td>
</tr>
<tr>
<td>cLAssociatedApsApMac</td>
<td>Provides the configured APs on the location.</td>
</tr>
</tbody>
</table>

### Verifying Location Configuration

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

```
Device# show ap location summary
```

<table>
<thead>
<tr>
<th>Location Name Tag</th>
<th>Description</th>
<th>Policy Tag</th>
<th>RF Tag</th>
<th>Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>first default-site-tag</td>
<td>first floor</td>
<td>default-policy-tag</td>
<td>default-rf-tag</td>
<td></td>
</tr>
<tr>
<td>second default-site-tag</td>
<td>second floor</td>
<td>default-policy-tag</td>
<td>default-rf-tag</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>AP Name</th>
<th>AP Mac</th>
<th>Site Tag Name</th>
<th>Policy Tag Name</th>
<th>RF Tag Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asim_5-1</td>
<td>005b.3400.02f0</td>
<td>default-site-tag</td>
<td>default-policy-tag</td>
<td>default-rf-tag</td>
</tr>
<tr>
<td>Yes</td>
<td>Filter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asim_5-2</td>
<td>005b.3400.03f0</td>
<td>default-site-tag</td>
<td>default-policy-tag</td>
<td>default-rf-tag</td>
</tr>
<tr>
<td>No</td>
<td>Default</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asim_5-9</td>
<td>005b.3400.0af0</td>
<td>default-site-tag</td>
<td>default-policy-tag</td>
<td>default-rf-tag</td>
</tr>
<tr>
<td>No</td>
<td>Location</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asim_5-10</td>
<td>005b.3400.0bf0</td>
<td>default-site-tag</td>
<td>default-policy-tag</td>
<td>default-rf-tag</td>
</tr>
<tr>
<td>No</td>
<td>Location</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Verifying Location Statistics

To view the AP location statistics, use the following command:
Device# `show ap location stats`

<table>
<thead>
<tr>
<th>Location name</th>
<th>APs joined</th>
<th>Clients joined</th>
<th>Clients on 11a</th>
<th>Clients on 11b</th>
</tr>
</thead>
<tbody>
<tr>
<td>first</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>second</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Verifying Location Statistics
RF Profile

- RF Tag Profiles, on page 33
- Configuring an AP Tag (GUI), on page 33
- Configuring AP Tag (CLI), on page 34
- Configuring RF Profile (GUI), on page 35
- Configuring an RF Profile (CLI), on page 36
- Configuring Wireless RF Tag (GUI), on page 37
- Configuring Wireless RF Tag (CLI), on page 38

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

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

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

Configuring Wireless RF Tag (GUI)

Procedure

1. a) Choose **Configuration > Tags & Profiles > Tags > RF.**
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 (IEEE 802.11a and IEEE 802.11b) in an RF tag.
- Ensure that you use the same AP tag name that you created when configuring the AP tag task too.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless tag rf rf-tag</td>
<td>Creates an RF tag and enters wireless RF tag configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless tag rf rftag1</td>
</tr>
<tr>
<td><strong>Step 3</strong> 24ghz-rf-policy rf-policy</td>
<td>Attaches an IEEE 802.11b RF policy to the RF tag.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-rf-tag)# 24ghz-rf-policy rfprof24_1</td>
</tr>
<tr>
<td><strong>Step 4</strong> description policy-description</td>
<td>Adds a description for the RF tag.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-rf-tag)# description Test</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-rf-tag)# end</td>
</tr>
<tr>
<td><strong>Step 6</strong> show wireless tag rf summary</td>
<td>Displays the available RF tags.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# show wireless tag rf summary</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 7</strong> show wireless tag rf detailed rf-tag</td>
<td>Displays detailed information of a particular RF tag.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# show wireless tag rf detailed rftag1</td>
<td></td>
</tr>
</tbody>
</table>

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x
Configuring Wireless RF Tag (CLI)
BIOS Protection

- BIOS Protection on the Controller, on page 41
- BIOS or ROMMON Upgrade with BIOS Protection, on page 41
- Upgrading BIOS, on page 42

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
```
Smart Licensing

- Information About Cisco Smart Licensing, on page 43
- Creating a Smart Account, on page 45
- Using Smart Licensing, on page 46
- Using Specified License Reservation (SLR), on page 46
- Enabling Specified License Reservation in CSSM, on page 47
- Enabling Smart Software Licensing, on page 47
- Enabling Smart Call Home Reporting, on page 48
- Configuring AIR License Level (GUI), on page 48
- Configuring AIR License Level (CLI), on page 49
- Configuring AIR Network Essentials License Level, on page 49
- Configuring AIR Network Advantage License Level, on page 50
- Verifying Smart Licensing Configurations, on page 50

Information About Cisco Smart Licensing

Cisco Smart Licensing is a Software Inventory Management System that provides floating licenses on a user account. Smart Licensing offers you Cisco Smart Software Manager, a centralized portal that enables you to manage all your Cisco software licenses from one centralized website.

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

Starting with Cisco IOS XE Gibraltar 16.12.1, the Cisco Catalyst 9800 Series Wireless Controller does not support satellite server for licensing reporting. You should use the Cisco Smart Software Manager (CSSM) for any licensing reporting.

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.

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.

You need to execute the `write memory` command once in the following cases:

- When the Standby becomes Active after the first switchover.
- When the license de-registers after the switchover.

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)

The AIR-DNA-A is the default mode.

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

For more details on CSSM, see:

Using Specified License Reservation (SLR)

<table>
<thead>
<tr>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command or Action</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Enabling Specified License Reservation in CSSM

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Login to CSSM.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter the request code in CSSM. (See Using Specified License Reservation (SLR))</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the licenses that are required as per the license active on your controller.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Generate <em>auth-code</em> file on your controller using the following command:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# conf t</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# license smart reservation install file &lt;&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Verify the authorization status on your controller using the following command:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show license reservation</td>
<td></td>
</tr>
</tbody>
</table>

### Enabling Smart Software Licensing

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Navigate to the Cisco Software Central web page using the following link:</td>
<td><a href="https://software.cisco.com/#">https://software.cisco.com/</a></td>
</tr>
<tr>
<td></td>
<td>The Cisco Software Central page is displayed.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>From the License tab, click Smart Software Licensing.</td>
<td>The Smart Software Licensing page is displayed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Inventory tab to view Virtual Account: Accounting page details.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Click New Token to register the product instances to this virtual account.</td>
<td>The Create Registration Token page is displayed.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Description field, enter a description for the ID token.</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>Check the Allow export-controlled functionality on the products registered with this token checkbox to enable export-controlled functionality.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Click Create Token.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Licenses cannot be purchased with the wireless controller. All licenses can be purchased with access points.</td>
<td></td>
</tr>
</tbody>
</table>

## Enabling Smart Call Home Reporting

### Procedure

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

| **Step 2**            | call-home reporting contact-email-addr 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. |

**Note** 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; Licensing.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Change Wireless License Level. The Change Wireless License Level dialog box is displayed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the License Level using the drop-downs.</td>
</tr>
<tr>
<td>Step 4</td>
<td>After changing the New Level values, click Save &amp; 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.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click refresh icon to refresh the device.</td>
</tr>
</tbody>
</table>

---
### Configuring AIR License Level (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures AIR license level.</td>
</tr>
<tr>
<td>license air level {air-network-advantage</td>
<td>air-network-essentials}</td>
</tr>
<tr>
<td>Example: Device(config)# license air level air-network-advantage</td>
<td></td>
</tr>
<tr>
<td>Device(config)# license air level air-network-essentials</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring AIR Network Essentials License Level

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures AIR network essentials license level.</td>
</tr>
<tr>
<td>license air level network-essentials addon air-dna-essentials</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# license air level network-essentials addon air-dna-essentials</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring AIR Network Advantage License Level

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> license air level air-network-advantage addon air-dna-advantage</td>
<td>Configures AIR network advantage license level.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# license air level air-network-advantage addon air-dna-advantage</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

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
Best Practices

- Infrastructure, on page 53
- Security, on page 57
- RF Management, on page 58
- Apple Devices, on page 67

Infrastructure

Disable Aironet IE

- Description—Aironet IE is a Cisco proprietary attribute used by Cisco devices for better connectivity. It contains information, such as the access point name, load, number of associated clients, and so on sent out by the access point (AP) in the beacon and probe responses of the Cisco Catalyst 9800 Series Wireless Controller. The Cisco Client Extensions (CCX) clients use this information to choose the best AP with which to associate.

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

Aironet IE is optional for CCX based clients, however it can cause compatibility issues with some types of wireless clients. The recommendation is to enable for WGB and Cisco voice, but for general production network, it can be beneficial to disable Aironet IE after testing.

CCX Aironet IE feature should be disabled.

- Status:
  - Selected—CCX Aironet IE must be disabled on one or more *ACTIVE* WLANs.
  - Unselected—CCX Aironet IE enabled on all *ACTIVE* WLANs.

- CLI Option—Enable support for Aironet IEs for a particular WLAN by entering this command:

  Device# config

  Device(config)# wlan <profile-name> <wlan-id> <ssid>

  Device(config-wlan)# ccx aironet-iesupport
- **CLI Option**—Disable support for Aironet IEs for a particular WLAN by entering this command:

```
Device# conf t
Device(config)# wlan <profile-name> <wlan-id> <ssid>
Device(config-wlan)# no ccx aironet-iesupport
```

### Disable Management over Wireless

- **Description**—The Cisco WLAN solution Disable Management over Wireless feature allows Cisco WLAN solution operators to monitor and configure local controller using a wireless client.

  Management over wireless should be disabled for security reasons. Clicking **Fix it Now** disables management over wireless.

- **Status:**
  - Selected—Enabled
  - Unselected—Disabled

- **CLI Option**—Disable management over wireless by entering this command:

```
Device# no wireless mgmt-via-wireless
```

- **CLI Option**—Enable management over wireless by entering this command:

```
Device# wireless mgmt-via-wireless
```

### HTTPs for Management

- **Description**—HTTPs for management provides greater security by allowing secure access.

  Secure Web Access (HTTPS) should be enabled for managing the Cisco Catalyst 9800 Series Wireless Controller. Web Access (HTTP) should be disabled.

- **Status:**
  - Selected—HTTPS enabled; HTTP disabled
  - Unselected—HTTPS enabled, HTTP enabled or HTTPS disabled, HTTP enabled

- **CLI Options:**

  - Disable the web mode to deny users to access the controller GUI using http://ip-address, by entering this command:

```
Device# conf t
Device(config)# no ip http secure-server
```

  - Enable Secure Web Access mode to allow users to access the controller GUI using https://ip-address, by entering this command:

```
Device# conf t
Device(config)# ip http secure-server
```
Load Balancing

- Description—In dense production networks, controllers have been verified to function optimally with load balancing ON and window size set at 5 or higher. In practical, this means load balancing behavior is only enabled when, for example, a large group of people congregate in a conference room or open area (meeting or class). Load balancing is very useful to spread these users between various available APs in such scenarios.

Load balancing should be enabled. For time sensitive application such as voice, it can cause roaming issues. Therefore, it is recommended to test before enabling load balancing on the Cisco Catalyst 9800 Series Wireless Controller. Clicking Restore Default enables load balancing on the Cisco Catalyst 9800 Series Wireless Controller, which may impact service at the time.

- Status:
  - Selected—Load balancing disabled on all active WLANs.
  - Unselected—Load balancing enabled on one or more active WLANs.

- CLI Option—Enable load balancing on a WLAN by entering this command:

```
Device# conf t
Device(config)# wlan <profile-name> <wlan-id> <ssid>
Device(config-wlan)# load-balance
```

- CLI Option—Disable load balancing on a WLAN by entering this command:

```
Device# conf t
Device(config)# wlan <profile-name> <wlan-id> <ssid>
Device(config-wlan)# no load-balance
```

NTP

- Description—Network Time Protocol (NTP) is very important for several features. It is mandatory to use NTP synchronization on the Cisco Catalyst 9800 Series Wireless Controller if you use any of these features: Location, SNMPv3, access point authentication, or MFP. The controller supports synchronization with NTP.

The NTP server is used to sync the Cisco Catalyst 9800 Series wireless controller's time.

- Status—If disabled, click Manual Configuration to manually configure the syncing with the NTP server.
  - Selected—NTP is configured on the Cisco Catalyst 9800 Series wireless controller.
  - Unselected—NTP is not configured on the Cisco Catalyst 9800 Series wireless controller.

- CLI Option:
  - Enable NTP server by entering this command:

```
Device# conf t
Device(config)# ntp server <server-name>
```
Virtual Gateway IP

• Description—virtual gateway IP should be enabled. Clicking Fix it Now enables virtual gateway IP.

• Status:
  • Selected—Enabled
  • Unselected—Disabled

Local Profiling

• Description—The controller in Cisco Catalyst 9800 series-enabled APs can determine the client type from the information received when a client device associates with the controller. This controller acts as the collector of the information, and either displays the information directly on the Cisco Catalyst 9800 Series Wireless Controller GUI dashboard or sends required data to the ISE optimally.

Local profiling (DHCP/HTTP) should be enabled on the Cisco Catalyst 9800 Series wireless controller. This may impact service at the time.

• CLI Option—Enable local profiling (DHCP/HTTP) on all WLANs by entering this command:

  Device# conf t
  Device(config)# wireless profile policy <policy name>
  Device(config-wireless-policy)# http-tlv-caching
  Device(config-wireless-policy)# dhcp-tlv-caching
  Device(config-wireless-policy)# radius-profiling

To disable local profiling on all WLANs, use the same CLIs with a no command. For instance:

  Device# conf t
  Device(config)# wireless profile policy <policy name>
  Device(config-wireless-policy)# no http-tlv-caching
  Device(config-wireless-policy)# no dhcp-tlv-caching
  Device(config-wireless-policy)# no radius-profiling

VRF and Routing Protocol

Cisco Catalyst 9800 Series Wireless Controller does not support VRFs or routing protocols. The controller should not be used as a router for wireless clients.

Site Tag

• We recommend that you use a custom site-tag instead of the default-site-tag for APs.
• We recommend that you limit the number of APs per site-tag to 400. For example, if you have more than 400 APs in a building, use two site-tags for the building.

Security

WLAN with WPA2 or 802.1X

• Description—WLAN should be using 802.1x or WPA2 security. You can enable this from the linked WLAN page. The default day 0 setting does not mandate configuring 802.1x.

• Status—If disabled, click Manual Configuration to specify the security setting of the WLAN.
  • Selected—Either 802.1x or WPA2 is enabled on at least one WLAN.
  • Unselected—Neither security is enabled on any WLAN.

• CLI option—Enable WLAN with WPA2 or 802.1x security by entering this command:

```
Device# conf t
Device(config)# wlan <profile-name> id <wlan-id>
```

Client Exclusion

• Description—When the user fails to authenticate, the controller excludes the client. The client cannot connect to the network until the exclusion timer expires or is manually overridden by the administrator.

Client exclusion detects authentication attempts made by a single device. When the device exceeds a maximum number of failures, that MAC address is not allowed to associate any longer to the controller.

Client exclusion is enabled by default on the master AP allowing it to exclude clients from joining the controller during the above events.

When you click Fix it, the following components are enabled:

• Excessive 802.11 Association Failures
• Excessive 802.1X Authentication Failures
• Excessive 802.1X Authentication Timeout
• IP Theft or IP Reuse
• Excessive Web Authentication Failures

• Status:
  • Selected—Client exclusion is enabled for all events
  • Unselected—Client exclusion is disabled for all events

• CLI Option—Enable client exclusion for all events by entering this command:
Device# config
Device (config)# wireless profile policy <default-policy-profile>
Device (config-wireless-policy)# exclusionlist timeout <secs>

Note
The valid values for exclusion-list timeout ranges between 0 and 2147483647 seconds. Here, 0 refers to no timeout.

CLI Option—Disable client exclusion for all events by entering this command:

Device# config
Device (config)# wireless profile policy <default-policy-profile>
Device (config-wireless-policy)# exclusionlist timeout 0

User Login Policies

• Description—The user login policies are provided to limit the number of concurrent logins of the local netusers of the controller. You can limit the number of concurrent logins, and the recommendation is greater than default of 0 (unlimited).

• Status:
  • Selected—User login policies enabled only if the login count is set to either 0 or 8.
  • Unselected—User login policies disabled only if the login count is set to either 0 or 8.

Note
0 refers to unlimited restrictions for user login policies.

• CLI Option:
  • Verify the user login policies by entering this command:

    Device# show run | i max-user-login

  • Configure user login policies by entering this command:

    Device# config
    Device (config)# wireless client max-user-login ?
    <0-8> Maximum number of login sessions for a single user, 0-8 (0=Unlimited)

RF Management

Auto Coverage Hole Detection

• Description—Auto CHD should be enabled.
The controller uses the quality of client signal levels reported by the APs to determine if the power level of that AP needs to be increased. Coverage Hole Detection (CHD) is controller independent, so the RF group leader is not involved in those calculations. The controller knows how many clients are associated with a particular AP and what are the signal-to-noise ratio (SNR) values for each client.

If a client SNR drops below the configured threshold value on the controller, the AP increases its power level to try to compensate for the client. The SNR threshold is based on the transmit power of the AP and the coverage profile settings on the controller.


- **Status:**
  - Selected—CHD enabled
  - Unselected—None or one enabled

- **CLI Option**—Enable auto CHD by entering this command:

  ```
  Device# conf t
  Device (config)# ap dot11 24ghz/5gHz rrm coverage
  ```

- **CLI Option**—Disable auto CHD by entering this command:

  ```
  Device# conf t
  Device (config)# no ap dot11 24ghz/5gHz rrm coverage
  ```

**Auto Dynamic Channel Assignment**

- **Description**—Auto DCA should be enabled to allow RRM to select best channels for each radio.

  When a wireless network is first initialized, all radios participating require a channel assignment to operate without interference - optimizing the channel assignments to allow for interference free operation is DCA’s job. Wireless network does this using the air metrics reported by each radio on every possible channel, and providing a solution that maximizes channel bandwidth and minimizes RF interference from all sources - Self (signal), other networks (foreign interference), Noise (everything else).

  DCA is enabled by default and provides a global solution to channel planning for your network.

- **Status:**
  - Selected—DCA is enabled for 802.11a/b
  - Unselected—None or one is enabled

- **CLI Option**—Enable auto DCA by entering this command:

  ```
  Device# conf t
  Device (config)# ap dot11 5ghz/24ghz rrm channel dca global auto
  ```

- **CLI Option**—Disable auto DCA by entering this command:

  ```
  Device# conf t
  Device (config)# no ap dot11 5ghz/24ghz rrm channel dca global auto
  ```
Auto Transmit Power Control

- Description—The controller dynamically controls the access point transmit power based on real-time wireless LAN conditions. You can choose between two versions of transmit power control: TPCv1 and TPCv2. With TPCv1, power can be kept low to gain extra capacity and reduce interference. With TPCv2, transmit power is dynamically adjusted with the goal of minimum interference. TPCv2 is suitable for dense networks. In this mode, there could be higher roaming delays and coverage hole incidents.

Auto TPC is enabled by default to allow RRM to select best transmit power for each radio.

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

![Note]

For optimal performance, use the Automatic setting to allow best transmit power for each radio.

- Status:
  - Selected—TPC enabled for 802.11a/b
  - Unselected—None or one enabled

- CLI Option—Enable Auto TPC by entering this command:

```
Device# conf t
Device (config)# ap dot11 5ghz rrm txpower auto
Device (config)# ap dot11 24ghz rrm txpower auto
```

CleanAir Detection

- Description—CleanAir should be enabled.

To effectively detect and mitigate RF interference, enable CleanAir whenever possible. There are recommendations to various sources of interference to trigger security alerts, such as generic DECT phones, jammer, and so on.

![Note]

Not all Cisco access points support CleanAir. Consult the data sheet of your Cisco AP model to see whether it supports CleanAir.

- Status:
  - Selected—Enabled
  - Unselected—Disabled
• CLI Option:
  • Verify CleanAir configuration on a network by entering this command:
    (Cisco Controller) > show 802.11{a|b} cleanair config
  • Enables CleanAir functionality on a network by entering this command:
    Device# configure terminal
    Device(config)# ap dot11 {5ghz | 24ghz} cleanair {alarm | device}
  • Enables interference detection specifically for jammer by entering this command:
    Device# configure terminal
    Device(config)# ap dot11 {5ghz | 24ghz} cleanair device jammer

Event Driven RRM

• Description—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 radio resource management (RRM) feature allows you to set a threshold for air quality (AQ) that, if exceeded, triggers an immediate channel change for the affected access point. Most RF management systems can avoid interference, but this information takes time to propagate through the system. Cisco CleanAir relies on AQ measurements to continuously evaluate the spectrum and can trigger a move within 30 seconds. For example, if an access point detects interference from a video camera, it can recover by changing channels within 30 seconds of the camera becoming active. Cisco CleanAir also identifies and locates the source of interference so that more permanent mitigation of the device can be performed at a later time.

Note
Spectrum EDRRM can be triggered, to detect a significant level of interference, only by Cisco CleanAir-enabled access points in local mode.

Event driven RRM is enabled by default.

• Status:
  • Selected—Event driven RRM is disabled on both 5GHz and 2.4GHz.
  • Unselected—Event driven RRM is enabled on either 5GHz or 2.4GHz.

• CLI Option—Enable Cisco CleanAir spectrum event-driven RRM by entering this command:
  Device# conf t
  Device (config)# ap dot11 {5ghz | 24ghz} rrm channel cleanair-event

WiFi Interference

• Description—To improve handling of WiFi Interference, Rogue Severity was added to the ED-RRM metrics. If a rogue access point is generating interference above a given threshold, this feature changes channels immediately instead of waiting until the next DCA cycle.
This should be used when ED-RRM is enabled. It should be avoided on buildings with very large number of collocated WiFi networks (multi-tenant buildings) that are 100% overlapping.

**Status**

- **Selected**—WiFi interference is enabled.
- **Unselected**—WiFi interference is disabled.

**CLI Option:**

- Verify the WiFi interference by entering this command:
  
  ```
  Device# show ap dot11 24ghz cleanair config
  ```

- To enable WiFi interference, you need to perform the following:
  
  - Configure duty cycle by entering this command:
    
    ```
    Device# conf t
    Device (config)# ap dot11 24ghz rrm channel cleanair-event rogue-contribution dutycycle 80
    ```
  
  - Enable EDRRM by entering this command:
    
    ```
    Device# conf t
    Device (config)# ap dot11 24ghz rrm channel cleanair-event
    ```
  
  - Enable Rogue contribution by entering this command:
    
    ```
    Device# conf t
    Device (config)# ap dot11 24ghz rrm channel cleanair-event rogue-contribution
    ```

**DCA Cisco AP Load**

- **Description**—Avoid using this option to avoid frequent changes in DCA due to varying load conditions, this is disabled by default.

**Status**

- **Selected**—AP Load is disabled.
- **Unselected**—AP Load is enabled.

**CLI Option:**

- Verify the current status by entering this command:
  
  ```
  Device# show ap dot11 24ghz channel | include Load
  ```

- Enable DCA Cisco AP Load by entering this command:
  
  ```
  Device# conf t
  Device(config)# ap dot11 24ghz rrm channel load
  ```

- Disable DCA Cisco AP Load by entering this command:
Best Channel Width

- Description—Dynamic bandwidth selection selects the widest channel width with the highest client data rates and lowest channel utilization per radio. This minimizes data retries and CRC errors on the 5 GHz band while avoiding rogue APs and CleanAir Interferers.

- Status:
  - Selected—Channel width is selected as Best on both bands.
  - Unselected—Channel width is not selected as Best on both bands.

- CLI Option—Enable best channel width by entering this command:

  ```
  Device# conf t
  Device(config)# no ap dot1 24ghz rrm channel load
  ```

Flexible Radio Assignment

- Description—Flexible radio assignment (FRA) enables automatic assignment of the XOR 2.4GHz radios to other roles such as 5 GHz and Monitor.

  We recommend that you enable FRA when you have APs such as the Cisco Aironet 2800 and 3800 Series that support XOR operation.

- Status:
  - Selected—FRA is disabled.
  - Unselected—FRA is enabled.

- CLI Option: Enable FRA by entering this command:

  ```
  Device# conf t
  Device (config)# ap dot1 5ghz rrm channel dca chan-width best
  ```

High SSID Counts

- Description—Number of WLANs should be less than 4.

  We recommend limiting the number of service set identifiers (SSIDs) configured at the controller. You can configure 16 simultaneous SSIDs (per radio on each AP), but as each WLAN/SSID needs separate probe responses and beaconing, the RF pollution increases as more SSIDs are added. Furthermore, some smaller wireless stations like PDA, WiFi Phones, and barcode scanners cannot cope with a high number of basic SSID (BSSID) information. This results in lockups, reloads, or association failures. Also the more SSIDs, the more beaconing needed, so less RF time is available for real data transmits. Cisco recommends one to three SSIDs for corporate, and one SSID for high-density designs. AAA override can be leveraged for per user VLAN/ settings on a single SSID scenario.
The AP must beacon at the lowest mandatory speed set for each WLAN, in order to be able to reach the farthest stations irrespective of their location. If they can hear the AP’s beacon, it considerably reduces the general traffic.

- **Status**—Click **Manual Configuration** to manually configure the number of service set identifiers (SSIDs) configured at the controller.
  - **Selected**—Active SSID count is 4 or less.
  - **Unselected**—Active SSID count is more than 4.

- **CLI Option:**
  - Verify the number of WLANs by entering this command:
    ```
    (Cisco Controller) > show wlan summary
    ```
  - Disable unwanted WLANs by entering this command:
    ```
    Device# conf t
    Device (config)# no wlan <wlan-name> <wlan-id> <ssid-name>
    ```

### Client Band Select

- **Description**—Band selection should be enabled. However, if there is interactive traffic such as voice or video on the WLAN, do not use band selection. Clicking **Enable** turns band selection on.

  Band selection enables client radios that are capable of dual-band (2.4 and 5 GHz) operation to move to a less congested 5 GHz AP. 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 APs because of the 802.11b/g limit of three non-overlapping channels. To prevent these sources of interference and improve overall network performance, you can configure band selection on controller:

  - Band selection is enabled globally by default.
  - Band selection works by regulating probe responses to clients. It makes 5 GHz channels more attractive to clients by delaying probe responses to clients on 2.4 GHz channels.
  - Evaluate band selection for voice, particularly focusing on roaming performance. See below for further explanation.
  - Most newer model clients prefer 5 GHz by default if the 5 GHz signal of the AP is equal to or stronger than the 2.4-GHz signal.
  - Band select should be enabled for high-density designs

Also, in high-density designs, the study of available UNII-2 channels should be made. Those channels that are unaffected by Radar and also usable by the client base should be added to the RRM DCA list as usable channels.

Dual-band roaming can be slow depending on the client. If a majority of the base of voice clients exhibits a slow roaming behavior, it is more likely that the client sticks to 2.4 GHz. In this case, it has scanning issues on 5 GHz. Generally when a client decides to roam, it scans its current channel and band first. The clients generally scan for an AP that has a significantly better signal level, maybe as much as 20 dB
and/or a significantly better SNR. Failing such available connection, the client may remain with its current AP. In this case, if the CU on 2.4 GHz is low and the call quality is not poor, then disabling the selected band is acceptable. However, the preferred design is to enable band selection on 5 GHz with all data rates enabled and 6 Mbps as mandatory. Then, set the 5 GHz RRM minimum Tx power level 6 dBm higher than the average 2.4 GHz power level set by RRM.

The goal of this configuration recommendation is to enable the client to obtain a band and channel with better SNR and Tx power initially. As already stated, generally when a client decides to roam, it scans its current channel and band first. So, if the client initially joins the 5 GHz band, then it is more likely to stay on the band if there are good power levels on 5 GHz. SNR levels on 5 GHz are generally better than 2.4 GHz because 2.4 GHz has only three Wi-Fi channels and is more susceptible to interference such as Bluetooth, iBeacons, and microwave signals.

802.11k is recommended to be enabled with dual-band reporting. This enables all 11k enabled clients to have the benefit of assisted roaming. With dual-band reporting enabled, the client receives a list of the best 2.4-GHz and 5-GHz APs upon a directed request from the client. Here, the client most likely looks at the top of the list for an AP on the same channel, and then on the same band as the client is currently on. This logic reduces scan times and saves battery power. Having 802.11k enabled on the WLC does not have a downside effect for non-802.11k clients.

• Status:
  • Selected—Client band select disabled on all active WLANs.
  • Unselected—Client band select enabled on one or more active WLANs.

• CLI Option:
  • Verify Band Select by entering this command:

    (Cisco Controller) >show wlan all

  • Enable Band Select on a WLAN by entering this command:

    Device# conf t
    Device (config)# wlan <wlan-name> <wlan-id> <ssid-name>
    Device (config-wlan)# band-select

### 5GHz Low Data Rates

- **Description**—We recommend that low data rates of 6 and 9 Mbps are disabled on 5GHz for better performance.

- **Note**
  
  Low data rates should not be disabled for low density deployments where these data rates are expected to be present.

- **Status**:
  • Selected—Low data rates of 6 and 9 Mbps are disabled on 5GHz.
  • Unselected—Low data rates of 6 and 9 Mbps are enabled on 5GHz.
• CLI Option:
  • Disable 6Mbps on 5GHz by entering this command:

        Device# conf t
        Device (config)# ap dot11 5ghz rate RATE_6M disable

  • Disable 9Mbps on 5GHz by entering this command:

        Device# conf t
        Device (config)# ap dot11 5ghz rate RATE_9M disable

2.4GHz Low Data Rates

• Description—Low data rates of 1, 2, and 5.5 Mbps should be disabled on 2.4Ghz and 11 Mbps set to *not mandatory* on 2.4Ghz for better performance.

  ![-](Note) Low data rates should not be disabled for low density deployments where these data rates are expected to be present.

• Status:
  • Selected—Low data rates of 1, 2 or 5.5 Mbps are disabled on 2.4GHz or 11 Mbps is set to *not mandatory*.
  • Unselected—Low data rates of 1, 2 or 5.5 Mbps are enabled on 2.4GHz or 11 Mbps is set to *mandatory*.

• CLI Option:
  • Disable 1Mbps on 2.4GHz by entering this command:

        Device# conf t
        Device (config)# ap dot11 24ghz rate RATE_1M disable

  • Disable 2Mbps on 2.4GHz by entering this command:

        Device# conf t
        Device (config)# ap dot11 24ghz rate RATE_2M disable

  • Disable 5.5Mbps on 2.4GHz by entering this command:

        Device# conf t
        Device (config)# ap dot11 24ghz rate RATE_5_5M disable

  • Configure or disable 11Mbps on 2.4GHz by entering this command:

        Device# conf t
        Device (config)# ap dot11 24ghz rate RATE_11M {disable | supported}
Apple Devices

WLAN Configuration

• Description—Allows you to identify if the WLAN is configured with recommended L2 security, QoS, and Advanced settings for Apple devices. Application Visibility should be enabled.

• Status—Click Detailed to manually configure the L2 security, QoS, and advanced settings for Apple devices for individual, active WLANs.
  • Selected—At least one WLAN is compliant with all the recommended WLAN configurations for Apple devices.
  • Unselected—None of the active WLANs are compliant with all the recommended WLAN configurations for Apple devices.

• Recommended configurations:
  • Security—Fast Transition should be adaptive enabled or enabled. If Fast transition is enabled, the Authentication Key Management should be psk or dot1x. Layer 3 security should be none. Over the DS needs to be disabled.
  • QOS—WMM policy should be set to required.
  • Advanced—11k Neighbor List or Dual Band should be enabled. 11v BSS Transition should be enabled. WLAN Radio policy should be all or 802.11a or 802.11 a/g. mDNS should be set to gateway mode.
  • Policy—Fastlane should be set in AutoQOS. Egress and Ingress QOS SSID policy should be set to platinum.

Optimized Roaming Disabled

• Description—Optimized roaming should be disabled because Apple devices use the newer 802.11r, 802.11k, or 802.11v roaming improvement.

• Status:
  • Selected—Optimized roaming is disabled.
  • Unselected—Optimized roaming is enabled.

• CLI Option:
  • Enable optimized roaming by entering this command:

          Device# conf t
          Device(config)# ap dot11 5ghz rrm optimized-roam

  • Disable optimized roaming by entering this command:
Device# conf t
Device(config)# no ap dot11 5ghz rrm optimized-roam

5GHz EDCA Fastlane

• Description—Configuring the EDCA Profile as Fastlane improves Apple device performance on 5GHz networks.

• Status:
  • Selected—The 5GHz EDCA Profile is configured as Fastlane.
  • Unselected—The 5GHz EDCA Profile is not configured as Fastlane.

• CLI Option:
  • Enable Fastlane by entering this command:

  Device# conf t
  Device(config)# ap dot11 5ghz edca-parameters fastlane

  • Disable Fastlane by entering this command:

  Device# conf t
  Device(config)# no ap dot11 5ghz edca-parameters fastlane

5GHz Enabled

• Description—Enable the 5GHz radio to provide a faster and less interfering network for Apple devices.

• Status:
  • Selected—5GHz radio is enabled on the network.
  • Unselected—5GHz radio is disabled on the network.

5GHz MCS Rates

• Description—All the MCS Rates (0-31) should be enabled on the 5GHz networks to help improve the performance of Apple client devices.

• Status:
  • Selected—All the MCS rates are enabled on the 5GHz network.
  • Unselected—Some of the MCS rates are disabled on the 5GHz network.
PART II

Lightweight Access Points

• Country Codes, on page 71
• Sniffer Mode, on page 77
• Monitor Mode, on page 81
• Sensor Mode, on page 83
• AP Priority, on page 89
• FlexConnect, on page 91
• Data DTLS, on page 129
• Converting Autonomous Access Points to Lightweight Mode, on page 131
• AP Crash File Upload, on page 145
• Rogue per AP, on page 149
• Access Point Plug-n-Play, on page 163
• 802.11 Parameters for Cisco Access Points, on page 165
• 802.1x Support, on page 177
• Configuring CAPWAP Link Aggregation Support, on page 185
• Configuring DHCP and NAT Functionality on Root Access Point, on page 191
• OFDMA Support for 11ax Access Points, on page 193
Country Codes

- Information About Country Codes, on page 71
- Prerequisites for Configuring Country Codes, on page 71
- Configuring Country Codes (GUI), on page 72
- How to Configure Country Codes, on page 72
- Configuration Examples for Configuring Country Codes, on page 74

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 20 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 (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.

**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. |

**How to Configure Country Codes**

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> show wireless country supported</td>
<td>Displays a list of all the available country codes.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# show wireless country supported</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ap dot11 24ghz shutdown</td>
<td>Disables the 802.11b/g network.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# ap dot11 5ghz shutdown</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| Step 5 | `ap dot11 5ghz shutdown`  
*Example:*  
Device(config)# ap dot11 24ghz shutdown | Disables the 802.11a network. |
| Step 6 | `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. |
| Step 7 | `show wireless country configured`  
*Example:*  
Device# show wireless country configured | Displays the configured countries. |
| 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 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 10 | `configure terminal`  
*Example:*  
Device# configure terminal | Enters global configuration mode. |
| Step 11 | `no ap dot11 5ghz shutdown`  
*Example:*  
Device(config)# no ap dot11 5ghz shutdown | Enables the 802.11a network. |
| Step 12 | `no ap dot11 24ghz shutdown`  
*Example:*  
Device(config)# no ap dot11 24ghz shutdown | Enables the 802.11b/g network. |
| Step 13 | `end`  
*Example:*  
Device(config)# end | Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode. |
| Step 14 | `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. |
### Configuration Examples for Configuring Country Codes

#### Displaying Channel List for Country Codes: Example

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

```
Device# show wireless country channels
```

---

**Configuration Examples for Configuring Country Codes**

**Step 15**

**Command or Action:**

```plaintext
ap name cisco-ap country country_code
```

**Example:**

```
Device# ap name AP02 country US
```

**Purpose:** 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 16**

**Command or Action:**

```plaintext
ap name cisco-ap no shutdown
```

**Example:**

```
Device# ap name AP02 no shutdown
```

**Purpose:** Enables the access point.

---

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x
Lightweight Access Points

Displaying Channel List for Country Codes: Example

Auto-RF

-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
Displaying Channel List for Country Codes: Example
Sniffer Mode

- Information about Sniffer, on page 77
- Prerequisites for Sniffer, on page 77
- Restrictions on Sniffer, on page 77
- How to Configure Sniffer, on page 78
- Verifying Sniffer Configurations, on page 80
- Examples for Sniffer Configurations and Monitoring, on page 80

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.

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.

## How to Configure Sniffer

### Configuring an Access Point as Sniffer (GUI)

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Wireless &gt; Access Points.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>On the General tab, update the name of the AP.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Specify the physical location where the AP is present.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose the <strong>Admin Status</strong> as <strong>Enabled</strong> if the AP is to be in enabled state.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Choose the mode for the AP as <strong>Sniffer</strong>.</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>In the <strong>Tags</strong> section, specify the appropriate policy, site, and RF tags that you created on the <strong>Configuration</strong> &gt; <strong>Tags &amp; Profiles</strong> &gt; <strong>Tags</strong> page.</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>Click <strong>Update &amp; Apply to Device</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring an Access Point as Sniffer (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ap name ap-name mode sniffer</code></td>
<td>Configures the access point as a sniffer.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>Where, <code>ap-name</code> is the name of the Cisco lightweight access point.</td>
</tr>
<tr>
<td></td>
<td>Device&gt;ap name access1 mode sniffer</td>
<td></td>
</tr>
</tbody>
</table>
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 5GHz 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 Choose the channel from the **Sniff Channel** drop-down list.
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> ap name ap-name sniff {dot11a channel server-ip-address | dot11b channel server-ip-address | dual-band channel server-ip-address}</td>
<td>Enables sniffing on the access point.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device#ap name access1 sniff dot11b 1 9.9.48.5</td>
<td>• <em>channel</em> 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.</td>
</tr>
<tr>
<td><strong>Step 3</strong> ap name ap-name no sniff {dot11a | dot11b | dual-band}</td>
<td>Disables sniffing on the access point.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device#ap name access1 no sniff dot11b</td>
<td>• <em>server-ip-address</em> is the IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark software.</td>
</tr>
</tbody>
</table>
Verifying Sniffer Configurations

### Table 2: Commands for verifying sniffer configurations

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>**show ap name ap-name config dot11 {24ghz</td>
<td>5ghz</td>
</tr>
<tr>
<td><strong>show ap name ap-name config slot slot-ID</strong></td>
<td>Displays the sniffing configuration details. <em>slot-ID ranges from 0 to 3. All access points have slot 0 and 1.</em></td>
</tr>
</tbody>
</table>

### 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`
Monitor Mode

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 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.

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.
## Enable Monitor Mode (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables monitor mode for the access point.</td>
</tr>
<tr>
<td><code>ap name ap-name mode monitor</code></td>
<td>Enables monitor mode for the access point.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enables monitor mode for the access point.</td>
</tr>
<tr>
<td><code>Device# ap name 3602a mode monitor</code></td>
<td>Enables monitor mode for the access point.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures the access point to scan only the Dynamic Channel Assignment (DCA) channels supported by its country of operation.</td>
</tr>
<tr>
<td><code>ap name ap-name monitor tracking-opt</code></td>
<td>Configures the access point to scan only the Dynamic Channel Assignment (DCA) channels supported by its country of operation.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Configures the access point to scan only the Dynamic Channel Assignment (DCA) channels supported by its country of operation.</td>
</tr>
<tr>
<td><code>Device# ap name 3602a monitor tracking-opt</code></td>
<td>Configures the access point to scan only the Dynamic Channel Assignment (DCA) channels supported by its country of operation.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Chooses up to four specific 802.11b channels to be scanned by the access point.</td>
</tr>
<tr>
<td><code>ap name ap-name monitor dot11b [first-channel second-channel third-channel fourth-channel]</code></td>
<td>Chooses up to four specific 802.11b channels to be scanned by the access point.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Chooses up to four specific 802.11b channels to be scanned by the access point.</td>
</tr>
<tr>
<td><code>Device# ap name 3602a monitor dot11b 1 2 3 4</code></td>
<td>Chooses up to four specific 802.11b channels to be scanned by the access point.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Displays all the access points in monitor mode.</td>
</tr>
<tr>
<td>`show ap dot11 {24ghz</td>
<td>5ghz} monitor-mode summary`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Displays all the access points in monitor mode.</td>
</tr>
<tr>
<td><code>Device# show ap dot11 5ghz monitor-mode summary</code></td>
<td>Displays all the access points in monitor mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Shows configuration and statistics of 802.11a channel assignment.</td>
</tr>
<tr>
<td>`show ap dot11 {24ghz</td>
<td>5ghz} channel`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Shows configuration and statistics of 802.11a channel assignment.</td>
</tr>
<tr>
<td><code>Device# show ap dot11 5ghz channel</code></td>
<td>Shows configuration and statistics of 802.11a channel assignment.</td>
</tr>
</tbody>
</table>
### Sensor Mode

- Introduction to Sensor Mode, on page 83
- Enabling Sensor Mode, on page 83
- Verifying Sensor Mode Configuration, on page 87

#### 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](#).

#### Enabling Sensor Mode

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>ap name ap-name mode sensor</code></td>
<td>Enables sensor mode for the access point</td>
</tr>
</tbody>
</table>

**Example:**

```
Device# ap name AP4001.7A39.2E12 mode sensor
```
Enabling Sensor Mode

Note
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 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 [<transmit-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]`
Enabling Sensor Mode

- 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]
- 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>
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)*
```
AP Priority

- Failover Priority for Access Points, on page 89
- Setting AP Priority, on page 89

Failover Priority for Access Points

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

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

- You can configure your wireless network so that the backup controller embedded controller recognizes a join request from a higher-priority access point, and if necessary, disassociates a lower-priority access point as a means to provide an available port.

- Failover priority is not in effect during the regular operation of your wireless network. It takes effect only if there are more association requests after a controller an embedded controller failure than there are available backup controller ports.

- AP priority is checked while connecting to the controller embedded 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.

This section contains the following subsections:

Setting AP Priority

Note

Priority of access points ranges from 1 to 4, with 4 being the highest.
### Setting AP Priority

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>ap name ap-name priority priority</code></td>
<td>Specifies the priority of an access point.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# ap name AP44d3.ca52.48b5 priority 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>show ap config general</code></td>
<td>Displays common information for all access points.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show ap config general</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>show ap name ap-name config general</code></td>
<td>Displays the configuration of a particular access point.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show ap name AP44d3.ca52.48b5 config general</td>
<td></td>
</tr>
</tbody>
</table>
Information About FlexConnect

FlexConnect (previously known as Hybrid Remote Edge Access Point or H-REAP) is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points (AP) in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller. In the connected mode, the FlexConnect access point can also perform local authentication.
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 values only after the session timer expires.

There is no deployment restriction on the number of FlexConnect access points per location. Multiple FlexConnect groups can be defined in a single location.

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

FlexConnect access points support a 1-1 network address translation (NAT) configuration. They also support port address translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the Unicast option. FlexConnect access points also support a many-to-one NAT or PAT boundary, except when you want true multicast to operate for all centrally switched WLANs.

**Note**

Although NAT and PAT are supported for FlexConnect access points, they are not supported on the corresponding controller. Cisco does not support configurations in which the controller is behind a NAT/PAT boundary.

VPN and Point-to-Point Tunnel Protocol (PPTP) are supported for locally switched traffic if these security types are accessible locally at the access point.

FlexConnect access points support multiple SSIDs.
Workgroup bridges and Universal Workgroup bridges are supported on FlexConnect access points for locally switched clients.

FlexConnect supports IPv6 clients by bridging the traffic to local VLAN, similar to 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.

**FlexConnect Authentication Process**

When an access point boots up, it looks for a controller. If it finds one, it joins the controller, downloads the latest software image and configuration from the controller, and initializes the radio. It saves the downloaded configuration in nonvolatile memory for use in standalone mode.

---

**Note**

Once the access point is rebooted after downloading the latest controller software, it must be converted to the FlexConnect mode.

---

**Note**

802.1X is not supported on the AUX port for Cisco 2700 series APs.

---

A FlexConnect access point can learn the controller IP address in one of these ways:

- If the access point has been assigned an IP address from a DHCP server, it can discover a controller through the regular CAPWAP or LWAPP discovery process.

---

**Note**

OTAP is not supported.

---

- If the access point has been assigned a static IP address, it can discover a controller through any of the discovery process methods except DHCP option 43. If the access point cannot discover a controller through Layer 3 broadcast, we recommend DNS resolution. With DNS, any access point with a static IP address that knows of a DNS server can find at least one controller.

- If you want the access point to discover a controller from a remote network where CAPWAP or LWAPP discovery mechanisms are not available, you can use priming. This method enables you to specify (through the access point CLI) the controller to which the access point is to connect.

When a FlexConnect access point can reach the controller (referred to as the connected mode), the controller assists in client authentication. When a FlexConnect access point cannot access the controller, the access point enters the standalone mode and authenticates clients by itself.

---

**Note**

The LEDs on the access point change as the device enters different FlexConnect modes. See the hardware installation guide for your access point for information on LED patterns.

---

When a client associates to a FlexConnect access point, the access point sends all authentication messages to the controller and either switches the client data packets locally (locally switched) or sends them to the...
controller (centrally switched), depending on the WLAN configuration. With respect to client authentication (open, shared, EAP, web authentication, and NAC) and data packets, the WLAN can be in any one of the following states depending on the configuration and state of controller connectivity:

- central authentication, central switching—In this state, the controller handles client authentication, and all client data is tunneled back to the controller. This state is valid only in connected mode.

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

For the FlexConnect local switching, central authentication deployments, if there is a passive client with a static IP address, it is recommended to disable the Learn Client IP Address feature under the **WLAN > Advanced** tab.

- local authentication, local switching—In this state, the FlexConnect access point handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode.

In connected mode, the access point provides minimal information about the locally authenticated client to the controller. The following information is not available to the controller:

- Policy type
- Access VLAN
- VLAN name
- Supported rates
- Encryption cipher

Local authentication is useful where you cannot maintain a remote office setup of a minimum bandwidth of 128 kbps with the round-trip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 576 bytes. In local authentication, the authentication capabilities are present in the access point itself. Local authentication reduces the latency requirements of the branch office.

Local authentication can only be enabled on the WLAN of a FlexConnect access point that is in local switching mode.

- Notes about local authentication are as follows:
  - Guest authentication cannot be done on a FlexConnect local authentication-enabled WLAN.
  - Local RADIUS on the controller is not supported.
  - Once the client has been authenticated, roaming is only supported after the controller and the other FlexConnect access points in the group are updated with the client information.
  - Local authentication in connected mode requires a WLAN configuration.
When locally switched clients that are connected to a FlexConnect access point renew the IP addresses, on joining back, the client continues to stay in the run state. These clients are not reauthenticated by the controller.

**Note**

- authentication down, switch down—In this state, the WLAN disassociates existing clients and stops sending beacon and probe requests. This state is valid in both standalone mode and connected mode.

- authentication down, local switching—In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive. This state is valid only in standalone mode.

When a FlexConnect access point enters standalone mode, WLANs that are configured for open, shared, WPA-PSK, or WPA2-PSK authentication enter the “local authentication, local switching” state and continue new client authentications. His configuration is also correct for WLANs that are configured for 802.1X, WPA-802.1X, WPA2-802.1X, or CCKM, but these authentication types require that an external RADIUS server be configured. You can also configure a local RADIUS server on a FlexConnect access point to support 802.1X in a standalone mode or with local authentication.

Other WLANs enter either the “authentication down, switching down” state (if the WLAN was configured for central switching) or the “authentication down, local switching” state (if the WLAN was configured for local switching).

When FlexConnect access points are connected to the controller (rather than in standalone mode), the controller uses its primary RADIUS servers and accesses them in the order specified on the RADIUS Authentication Servers page or in the `config radius auth add` CLI command (unless the server order is overridden for a particular WLAN). However, to support 802.1X EAP authentication, FlexConnect access points in standalone mode need to have their own backup RADIUS server to authenticate clients.

**Note**

A controller does not use a backup RADIUS server. The controller uses the backup RADIUS server in local authentication mode.

You can configure a backup RADIUS server for individual FlexConnect access points in standalone mode by using the controller CLI or for groups of FlexConnect access points in standalone mode by using either the GUI or CLI. A backup server configured for an individual access point overrides the backup RADIUS server configuration for a FlexConnect.

When web-authentication is used on FlexConnect access points at a remote site, the clients get the IP address from the remote local subnet. To resolve the initial URL request, the DNS is accessible through the subnet's default gateway. In order for the controller to intercept and redirect the DNS query return packets, these packets must reach the controller at the data center through a CAPWAP connection. During the web-authentication process, the FlexConnect access points allow 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.

**Restrictions for FlexConnect**

- 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.
- 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 support IPv6 ACLs, neighbor discovery caching, and DHCPv6 snooping of IPv6 NDP packets.

• 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.

• When you enable local switching on WLAN 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.

• For Wi-Fi Protected Access Version 2 (WPA2) in FlexConnect standalone mode or local authentication in connected mode or CCKM fast roaming in connected mode, only Advanced Encryption Standard (AES) is supported.

• For Wi-Fi Protected Access (WPA) in FlexConnect standalone mode or local-auth in connected mode or CCKM fast-roaming in connected mode, only Temporal Key Integrity Protocol (TKIP) is supported.

• WPA2 with TKIP and WPA with AES is not supported in standalone mode, local-auth in connected mode, and CCKM fast-roaming in connected mode.

• Only open and WPA (PSK and 802.1x) authentication is supported on the Cisco Aironet 1830 Series and 1850 Series APs.

• 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.

• IPv6 RADIUS Server is not configurable for FlexConnect APs. Only IPv4 configuration is supported.
## Configuring a Site Tag

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wireless tag site <em>site-name</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless tag site default-site-tag</td>
<td></td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Configures site tag and enters site tag configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>flex-profile <em>flex-profile-name</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-site-tag)# flex-profile rr-xyz-flex-profile</td>
<td></td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Maps a flex profile to a site tag.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ap-profile <em>ap-profile</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-site-tag)# ap-profile xyz-ap-profile</td>
<td></td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Assigns an AP profile to the wireless site.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>description <em>site-tag-name</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-site-tag)# description &quot;default site tag&quot;</td>
<td></td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Adds a description for the site tag.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>no local-site</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-site-tag)# no local-site</td>
<td></td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Moves the access point to FlexConnect mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-site-tag)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Saves the configuration, exits the configuration mode, and returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>show wireless tag site summary</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show wireless tag site summary</td>
<td></td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>(Optional) Displays the summary of site tags.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a Policy Tag (CLI)

Follow the procedure given below to configure a policy tag:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wireless tag policy <em>policy-tag-name</em></td>
<td>Configures policy tag and enters policy tag configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-policy-tag)# wireless tag policy default-policy-tag</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>wlan <em>wlan-name</em> policy <em>profile-policy-name</em></td>
<td>Maps a policy profile to a WLAN profile.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-policy-tag)# wlan rr-xyz-wlan-aa policy rr-xyz-policy-1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
<td>Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-policy-tag)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show wireless tag policy summary</td>
<td>(Optional) Displays the configured policy tags.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# show wireless tag policy summary</td>
<td></td>
</tr>
</tbody>
</table>

**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 AP (GUI)

**Procedure**

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

2. To edit the configuration details of an AP, select the row for that AP.
   The Edit AP window is displayed.
### 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:

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures a wireless flex profile and enters wireless flex profile configuration mode.</td>
</tr>
<tr>
<td><code>wireless profile flex flex-profile-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless profile flex Flex-profile-1</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures an ACL policy.</td>
</tr>
<tr>
<td><code>acl-policy acl-policy-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-flex-profile)# acl-policy ACL1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to wireless flex profile configuration mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-flex-profile-acl)# exit</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures native vlan-id information.</td>
</tr>
<tr>
<td><code>native-vlan-id</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-flex-profile)# native-vlan-id 25</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Configures a VLAN.</td>
</tr>
<tr>
<td><code>vlan vlan-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-flex-profile)# vlan-name VLAN0169</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Configures an ACL for the interface.</td>
</tr>
<tr>
<td><code>acl acl-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-flex-profile-vlan)# acl ACL1</td>
</tr>
</tbody>
</table>
### Configuring FlexConnect

#### Note
The configuration tasks must be performed in the order in which they are listed here.

### 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.

```plaintext
ip dhcp pool NATIVE
   network 209.165.200.224 255.255.255.224
   default-router 209.165.200.225
   dns-server 192.168.100.167
!
ip dhcp pool LOCAL-SWITCH
   network 209.165.201.224 255.255.255.224
   default-router 209.165.201.225
   dns-server 192.168.100.167
!
interface FastEthernet1/0/1
   description Uplink port
   no switchport
   ip address 209.165.202.225 255.255.255.224
!
interface FastEthernet1/0/2
```

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td><strong>vlan-id vlan-id</strong></td>
<td>Configures VLAN information.</td>
</tr>
</tbody>
</table>

**Example:**

```plaintext
Device(config-wireless-flex-profile-vlan)# vlan-id 169
```
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

<table>
<thead>
<tr>
<th>WLAN</th>
<th>Security</th>
<th>Authentication</th>
<th>Switching</th>
<th>Interface Mapping (VLAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>WPA1+WPA2</td>
<td>Central</td>
<td>Central</td>
<td>Management (centrally switched VLAN)</td>
</tr>
<tr>
<td>Employee-local</td>
<td>WPA1+WPA2</td>
<td>Local</td>
<td>Local</td>
<td>101 (locally switched VLAN)</td>
</tr>
<tr>
<td>(PSK)</td>
<td></td>
<td>(PSK)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guest-central</td>
<td>Web authentication</td>
<td>Central</td>
<td>Central</td>
<td>Management (centrally switched VLAN)</td>
</tr>
<tr>
<td>Employee-local-auth</td>
<td>WPA1+WPA2</td>
<td>Local</td>
<td>Local</td>
<td>101 (locally switched VLAN)</td>
</tr>
</tbody>
</table>

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 check box.
Step 4  
Click Update & Apply to Device.

Configuring Local Switching in FlexConnect Mode (CLI)

**Procedure**

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

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

| Step   | Command or Action                     | Purpose                                                        |
|--------|---------------------------------------|                                                               |
| Step 1 | configure terminal                    | Enters global configuration mode.                             |
|        | Example: Device# configure terminal    |                                                                |
|        |                                       | Enters global configuration mode.                             |
| Step 2 | wireless profile policy profile-policy | Configures WLAN policy profile and enters the wireless policy  |
|        | Example: Device(config)# wireless      | configuration mode.                                           |
|        | profile policy rr-xyz-policy-1         | Configures WLAN policy profile and enters the wireless policy  |
|        |                                       | configuration mode.                                           |
| Step 3 | central switching                     | Configures the WLAN for central switching.                    |
|        | Example: Device(config-wireless-policy)| Configures the WLAN for central switching.                    |
|        | # central switching                   | Configures the WLAN for central switching.                    |
| Step 4 | end                                    | Returns to privileged EXEC mode. Alternatively, you can also   |
|        | Example: Device(config)# end           | press Ctrl-Z to exit global configuration mode.               |
|        |                                       | 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 the Configuring a Site Tag (CLI), on page 19

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Tags &amp; Profiles &gt; Policy.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Policy Profile page, select a policy profile name. The Edit Policy Profile window is</td>
</tr>
<tr>
<td></td>
<td>displayed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the General tab, deselect Central Authentication check box.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Update &amp; Apply to Device.</td>
</tr>
</tbody>
</table>
**Configuring an Access Point for Local Authentication on a WLAN (CLI)**

**Procedure**

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

**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 103.

In the example scenarios (see Configuring the Controller for FlexConnect, on page 103), 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 allotted 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

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

| **Step 2** | |
| wireless profile flex flex-profile-name | Configures a wireless flex profile and enters wireless flex profile configuration mode. |
| **Example:** | |
| Device(config)# wireless profile flex test | |

| **Step 3** | |
| fallback-radio-shut | Enables radio interface shutdown. |
| **Example:** | |
| Device(config-wireless-flex-profile)# fallback-radio-shut | |

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

| **Step 5** | |
| show wireless profile flex detailed flex-profile-name | (Optional) Displays detailed information about the selected profile. |
| **Example:** | |
| Device# show wireless profile flex detailed test | |
Flex AP Local Authentication on AP (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 Profile** window that is displayed, click the **Local Authentication** tab.

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 on AP (CLI)

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa new-model</td>
<td>Creates a AAA authentication model.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>2</td>
<td>aaa session-id common</td>
<td>Ensures that all the session IDs information that is sent out from the RADIUS group for a given call are identical.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# aaa session-id common</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>dot1x system-auth-control</td>
<td>Enables system authorization control for the RADIUS group.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# dot1x system-auth-control</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>eap profile name</td>
<td>Creates an EAP profile.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# eap profile aplocal-test</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>method fast</td>
<td>Configures the FAST method on the profile.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-eap-profile)# method fast</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>exit</td>
<td>Returns to configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-radius-server)# exit</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>wireless profile flex flex-profile</td>
<td>Configures the flex policy.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless profile flex default-flex-profile</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>local-auth ap eap-fast name</td>
<td>Configures EAP-FAST profile details.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-flex-profile)# local-auth ap eap-fast aplocal-test</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>local-auth ap leap</td>
<td>Configures the LEAP method.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-flex-profile)# local-auth ap leap</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>local-auth ap peap</td>
<td>Configures the PEAP method.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-flex-profile)# local-auth ap peap</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>local-auth ap username username</td>
<td>Configures username and password.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-flex-profile)# local-auth ap username test1 test1</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>aaa new-model</strong></td>
<td>Creates a AAA authentication model.</td>
</tr>
<tr>
<td><strong>no shutdown</strong></td>
<td>Enables the configuration.</td>
</tr>
<tr>
<td><strong>no central authentication</strong></td>
<td>Disables central (controller) authentication.</td>
</tr>
<tr>
<td><strong>wireless profile policy policy-profile</strong></td>
<td>Configures profile policy.</td>
</tr>
<tr>
<td><strong>shutdown</strong></td>
<td>Disables the policy profile.</td>
</tr>
<tr>
<td><strong>local-auth ap username username password</strong></td>
<td>Configures another username and password.</td>
</tr>
<tr>
<td><strong>exit</strong></td>
<td>Returns to configuration mode.</td>
</tr>
</tbody>
</table>

### Command or Action Details

**Step 1**

Device(config)# aaa new-model

**Step 2**

Device(config)# local-auth ap username test2 test2

**Step 3**

Device(config)# exit

**Step 4**

Device(config)# wireless profile policy default-policy-profile

**Step 5**

Device(config-wireless-policy)# shutdown

**Step 6**

Device(config)# no central authentication

**Step 7**

Device(config)# vlan-id 54

**Step 8**

Device(config)# no shutdown
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>aaa session-id common</td>
<td>Ensures that all the session ID's information that is sent out, from the RADIUS group for a given call are identical.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# aaa session-id common</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>dot1x system-auth-control</td>
<td>Enables the system authorization control for the RADIUS group.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# dot1x system-auth-control</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>radius server server-name</td>
<td>Specifies the RADIUS server name.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# radius server Test-SERVER1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>address {ipv4</td>
<td>ipv6} ip address {auth-port port-number</td>
</tr>
<tr>
<td></td>
<td>acct-port port-number}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: 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</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>key string</td>
<td>Specifies the authentication and encryption key used between the device and the RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-radius-server)# key test123</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>radius server server-name</td>
<td>Specifies the RADIUS server name.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# radius server Test-SERVER2</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>address {ipv4</td>
<td>ipv6} ip address {auth-port port-number</td>
</tr>
<tr>
<td></td>
<td>acct-port port-number}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>9</td>
<td>key <em>string</em></td>
<td>Specifies the authentication and encryption key used between the device and the RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-radius-server)# key test113</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>exit</td>
<td>Returns to configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-radius-server)# exit</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>aaa group server radius server-group</td>
<td>Creates a RADIUS server group identification.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# aaa group server radius aaa_group_name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td>server-group refers to the server group name. The valid range is from 1 to 32 alphanumeric characters.</td>
</tr>
<tr>
<td>12</td>
<td>exit</td>
<td>Exits from RADIUS server-group configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-sg-radius)# exit</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>radius server server-name</td>
<td>Specifies the RADIUS server name.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# radius server Test-SERVER1</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>radius server server-name</td>
<td>Specifies the RADIUS server name.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-radius-server)# radius server Test-SERVER2</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>exit</td>
<td>Exit from RADIUS server configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-radius-server)# exit</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>wireless profile flex flex-profile</td>
<td>Creates a new flex policy.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless profile flex default-flex-profile</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>local-auth radius-server-group server-group</td>
<td>Configures the authentication server group name.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-flex-profile)# local-auth radius-server-group aaa_group_name</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>exit</td>
<td>Returns to configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>---------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-flex-profile)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 19</strong> wireless profile policy policy-profile</td>
<td>Configures a WLAN policy profile.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless profile policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>default-policy-profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 20</strong> shutdown</td>
<td>Disables a policy profile.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# shutdown</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 21</strong> no central authentication</td>
<td>Disables central (controller) authentication.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# no central authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 22</strong> vlan-id vlan-id</td>
<td>Configures a VLAN name or VLAN Id.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# vlan-id 54</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 23</strong> no shutdown</td>
<td>Enables the configuration.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# no shutdown</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## 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.
## Configuring a Wireless Profile Policy and NAT-PAT

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

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wlan wlan-name wlan-id SSID-name</td>
<td>Enters the WLAN configuration sub-mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wlan wlan-demo 1 ssid-demo</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you have already configured WLAN, enter wlan wlan-name command.</td>
</tr>
<tr>
<td><strong>Step 3</strong> no shutdown</td>
<td>Shut down the WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wlan)# no shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wlan)# end</td>
<td></td>
</tr>
</tbody>
</table>
### Mapping a WLAN to a Policy Profile

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>wireless tag policy policy-tag-name</code></td>
<td>Configures a policy tag and enters policy tag configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# wireless tag policy demo-tag</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Site Tag

Follow the procedure given below to configure a site tag:

**Procedure**

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

### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
## 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 WLAN using the (ipv4 dhcp required) command. This ensures that the client that is associating with the split WLAN does DHCP.

### Configuring Split Tunneling for a WLAN or Remote LAN

#### Defining an Access Control List for Split Tunneling

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

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Linking an ACL Policy to the Defined ACL

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless profile flex flex-profile</td>
<td>Configures the Flex profile and enters flex profile configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless profile flex flex-profile</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> acl-policy acl policy name</td>
<td>Configures an ACL policy for the defined ACL.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-flex-profile)# acl-policy split_mac_acl</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-flex-profile)# end</td>
<td></td>
</tr>
</tbody>
</table>
## Creating a WLAN

Follow the procedure given below to create a WLAN.

### Procedure

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

## 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>wireless profile policy profile-policy</code></td>
<td>Configures a WLAN policy profile and enters wireless policy configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless profile policy split-tunnel-enabled-policy</td>
<td></td>
</tr>
</tbody>
</table>
### Mapping WLAN to a Policy Profile

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

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless tag policy <em>policy-tag-name</em></td>
<td>Configures a policy tag and enters policy tag configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless tag policy split-tunnel-enabled-tag</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Site Tag

Follow the procedure given below to configure a site tag:

**Procedure**

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

### 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.
### 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 VLAN0-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.

### Configuring VLAN-based Central Switching (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ap ethernet-mac-address</td>
<td>Configures an AP and enters ap tag configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ap 188b.9dbe.6eac</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>policy-tag policy-tag-name</td>
<td>Maps a policy tag to an AP.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-tag)# policy-tag</td>
<td></td>
</tr>
<tr>
<td></td>
<td>split-tunnel-enabled-tag</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>site-tag site-tag-name</td>
<td>Maps a site tag to an AP.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-tag)# site-tag flex-site</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-tag)# end</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>wireless profile policy</strong> <em>profile-policy</em>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config)# wireless profile policy default-policy-profile</td>
<td>Configures a wireless policy profile.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>no central switching</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# no central switching</td>
<td>Configures a WLAN for local switching.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>no central dhcp</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# no central dhcp</td>
<td>Configures local DHCP mode, where the DHCP is performed in an AP.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>central authentication</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# central authentication</td>
<td>Configures a WLAN for central authentication.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>aaa-override</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# aaa-override</td>
<td>Configures AAA policy override.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>flex vlan-central-switching</strong>&lt;br&gt;<strong>Example:</strong></td>
<td>Configures VLAN-based central switching.</td>
</tr>
</tbody>
</table>
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.

Configuring OfficeExtend Access Points

Follow the procedure given below to configure OfficeExtend access points.

Procedure

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

| **Step 2** |         |
| wireless profile flex flex-profile-name | Configures a wireless flex profile and enters wireless flex profile configuration mode. |
| Example: |         |
| Device(config)# wireless profile flex test |         |

| **Step 3** |         |
| office-extend | Enables the OfficeExtend AP mode for a flexconnect AP. |
| Example: |         |
Disabling OfficeExtend Access Point

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless profile flex flex-profile-name</td>
<td>Configures a wireless flex profile and enters wireless flex profile configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless profile flex test</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>no office-extend</td>
<td>Disables OfficeExtend AP mode for a flexconnect AP.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-flex-profile)# no office-extend</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exits configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-flex-profile)# end</td>
<td></td>
</tr>
</tbody>
</table>

Clearing Personal SSID from an OfficeExtend Access Point

To clear the personal SSID from an access point, run the following command:
### 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
  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 ARP is the most common method for learning about other routes, enables an Ethernet host with no routing information to communicate with hosts on other networks or subnets. The host assumes that all hosts are on
the same local Ethernet and that they can use ARP to learn their MAC addresses. If a Device receives an ARP request for a host that is not on the same network as the sender, the Device evaluates whether it has the best route to that host. If it does, it sends an ARP reply packet with its own Ethernet MAC address, and the host that sent the request sends the packet to the Device, which forwards it to the intended host. Proxy ARP treats all networks as if they are local, and performs ARP requests for every IP address.

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

# Enabling Proxy ARP for FlexConnect APs

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

## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless profile flex flex-policy</td>
<td>Configures WLAN policy profile and enters wireless flex profile configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# wireless profile flex flex-test</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> arp-caching</td>
<td>Enables ARP caching.</td>
</tr>
<tr>
<td>Example: Device(config-wireless-flex-profile)# arp-caching</td>
<td></td>
</tr>
<tr>
<td>Note: Use the no arp-caching command to disable ARP caching.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device(config-wireless-flex-profile)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>section wireless profile flex</td>
</tr>
<tr>
<td>Example: Device# show running-config</td>
<td>section wireless profile flex</td>
</tr>
<tr>
<td><strong>Step 6</strong> show wireless profile flex detailed flex-profile-name</td>
<td>(Optional) Displays detailed information of the flex profile.</td>
</tr>
<tr>
<td>Example: Device# show wireless profile flex detailed flex-test</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> show arp summary</td>
<td>(Optional) Displays ARP summary.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Enabling Proxy ARP for FlexConnect APs

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device# show arp summary</code></td>
<td></td>
</tr>
</tbody>
</table>
Data DTLS

- Information About Data Datagram Transport Layer Security, on page 129
- Configuring Data DTLS (GUI), on page 129
- Configuring Data DTLS (CLI), on page 130

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.

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.
Configuring Data DTLS (CLI)

Follow the procedure given below to enable DTLS data encryption for the access points on the controller:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ap profile ap-profile</code></td>
<td>Configures an AP profile and enters AP profile configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# ap profile test-ap-profile</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You can use the default AP profile (default-ap-profile) or create a named AP profile, as shown in the example.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>link-encryption</code></td>
<td>Enables link encryption based on the profile. Answer yes, when the system prompts you with this message: Enabling link-encryption will reboot the APs with link-encryption. Are you sure you want to continue? (y/n) [y]:</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-ap-profile)# link-encryption</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-ap-profile)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>show wireless dtls connections</code></td>
<td>(Optional) Displays the DTLS session established for the AP that has joined this controller.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# show wireless dtls connections</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>show ap link-encryption</code></td>
<td>(Optional) Displays the link encryption-related statistics (whether link encryption is enabled or disabled) counter received from the AP.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# show ap link-encryption</td>
<td></td>
</tr>
</tbody>
</table>
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.
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.

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

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.

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.

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.

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.

Cisco Wave2 APs support strings with length up to 256 characters only.
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 display the MAC addresses of converted access points on information pages in the controller GUI:

- On the AP Summary window, the controller lists the Ethernet MAC addresses of the converted access points.
- On the AP Detail window, the controller lists the BSS MAC addresses and Ethernet MAC addresses of the converted access points.
- On the Radio Summary 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.

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)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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)

<table>
<thead>
<tr>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
</tr>
</tbody>
</table>
| **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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ap auth-list ap-policy authorize-ap</td>
<td>Configures an access point authorization</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>policy.</td>
</tr>
<tr>
<td>Device(config)# <code>ap auth-list ap-policy authorize-ap</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> username <code>user_name</code> mac <code>[aaa attribute</code></td>
<td>(Optional) Configures the MAC address of an</td>
</tr>
<tr>
<td>list <code>list_name</code>]</td>
<td>access point locally.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# <code>username aaa.bbb.ccc</code> mac <code>aaa attribute list attrlist</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> aaa new-model</td>
<td>Enables new access control commands and</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>functions.</td>
</tr>
<tr>
<td>Device(config)# <code>aaa new-model</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> aaa authorization credential-download</td>
<td>Downloads EAP credentials from the local</td>
</tr>
<tr>
<td>(auth_list</td>
<td>default) local</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# <code>aaa authorization credential-download auth_download local</code></td>
<td></td>
</tr>
</tbody>
</table>
### Authorizing Access Points Using RADIUS Server (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> radius server *server-name*</td>
<td>Enters RADIUS server configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# radius server ise</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> address (ipv4</td>
<td>ipv6) radius-server-ipv4-address-or-name auth-port udp-port-auth-server acct-port udp-port-acct-server</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Device(config-radius-server)# address ipv4 224.0.0.1 auth-port 1645 acct-port 1646</td>
<td>Sets a clear text encryption key for the RADIUS authentication server.</td>
</tr>
<tr>
<td><strong>Step 5</strong> key 0 cisco</td>
<td>Reverts to the Privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Reverts to the Privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> aaa group server radius server-group</td>
<td>Configures RADIUS server group definition.</td>
</tr>
<tr>
<td><strong>Step 8</strong> server name ise</td>
<td>Configures the RADIUS server name.</td>
</tr>
<tr>
<td><strong>Step 9</strong> ip radius source-interface vlan</td>
<td>Configures interface for source address in RADIUS packets.</td>
</tr>
<tr>
<td><strong>Step 10</strong> exit</td>
<td>Reverts to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 11</strong> aaa authorization network default group default-server-group local</td>
<td>Sets the authorization method to local.</td>
</tr>
<tr>
<td><strong>Step 12</strong> aaa authorization credential-download default group default-server-group local</td>
<td>Configures local database to download EAP credentials from the local, RADIUS, or LDAP server.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>no ap reset-button</td>
<td>Disables the Reset buttons on all converted access points that are associated to the device.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# no ap reset-button</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>ap name cisco_ap reset-button</td>
<td>Enables the Reset button on the converted access point that you specify.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# ap name AP02 reset-button</td>
<td></td>
</tr>
</tbody>
</table>

Monitoring the AP Crash Log Information

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

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
How to Configure a Static IP Address on an Access Point

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

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap name Cisco_AP static-ip ip-address static_ip_address netmask static_ip_netmask gateway static_ip_gateway</td>
<td>Configures a static IP address on the access point. This command contains the following keywords and arguments:</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# ap name AP03 static-ip ip-address 9.9.9.16 netmask 255.255.0.0 gateway 9.9.9.2</td>
<td></td>
</tr>
</tbody>
</table>

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 can configure the DNS server IP address and domain name. You must perform Steps 3 and Step 4 after the access points reboot.
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><em>enable</em></td>
<td>Example: Device# enable</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>configure terminal</em></td>
<td>Example: Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures a DNS server so that a specific access point or all access points can discover the device using DNS resolution.</td>
</tr>
<tr>
<td><em>ap static-ip name-server nameserver_ip_address</em></td>
<td>Example: Device(config)# ap static-ip name-server 10.10.10.205</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To undo the DNS server configuration, enter the <code>no ap static-ip name-server nameserver_ip_address</code> command.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Configures the domain to which a specific access point or all access points belong.</td>
</tr>
<tr>
<td><em>ap static-ip domain static_ip_domain</em></td>
<td>Example: Device(config)# ap static-ip domain domain1</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To undo the domain name configuration, enter the <code>no ap static-ip domain static_ip_domain</code> command.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><em>end</em></td>
<td>Example: Device(config)# end</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Displays the IP address configuration for the access point.</td>
</tr>
<tr>
<td><em>show ap name Cisco_AP config general</em></td>
<td>Example: Device# show ap name AP03 config general</td>
</tr>
</tbody>
</table>

---

### Configuring a Static IP Address on an Access Point (GUI)

**Procedure**

1. **Step 1** Choose **Configuration** > **Wireless** > **Access Points**.
2. **Step 2** On the **All Access Points** section, click on an **AP Name**.
3. **Step 3** In the **Edit AP** window that is displayed, go to the **IP Config** section.
4. **Step 4** Select the **Static IP (IPv4/IPv6)** check box. This activates the static IP details pane.
5. **Step 5** Enter the **Static IP**, **Netmask**, **Gateway**, and **DNS IP Address**.
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>[no] ap auth-list ap-policy authorize-ap profile-name</td>
<td>Configures an AP authorization policy.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# ap auth-list ap-policy authorize-ap</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>show ap auth-list value-in-dBm</td>
<td>Shows the status of AP MAC authorization.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# show ap auth-list</td>
<td></td>
</tr>
</tbody>
</table>

### Sample Configuration

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 e4c72281151a 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 can be alphanumeric and must have characters in lowercase; spaces or special characters are not allowed. 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Configuration &gt; Tags &amp; Profiles &gt; AP Join.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the name of the AP Join Profile or click Add to create a new one.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Add/Edit AP Join Profile window that is displayed, click the CAPWAP tab and then click the Advanced tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Check the Enable VLAN Tagging check box to enable VLAN tagging for the AP Join Profile.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Update &amp; Apply to Device.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>ap name ap-name vlan-tag vlan-id</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# ap name AP1 vlan-tag 12</td>
</tr>
<tr>
<td></td>
<td>Device# ap name AP1 no vlan-tag</td>
</tr>
<tr>
<td></td>
<td>Configures VLAN tagging for a non-bridge AP. Use the no form of this command to disable the configuration.</td>
</tr>
</tbody>
</table>
### Configuring Ethernet VLAN Tagging on Access Points (CLI)

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ap vlan-tag vlan-id</code></td>
<td>Configure VLAN tagging for all nonbridge APs. Use the <code>no</code> form of this command to disable the configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# ap vlan-tag 1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# ap no vlan-tag</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show ap config general</code></td>
<td>(Optional) Shows the common information of all the APs.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show ap config general</td>
<td></td>
</tr>
</tbody>
</table>
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:

- In case of a device failure—A system report is generated on the member that failed.
- In case of a switchover—System reports are generated only on high availability (HA) members. Reports are not generated for non-HA members.

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 switch goes down to ROMMON/bootloader.
Except for the full core and trace logs, everything else is a text file.

### Crashinfo Files

By default, the system report file is generated and saved in the /crashinfo directory. If it cannot be saved to the crashinfo partition because of lack of space, it will be saved to the /flash directory.

To display the files, enter the `dir crashinfo:` command. The following is a sample output of a crashinfo directory:

```
Switch#dir crashinfo:
Directory of crashinfo:/
46553 drwx 1024 Jun 29 2015 14:52:09 +00:00 ap_crash
12 -rw- 0 Jan 1 1970 00:00:11 +00:00 koops.dat
11 -rw- 0 Mar 22 2013 07:50:30 +00:00 deleted_crash_files
13 -rw- 594269 Mar 22 2013 07:50:30 +00:00 crashinfo_platform_mgr_20130322-075017-UTC
14 -rw- 44 Sep 9 2015 09:28:47 +00:00 last_crashinfo
15 -rw- 355 Sep 9 2015 09:29:31 +00:00 last_systemreport_log
16 -rw- 105753 Mar 22 2013 07:50:47 +00:00 system-report_1_20130322-075017-UTC.gz
17 -rw- 39 Sep 9 2015 09:29:31 +00:00 last_systemreport
18 -rw- 585996 Mar 22 2013 08:01:58 +00:00 crashinfo_platform_mgr_20130322-080144-UTC
19 -rw- 105065 Mar 22 2013 08:02:15 +00:00 system-report_1_20130322-080144-UTC.gz
20 -rw- 3426209 Sep 9 2015 06:49:12 +00:00 crashinfo_iosd_20150909-064754-UTC
21 -rw- 9540376 Sep 9 2015 06:49:13 +00:00 fullcore_iosd_20150909-064754-UTC
22 -rw- 469476 Sep 9 2015 06:49:56 +00:00 system-report_1_20150909-064754-UTC.gz
23 -rw- 3425350 Sep 9 2015 09:28:47 +00:00 crashinfo_iosd_20150909-092728-UTC
24 -rw- 953553 Sep 9 2015 09:28:47 +00:00 fullcore_iosd_20150909-092728-UTC
25 -rw- 459709 Sep 9 2015 09:29:28 +00:00 system-report_1_20150909-092728-UTC.gz
26 -rw- 0 Sep 22 2015 11:11:33 +00:00 tracelogs.J8C

50601 drwx 10240 Oct 28 2015 22:42:50 +00:00 tracelogs

248354816 bytes total (204800000 bytes free)
```

The system report contains all available trace files since system boot. In the case of WNCD trace files, if the number of trace files generated since system boot is greater than 400. In addition to other process trace files, only 400 latest WNCD trace files are added to the system report.

System reports are located in the crashinfo directory in the following format:

```
system-report_[switch number]_[date]-[timestamp]-UTC.gz
```

After a switch crashes, check for a system report file. The name of the most recently generated system report file is stored in the last_systemreport file under the crashinfo directory. The system report and crashinfo files assist Cisco Technical Assistance Center while troubleshooting issues.

### Note

It is important to clear the system reports or trace archives from the flash or crashinfo directory after they are copied out in order to have space available for trace logs and other purposes.
## Configuring AP Crash File Upload (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>enable</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device# enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>ap name</strong> <em>ap-name</em> <strong>crash-file get-crash-data</strong></td>
<td>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.</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>ap name</strong> <em>ap-name</em> <strong>crash-file get-radio-core-dump slot</strong> {0</td>
<td>1}</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>ap name</strong> <em>ap-name</em> <strong>core-dump tftp-ip crash-file uncompress</strong></td>
<td>Uploads the AP crash coredump file to the given TFTP location.</td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>show ap crash-file</strong></td>
<td>Verifies whether the crash file is downloaded to the device.</td>
</tr>
</tbody>
</table>
Configuring AP Crash File Upload (CLI)
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 containsthe following parameters – CAPWAPIIPv4/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
Click the Add button. The Add AP Join Profile screen appears.

Step 3
Click the General tab.

Step 4
Enter a name in the Name field and a description for the AP join profile in the Description field.

Step 5
Select the LED State checkbox to set the LED state of all APs connected to the device to blink so that the APs are easily located.

Step 6
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 7
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 CAPWAPjoin request to the device. The device sends a CAPWAPjoin 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. When the access point joins the device, the device manages its configuration, firmware, control transactions, and data transactions.

Step 8
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.
Configure Fast Heartbeat Timeout to assist AP in sending primary discovery request periodically to the configured backup controllers along with the primary, secondary, and tertiary-base controllers.

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.

• 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 9

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.

c. From the **Power Injector Type** drop-down list, choose power injector type from the following options:
   - Installed—If you want the AP to examine and remember the MAC address of the currently connected switch port. (This selection assumes that a power injector is connected.)
   - Override—To enable the AP to operate in high-power mode without first verifying a matching MAC address.

d. In the **Injector Switch MAC** field, enter the MAC address of the switch.

e. Enter the relevant country code. The country code enables you to specify a particular country of operation (such as FR for France or ES for Spain).

f. From the **EAP Type** drop-down list, choose the EAP type as EAP-FAST, EAP TLS, or EAP-PEAP.

g. From the **AP Authorization Type** drop-down list, choose the type as either CAPWAP DTLS + or CAPWAP DTLS.

h. In the **Client Statistics Reporting Interval** section, enter the interval for 5 GHz and 2.4 GHz radios in seconds.

i. Check the **Enable** check box to enable extended module.

j. From the **Profile Name** drop-down list, choose a profile name for mesh.

k. 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 10**  
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.
Configure an AP Profile

Follow the procedure given below to configure an AP profile:

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. Enter the group NAS ID. Network Access Server identifier (NAS-ID) is sent to the RADIUS server by the controller through an authentication request to classify users to different groups so that the RADIUS server can send a customized authentication response.
c. Click Save & Apply to Device.

Step 11 In the Rogue AP tab, check the Rogue Detection check box to enable rogue detection.
Step 12 In the Rogue Detection Minimum RSSI field, enter the RSSI value.
Step 13 In the Rogue Detection Transient Interval field, enter the transient interval value.
Step 14 In the Rogue Detection Report Interval field, enter the report interval value.
Step 15 Check the Rogue Containment Automatic Rate Selection check box to enable rogue containment automatic rate selection.
Step 16 Check the Auto Containment on FlexConnect Standalone check box to enable the feature.
Step 17 Click Save & Apply to Device.
## Proceedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ap profile ap-profile</td>
<td>Configures an AP profile and enters the AP profile configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ap profile xyz-ap-profile</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>description ap-profile-name</td>
<td>Adds a description for the AP profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-profile)# description &quot;xyz ap profile&quot;</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>rogue detection enable</td>
<td>Enables rogue detection for individual access points.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-profile)# rogue detection enable</td>
<td>Rogue detection is enabled by default. Use this command if rogue detection is disabled.</td>
</tr>
<tr>
<td>5</td>
<td>rogue detection report-interval interval</td>
<td>Specifies the time interval, in seconds, at which APs should send the rogue detection report to the controller.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-profile)# rogue detection report-interval 12</td>
<td>The default value for interval is 10.</td>
</tr>
<tr>
<td>6</td>
<td>rogue detection min-rssi rssi</td>
<td>Specifies the minimum RSSI value that rogues should have for APs to detect them.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-profile)# rogue detection min-rssi -128</td>
<td>The minimum RSSI value is –128.</td>
</tr>
<tr>
<td>7</td>
<td>rogue detection min-transient-time transient</td>
<td>Specifies the time interval at which rogues have to be consistently scanned for by APs after the first time the rogues are scanned.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-profile)# rogue detection min-transient-time 120</td>
<td>The lowest value for minimum transient time is 0.</td>
</tr>
<tr>
<td>8</td>
<td>rogue detection containment flex-connect</td>
<td>Sets the auto containment options for standalone FlexConnect access points.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-profile)# rogue detection containment flex-connect</td>
<td>By default, this option is disabled.</td>
</tr>
<tr>
<td>9</td>
<td>rogue detection containment auto-rate</td>
<td>Sets the auto rate for containment of rogues.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-profile)# rogue detection containment auto-rate</td>
<td>By default, auto-rate is disabled.</td>
</tr>
</tbody>
</table>
Define a Wireless Site Tag and Assign an AP Profile (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Tags &amp; Profiles &gt; Tags.</td>
<td>Enterstheglobalconfigurationmode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Tags page, click the Site tab and click Add.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Add Site Tag window, enter the name in the name field.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose the AP profile from the AP Join Profile drop-down list.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save &amp; Apply to Device.</td>
<td></td>
</tr>
</tbody>
</table>

Define a Wireless Site Tag and Assign an AP Profile (CLI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless tag sitesite-tag</td>
<td>Enters the wireless site tag configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless tag site default-site-tag</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ap-profile ap-profile</td>
<td>Assigns an AP profile to the wireless site.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-site-tag)# ap-profile xyz-ap-profile</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
<td>Returns to the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-site-tag)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Associating Wireless Tag to an AP (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Tags &amp; Profiles &gt; Tags.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Click AP tab to configure the following:</td>
<td></td>
</tr>
<tr>
<td>• Tag Source</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• 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)

Follow 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 ap mac-address</td>
<td>Configures Cisco APs and enters the ap configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# ap F866.F267.7DFB</td>
<td></td>
</tr>
<tr>
<td>Step 3 site-tag site-tag-name</td>
<td>Maps a wireless site tag to the AP.</td>
</tr>
<tr>
<td>Example: Device(config-ap-tag)# site-tag sitetag1</td>
<td></td>
</tr>
</tbody>
</table>

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.

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 4: Rogue Detection: Predefined Levels**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Critical</th>
<th>High</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cleanup Timer</td>
<td>3600</td>
<td>1200</td>
<td>240</td>
</tr>
<tr>
<td>AAA Validate Clients</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Adhoc Reporting</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Monitor-Mode Report Interval</td>
<td>10 seconds</td>
<td>30 seconds</td>
<td>60 seconds</td>
</tr>
<tr>
<td>Minimum RSSI</td>
<td>-128 dBm</td>
<td>-80 dBm</td>
<td>-80 dBm</td>
</tr>
<tr>
<td>Transient Interval</td>
<td>600 seconds</td>
<td>300 seconds</td>
<td>120 seconds</td>
</tr>
<tr>
<td>Auto Contain</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Works only on Monitor Mode APs.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Contain Level</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Auto Contain Same-SSID</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Auto Contain Valid Clients on Rogue AP</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Auto Contain Adhoc</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Containment Auto-Rate</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Validate Clients with CMX</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Containment FlexConnect</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>RLDP</td>
<td>Monitor-AP if RLDP scheduling is disabled.</td>
<td>Monitor-AP if RLDP scheduling is disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Setting Rogue Detection Security-level

Follow the procedure given below to set the rogue detection security-level:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wireless wps rogue security-level custom</code></td>
<td>Configures rogue detection security level as custom.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless wps rogue security-level custom</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>wireless wps rogue security-level low</code></td>
<td>Configures rogue detection security level for basic rogue detection setup for small-scale deployments.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless wps rogue security-level low</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>wireless wps rogue security-level high</code></td>
<td>Configures rogue detection security level for rogue detection setup for medium-scale deployments.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless wps rogue security-level high</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>wireless wps rogue security-level critical</code></td>
<td>Configures rogue detection security level for rogue detection setup for highly sensitive deployments.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless wps rogue security-level critical</td>
<td></td>
</tr>
</tbody>
</table>

### 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 DNA Center and other third-party infrastructure.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>network-assurance enable</td>
<td>Enables wireless service assurance.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# network-assurance enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>wireless wps rogue network-assurance enable</td>
<td>Enables wireless service assurance for rogue devices. This ensures that the WSA rogue events are sent to the event queue.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# wireless wps rogue network-assurance enable</td>
<td></td>
</tr>
</tbody>
</table>

**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 : 2
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.
Access Point Plug-n-Play

- Overview of Access Point Plug-n-Play, on page 163
- Provisioning AP from PnP Server, on page 163
- Verifying AP Tag Configuration, on page 164

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:

```bash
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:

```bash
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:

```plaintext
Device# show ap tag summary
Number of APs: 5
```

<table>
<thead>
<tr>
<th>AP Name</th>
<th>AP Mac</th>
<th>Site Tag Name</th>
<th>Policy Tag Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>d42c.4482.6102</td>
<td>d42c.4482.6102</td>
<td>default-site-tag</td>
<td>default-policy-tag</td>
</tr>
<tr>
<td>default-rf-tag</td>
<td>No</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>00c1.64d8.6af0</td>
<td>00c1.64d8.6af0</td>
<td>named-site-tag</td>
<td>named-policy-tag</td>
</tr>
<tr>
<td>named-rf-tag</td>
<td>No</td>
<td>AP</td>
<td></td>
</tr>
</tbody>
</table>

The details in the second row reflect the tag source coming from a PNP server.

---

Note: The following examples show how to verify the AP tag configuration:

```plaintext
Device# show ap tag summary
Number of APs: 5
```

<table>
<thead>
<tr>
<th>AP Name</th>
<th>AP Mac</th>
<th>Site Tag Name</th>
<th>Policy Tag Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>d42c.4482.6102</td>
<td>d42c.4482.6102</td>
<td>default-site-tag</td>
<td>default-policy-tag</td>
</tr>
<tr>
<td>default-rf-tag</td>
<td>No</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>00c1.64d8.6af0</td>
<td>00c1.64d8.6af0</td>
<td>named-site-tag</td>
<td>named-policy-tag</td>
</tr>
<tr>
<td>named-rf-tag</td>
<td>No</td>
<td>AP</td>
<td></td>
</tr>
</tbody>
</table>

The details in the second row reflect the tag source coming from a PNP server.
### 2.4-GHz Radio Support

**Configuring 2.4-GHz Radio Support for the Specified Slot Number**

**Before you begin**

The term 802.11b radio or 2.4-GHz radio will be used interchangeably.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# enable</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>ap name ap-name dot11 24ghz slot 0 SI</code></td>
<td>Enables Spectrum Intelligence (SI) for the dedicated 2.4-GHz radio hosted on slot 0 for a specific access point. Here, 0 refers to the Slot ID.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 SI</code></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 3    | `ap name ap-name dot11 24ghz slot 0 antenna {ext-ant-gain antenna_gain_value | selection [internal | external]}` | 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). |
| 4    | `ap name ap-name dot11 24ghz slot 0 beamforming` | Configures beamforming for the 2.4-GHz radio hosted on slot 0 for a specific access point. |
| 5    | `ap name ap-name dot11 24ghz slot 0 channel {channel_number | auto}` | Configures advanced 802.11 channel assignment parameters for the 2.4-GHz radio hosted on slot 0 for a specific access point. |
| 6    | `ap name ap-name dot11 24ghz slot 0 cleanair` | Enables CleanAir for 802.11b radio hosted on slot 0 for a specific access point. |
| 7    | `ap name ap-name dot11 24ghz slot 0 dot11n antenna {A | B | C | D}` | 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. |
| 8    | `ap name ap-name dot11 24ghz slot 0 shutdown` | Disables 802.11b radio hosted on slot 0 for a specific access point. |
| 9    | `ap name ap-name dot11 24ghz slot 0 txpower {tx_power_level | auto}` | Configures transmit power level for 802.11b radio hosted on slot 0 for a specific access point. |
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 doc.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# enable</td>
</tr>
<tr>
<td>Purpose</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>ap name ap-name dot11 5ghz slot 1 SI</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 SI</td>
</tr>
<tr>
<td>Purpose</td>
<td>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.</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>ap name ap-name dot11 5ghz slot 1 antenna ext-ant-gain antenna_gain_value</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna ext-ant-gain</td>
</tr>
<tr>
<td>Purpose</td>
<td>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.</td>
</tr>
<tr>
<td>Step 4</td>
<td>**ap name ap-name dot11 5ghz slot 1 antenna mode [omni</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna mode sectorA</td>
</tr>
<tr>
<td>Purpose</td>
<td>Configures the antenna mode for 802.11a radios for a specific access point hosted on slot 1.</td>
</tr>
<tr>
<td>Step 5</td>
<td>**ap name ap-name dot11 5ghz slot 1 antenna selection [internal</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Purpose</td>
<td>Configures the antenna selection for 802.11a radios for a specific access point hosted on slot 1.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
</tr>
<tr>
<td>6</td>
<td><strong>ap name ap-name dot11 5ghz slot 1 beamforming</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 beamforming</td>
</tr>
<tr>
<td>7</td>
<td>**ap name ap-name dot11 5ghz slot 1 channel {channel_number</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 channel auto</td>
</tr>
<tr>
<td>8</td>
<td><strong>ap name ap-name dot11 5ghz slot 1 cleanair</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 cleanair</td>
</tr>
<tr>
<td>9</td>
<td>**ap name ap-name dot11 5ghz slot 1 dot11n antenna {A</td>
</tr>
</tbody>
</table>
|      | **Example:** Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 dot11n antenna A | 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. |
| 10   | **ap name ap-name dot11 5ghz slot 1 rrm channel channel** | Is another way of changing the channel hosted on slot 1 for a specific access point. |
|      | **Example:** Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 rrm channel 2 | Here, *channel*- Refers to the new channel created using 802.11h channel announcement. The valid range is from 1 to 173, provided 173 is a valid channel in the country where the access point is deployed. |
| 11   | **ap name ap-name dot11 5ghz slot 1 shutdown** | Disables 802.11a radio hosted on slot 1 for a specific access point. |
|      | **Example:** Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 shutdown |         |
### Information About Dual-Band Radio Support

The Dual-Band (XOR) radio in APs like Cisco 2800, 3800, 4800, and the 9100 series AP models offers 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 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. When a radio moves between bands (from 2.4GHz to 5GHz 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, the radios operate as a macro cell and micro cell. Macro-micro client steering is used to steer a client between macro and micro.

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 steering of the band on the radio—The band on the XOR radio is changed by the Flexible Radio Assignment (FRA) feature that monitors and changes the band as per site requirements.

### Configuring Default XOR Radio Support

#### Before you begin

**Note**

The default radio points to the XOR radio hosted on slot 0.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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
  ```
<p>| Configures the 802.11 dual-band antenna on a specific Cisco access point. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# ap name ap-name dot11 dual-band antenna ext-ant-gain 2</td>
<td><em>antenna_gain_value</em>—The valid range is from 0 to 40.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>ap name ap-name [no] dot11 dual-band shutdown</td>
<td>Shuts down the default dual-band radio on a specific Cisco access point.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# ap name ap-name dot11 dual-band shutdown</td>
<td>Use the no form of the command to enable the radio.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>ap name ap-name dot11 dual-band txpower {transmit_power_level</td>
<td>auto}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# ap name ap-name dot11 dual-band txpower 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>ap name ap-name dot11 dual-band role manual client-serving</td>
<td>Switches to client–serving mode on the Cisco access point.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# ap name ap-name dot11 dual-band role manual client-serving</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>ap name ap-name dot11 dual-band band 24ghz</td>
<td>Switches to 2.4-GHz radio band.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# ap name ap-name dot11 dual-band band 24ghz</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>ap name ap-name dot11 dual-band channel channel-number</td>
<td>Enters the channel for the dual band.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# ap name ap-name dot11 dual-band channel 2</td>
<td>channel-number—The valid range is from 1 to 173.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>ap name ap-name dot11 dual-band channel auto</td>
<td>Enables the auto channel assignment for the dual-band.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# ap name ap-name dot11 dual-band channel auto</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>ap name ap-name dot11 dual-band channel width {20 MHz</td>
<td>40 MHz</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# ap name ap-name dot11 dual-band channel width 20 MHz</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Enables the Cisco CleanAir feature on the dual-band radio.</td>
</tr>
<tr>
<td><code>ap name ap-name dot11 dual-band cleanair</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# ap name ap-name dot11 dual-band cleanair</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Selects a band for the Cisco CleanAir feature. Use the <code>no</code> form of this command to disable the Cisco CleanAir feature.</td>
</tr>
<tr>
<td><code>ap name ap-name dot11 dual-band cleanair</code></td>
<td></td>
</tr>
<tr>
<td>`band {24 GHz</td>
<td>5 GMHz}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# ap name ap-name [no] dot11 dual-band cleanair band 5 GHz</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>Configures the 802.11n dual-band parameters for a specific access point.</td>
</tr>
<tr>
<td>`ap name ap-name dot11 dual-band dot11n antenna {A</td>
<td>B</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# ap name ap-name dot11 dual-band dot11n antenna A</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>Displays the auto-RF information for the Cisco access point.</td>
</tr>
<tr>
<td><code>show ap name ap-name auto-rf dot11 dual-band</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# show ap name ap-name auto-rf dot11 dual-band</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>Displays the list of BSSIDs for the Cisco access point.</td>
</tr>
<tr>
<td><code>show ap name ap-name wlan dot11 dual-band</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# show ap name ap-name wlan dot11 dual-band</code></td>
<td></td>
</tr>
</tbody>
</table>

## 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**.
### Configuring XOR Radio Support for the Specified Slot Number

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap name <em>ap-name</em> dot11 dual-band slot 0 antenna ext-ant-gain external_antenna_gain_value</td>
<td>Configures dual-band antenna for the XOR radio hosted on slot 0 for a specific access point. <em>external_antenna_gain_value</em> - Is the external antenna gain value in multiples of .5 dBi unit. The valid range is from 0 to 40.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 antenna ext-ant-gain 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ap name <em>ap-name</em> dot11 dual-band slot 0 band {24ghz</td>
<td>5ghz}</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 band 24ghz</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ap name <em>ap-name</em> dot11 dual-band slot 0 channel {channel_number</td>
<td>auto</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 channel 3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ap name <em>ap-name</em> dot11 dual-band slot 0 cleanair band {24Ghz</td>
<td>5Ghz}</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 cleanair band 24Ghz</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ap name <em>ap-name</em> dot11 dual-band slot 0 dot11n antenna {A</td>
<td>B</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 dot11n antenna A</td>
<td></td>
</tr>
<tr>
<td>A- Enables antenna port A.</td>
<td></td>
</tr>
<tr>
<td>B- Enables antenna port B.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>ap name ap-name dot11 dual-band slot 0 role {auto | manual [client-serving | monitor]}</td>
<td>Enables antenna port C. Enables antenna port D. 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.</td>
</tr>
<tr>
<td>ap name ap-name dot11 dual-band slot 0 shutdown</td>
<td>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.</td>
</tr>
<tr>
<td>ap name ap-name dot11 dual-band slot 0 txpower {tx_power_level | auto}</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device# enable</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

```
Step 2 ap name ap-name dot11 rx-dual-band slot 2 cleanair band {24Ghz | 5Ghz}
```

**Purpose**

Enables CleanAir with receiver only (Rx-only) dual-band radio on a specific access point.

**Example:**

```
Device# ap name AP-SIDD-A06 dot11 rx-dual-band slot 2 cleanair band 24Ghz
```

Here, 2 refers to the slot ID.

Use the `no` form of this command to disable CleanAir.

```
Device# ap name AP-SIDD-A06 [no] dot11 rx-dual-band slot 2 cleanair band 24Ghz
```

Disabling Receiver Only Dual-Band Radio on a Cisco Access Point

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device# enable</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

```
Step 2 ap name ap-name dot11 rx-dual-band slot 2 shutdown
```

**Purpose**

Disables receiver only dual-band radio on a specific Cisco access point.

**Example:**

```
Device# ap name AP-SIDD-A06 dot11 rx-dual-band slot 2 shutdown
```

Here, 2 refers to the slot ID.

Use the `no` form of this command to enable receiver only dual-band radio.

```
Device# ap name AP-SIDD-A06 [no] dot11 rx-dual-band slot 2 shutdown
```

Configuring Client Steering (CLI)

**Before you begin**

Enable Cisco CleanAir on the corresponding dual-band radio.
## Configuring Client Steering (CLI)

<table>
<thead>
<tr>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong></td>
<td>Configures the macro-to-micro probe in RSSI. The range is between -6 to -3.</td>
</tr>
</tbody>
</table>
| wireless macro-micro steering probe-suppression hysteresis **RSSI-in-dBm** | Example: 
Device(config)# wireless macro-micro steering probe-suppression hysteresis -5 |
| **Step 9** | Enables probe suppression mode. |
| wireless macro-micro steering probe-suppression probe-only | Example: 
Device(config)# wireless macro-micro steering probe-suppression probe-only |
| **Step 10** | Enables probe and single authentication suppression mode. |
| wireless macro-micro steering probe-suppression probe-auth | Example: 
Device(config)# wireless macro-micro steering probe-suppression probe-auth |
| **Step 11** | Displays the wireless client steering information. |
| show wireless client steering | Example: 
Device# show wireless client steering |

### 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
```

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Subband</th>
<th>Radio</th>
<th>Mac</th>
<th>Status</th>
<th>Channel</th>
<th>Power Level</th>
<th>Slot ID</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>4800</td>
<td>All</td>
<td>3890.a5e6.f360</td>
<td>Enabled</td>
<td>(40)* *1/8</td>
<td>(22 dBm)</td>
<td>0</td>
<td>Sensor</td>
<td></td>
</tr>
<tr>
<td>4800</td>
<td>All</td>
<td>3890.a5e6.f360</td>
<td>Enabled</td>
<td>N/A</td>
<td>N/A</td>
<td>2</td>
<td>Monitor</td>
<td></td>
</tr>
</tbody>
</table>
802.1x Support

- Introduction to the 802.1x Authentication, on page 177
- Limitations of the 802.1x Authentication, on page 178
- Topology - Overview, on page 178
- Configuring 802.1x Authentication Type and LSC AP Authentication Type (GUI), on page 179
- Configuring 802.1x Authentication Type and LSC AP Authentication Type, on page 179
- Enabling 802.1x on the Switch Port, on page 182
- Verifying 802.1x on the Switch Port, on page 183
- Verifying the Authentication Type, on page 184

Introduction to the 802.1x Authentication

IEEE 802.1x port-based authentication is configured 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 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.

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 Dot1x credentials configuration for AP, since AP will use EAP-FAST with MSCHAP Version 2 method.

Starting from Cisco IOS XE Amsterdam 17.1.1, TLS 1.2 is supported in EAP-FAST authentication protocol.
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.

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.
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 2** configure terminal | Enables privileged EXEC mode. Enters global configuration mode.
   **Example:** Device# configure terminal

**Step 3** ap profile &lt;profile-name&gt; | Specify a profile name.
   **Example:** Device(config)# ap profile new-profile

**Step 4** dot1x {max-sessions | username | eap-type | lsc-ap-auth-state} | 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.
   **Example:** Device(config-ap-profile)# dot1x eap-type

**Step 5** dot1x eap-type {EAP-FAST | EAP-TLS | EAP-PEAP} | Configures the dot1x authentication type: EAP-FAST, EAP-TLS, or EAP-PEAP.
   **Example:** Device(config-ap-profile)# dot1x eap-type

**Step 6** dot1x lsc-ap-auth-state {CAPWAP-DTLS | Dot1x-port-auth | Both} | 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.
   **Both:** Uses LSC for both CAPWAP-DTLS and Dot1x authentication with port.
   **Example:** Device(config-ap-profile)# dot1x lsc-ap-auth-state Dot1x-port-auth

**Step 7** end | Exits the AP profile configuration mode and enters privileged EXEC mode.
   **Example:** Device(config-ap-profile)# end

---

**Configuring the 802.1x Username and Password (GUI)**

**Procedure**

**Step 1** Choose Configuration &gt; Tags & Profiles &gt; 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>Device&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
<td>configure terminal</td>
<td>Enables privileged EXEC mode. Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
<td>ap profile &lt;profile-name&gt;</td>
<td>Specify a profile name.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>Device(config)# ap profile new-profile</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
<td>dot1x {max-sessions</td>
<td>username</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>Device(config-ap-profile)# dot1x eap-type</td>
<td>max-sessions: Configures the maximum 802.1x sessions initiated per AP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>username: Configures the 802.1x username for all Aps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>eap-type: Configures the dot1x authentication type with the switch port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>lsc-ap-auth-state: Configures the LSC authentication state on the AP.</td>
</tr>
<tr>
<td>Step 5</td>
<td></td>
<td>dot1x username &lt;username&gt; password {0</td>
<td>8} &lt;password&gt;</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
<td>0: Specifies an unencrypted password will follow.</td>
</tr>
</tbody>
</table>
Enabling 802.1x on the Switch Port

The following procedure enables 802.1x on the switch port:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enables privileged EXEC mode. Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>aaa new-model</code></td>
<td>Enables AAA.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`aaa authentication dot1x {default</td>
<td>listname} method1[method2...]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa authentication dot1x default group radius</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>dot1x system-auth-control</code></td>
<td>Globally enables 802.1X port-based authentication.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# dot1x system-auth-control</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>interface type slot/port</code></td>
<td>Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# interface fastethernet2/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>`authentication port-control {auto</td>
<td>force-authorized</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-if)# authentication port-control auto</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 8**

`dot1x pae [supplicant | authenticator | both]`

**Example:**

```
Device(config-if)# dot1x pae authenticator
```

**Step 9**

`end`

**Example:**

```
Device(config-if)# end
```

**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
```
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

Configuring CAPWAP Link Aggregation Support

- Information About Link Aggregation, on page 185
- Information About CAPWAP LAG Support, on page 185
- Restrictions for CAPWAP LAG Support, on page 186
- Enabling CAPWAP LAG Support on Controller, on page 186
- Enabling CAPWAP LAG Globally on Controller, on page 186
- Disabling CAPWAP LAG Globally on Controller, on page 187
- Enabling CAPWAP LAG for an AP Profile, on page 187
- Disabling CAPWAP LAG for an AP Profile, on page 188
- Disabling CAPWAP LAG Support on Controller, on page 188
- Verifying CAPWAP LAG Support Configurations, on page 189

Information About 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.

Information About CAPWAP LAG Support

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 (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
Restrictions for CAPWAP LAG Support

- Access points 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.

Enabling CAPWAP LAG Support on Controller

### Enabling CAPWAP LAG Support on Controller

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ap lag support</td>
<td>Enables CAPWAP LAG support on the controller.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ap lag support</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>After executing this command, you get to view the following warning statement:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Changing the lag support will cause all the APs to disconnect.</td>
<td></td>
</tr>
<tr>
<td>Thus, all APs with LAG capability reboots and joins the enabled CAPWAP LAG.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>ap profile ap-profile</td>
<td>Configures an AP profile and enters AP profile configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# ap profile xyz-ap-profile</td>
<td>Note When you delete a named profile, the APs associated with that profile will not revert to the default profile.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>lag</td>
<td>Enables CAPWAP LAG for an AP profile.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-ap-profile)# lag</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Exits configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-ap-profile)# end</td>
<td></td>
</tr>
</tbody>
</table>
Disabling CAPWAP LAG for an AP Profile

Procedure

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

| **Step 2** | Configures an AP profile and enters AP profile configuration mode. |
| `ap profile ap-profile` | Example: |
| Device(config)# `ap profile xyz-ap-profile` | |

**Note** When you delete a named profile, the APs associated with that profile will not revert to the default profile.

| **Step 3** | Disables CAPWAP LAG for an AP profile. |
| `no lag` | Example: |
| Device(config-ap-profile)# `no lag` | |

| **Step 4** | Exits configuration mode and returns to privileged EXEC mode. |
| `end` | Example: |
| Device(config-ap-profile)# `end` | |

Disabling CAPWAP LAG Support on Controller

Procedure

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

| **Step 2** | Disables CAPWAP LAG support on the controller. |
| `no ap lag support` | Example: |
| Device(config)# `no ap lag support` | |

**Note** All APs with LAG capability reboots and joins the disabled CAPWAP LAG.

| **Step 3** | Exits configuration mode and returns to privileged EXEC mode. |
| `end` | Example: |
| Device(config)# `end` | |
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.
```
Verifying CAPWAP LAG Support Configurations
CHAPTER 21

Configuring DHCP and NAT Functionality on Root Access Point

• Information About DHCP and NAT Functionality on Root AP (RAP), on page 191
• Configuring DHCP Server on Root Access Point (RAP), on page 192
• Verifying DHCP Server for Root AP Configuration, on page 192

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

- This feature is applicable for Cisco Aironet 1542 series outdoor access points only.

Note

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 functionality 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ap profile ap-profile-name</code></td>
<td>Configures an AP Profile.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ap profile ap-profile-name</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>dhcp-server</code></td>
<td>Configures DHCP server on the root access point.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-ap-profile)# dhcp-server</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
<td>Saves the configuration and exits configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-ap-profile)# end</td>
<td></td>
</tr>
</tbody>
</table>

## 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
-----------------------------------------------
Dhcp Server : Enabled
```
CHAPTER 22

OFDMA Support for 11ax Access Points

- Information About OFDMA Support for 11ax Access Points, on page 193
- Configuring 11AX (GUI), on page 194
- Configuring Channel Width, on page 194
- Configuring 802.11ax Radio Parameters (CLI), on page 195
- Setting up the 802.11ax Radio Parameters, on page 195
- Configuring OFDMA on a WLAN, on page 196
- Verifying Channel Width, on page 197
- Verifying Client Details, on page 198
- Verifying Radio Configuration, on page 199

Information About OFDMA Support for 11ax Access Points

The Cisco Catalyst 9100 series access points are the next generation WiFi 802.11ax access point, which is ideal for high-density high-definition applications.

The IEEE 802.11ax protocol aims to improve user experience and network performance in high density deployments for both 2.4 GHz and 5 GHz. The 802.11ax APs supports transmission or reception to more than one client simultaneously using Orthogonal Frequency Division Multiplexing (OFDMA).

The IEEE 802.11ax supports uplink MU-MIMO and also adds OFDMA for multiple users in the uplink and downlink. All the users in IEEE 802.11ax OFDMA have the same time allocations and it ends at the same time. In MU-MIMO and OFDMA, multiple stations (STAs) either simultaneously transmit to a single STA or simultaneously receive from a single STA independent data streams over the same radio frequencies.

Supported Modes on 11ax Access Points

The following AP modes are supported:

- Local mode
- Flex-connect mode
- Bridge mode
- Flex+Mesh mode
Configuring 11AX (GUI)

You can configure 11ax for the frequencies, 5 GHz and 2.4 GHz.

Procedure

**Step 1** Choose Configuration > Radio Configurations > High Throughput.

**Step 2** Click the 5 GHz Band tab.
   a) Expand the 11ax section.
   b) Select the Enable 11ax and Multiple Bssid check boxes, if required.
   c) Check either the Select All check box to configure all the data rates or select the desired options from the available data rates list.

**Step 3** Click the 2.4 GHz Band tab.
   a) Expand the 11ax section.
   b) Select the Enable 11ax and Multiple Bssid check boxes, if required.
   c) Check either the Select All check box to configure all the data rates or select the desired options from the available data rates list.

Configuring Channel Width

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`ap dot11 (24ghz</td>
<td>5ghz) rrm channel dca chan-width 160`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap dot11 5ghz rrm channel dca chan-width 160</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`ap dot11 (24ghz</td>
<td>5ghz) rf-profile profile-name`</td>
</tr>
</tbody>
</table>
Configuring 802.11ax Radio Parameters (CLI)

Follow the procedure given below to configure radio parameters:

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>`ap dot11 {24ghz</td>
<td>5ghz} dot11ax`</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>`ap dot11 {24ghz</td>
<td>5ghz} dot11ax mcs tx index index spatial-stream spatial-stream-value`</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>ap led-brightness brightness-level</code></td>
<td>(Optional) Configures the led brightness level.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
</tbody>
</table>

Setting up the 802.11ax Radio Parameters

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring OFDMA on a WLAN

**Purpose**
- Enter the global configuration mode.
- Enter the WLAN configuration mode.

**Procedure**

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

**Example:**

- Device# configure terminal

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>wlan wlan1</td>
<td>Enters the WLAN configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

- Device(config)# wlan wlan1

**Note**

For Cisco Catalyst 9115 and 9120 series APs, the configuration given below are per radio, and not per WLAN. This feature remains enabled on the controller, if it is enabled on any of the WLANs.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><code>dot11ax downlink-ofdma</code></td>
<td>Enables the downlink connection that uses the OFDMA technology. Use the <code>no</code> form of the command to disable the configuration.</td>
</tr>
<tr>
<td>4</td>
<td><code>dot11ax uplink-ofdma</code></td>
<td>Enables the uplink connection that uses the OFDMA technology.</td>
</tr>
<tr>
<td>5</td>
<td><code>dot11ax downlink-mumimo</code></td>
<td>Enables the downlink connection that uses the MUMIMO technology.</td>
</tr>
<tr>
<td>6</td>
<td><code>dot11ax uplink-mumimo</code></td>
<td>Enables the uplink connection that uses the MUMIMO technology.</td>
</tr>
<tr>
<td>7</td>
<td><code>dot11ax twt-broadcast-support</code></td>
<td>Enables the TWT broadcast support operation.</td>
</tr>
</tbody>
</table>

## Verifying Channel Width

To verify the channel width and other channel information, use the following `show` commands:

- **Device# show ap dot11 5ghz summary**

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Mac Address</th>
<th>Slot</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Channel</th>
<th>Width</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP80e0.1d75.6954</td>
<td>80e0.1d7a.7620</td>
<td>1</td>
<td>Enabled</td>
<td>Up</td>
<td>(52)*</td>
<td>160</td>
</tr>
</tbody>
</table>

- **Device# show ap dot11 dual-band summary**

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Subband</th>
<th>Radio Mac</th>
<th>Status</th>
<th>Channel</th>
<th>Power Level</th>
<th>Slot ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>kart128021mi</td>
<td>All</td>
<td>002a.1058.38a0</td>
<td>Enabled</td>
<td>(52)*</td>
<td>(1)*</td>
<td>1</td>
</tr>
</tbody>
</table>

- **Device# show ap name <ap-name> channel**

  | 802.11b/g Current Channel | : 11 |
  | Slot ID                  | : 0  |
  | Allowed Channel List     | : 1,2,3,4,5,6,7,8,9,10,11 |
  | **802.11a Current Channel** | **52 (160 MHz)** |
  | Slot ID                  | : 1  |
Verifying Client Details

To verify the client information, use the following `show` commands:

```
Device# show wireless client mac-address <mac-address> detail
```

---

**Client MAC Address**: a886.ddb2.05e9
**Client IPv4 Address**: 169.254.175.214
**Client Username**: N/A
**Voice Client Type**: Unknown
**AP MAC Address**: c025.5c55.e400
**AP Name**: APe4c7.22b2.948e
**Device Type**: N/A
**Device Version**: N/A
**AP slot**: 0
**Client State**: Associated
**Policy Profile**: default-policy-profile
**Flex Profile**: default-flex-profile
**Wireless LAN Id**: 1
**Wireless LAN Name**: SSS_OPEN
**BSSID**: c025.5c55.e406
Verifying Radio Configuration

To verify the radio configuration information, use the following show commands:

Device# show wireless client summary

Number of Local Clients: 1

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>AP Name</th>
<th>WLAN</th>
<th>State</th>
<th>Protocol Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>a886.ddb2.05e9</td>
<td>APe4c7.22b2.948e</td>
<td>1</td>
<td>Run</td>
<td>802.11ax(5) None</td>
</tr>
</tbody>
</table>

Device# show wireless stats client detail

Total Number of Clients : 1

Protocol Statistics

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Client Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b</td>
<td>0</td>
</tr>
<tr>
<td>802.11g</td>
<td>0</td>
</tr>
<tr>
<td>802.11a</td>
<td>0</td>
</tr>
<tr>
<td>802.11n-2.4 GHz</td>
<td>0</td>
</tr>
<tr>
<td>802.11n-5 GHz</td>
<td>0</td>
</tr>
<tr>
<td>802.11ac</td>
<td>0</td>
</tr>
<tr>
<td><strong>802.11ax</strong></td>
<td><strong>1</strong></td>
</tr>
</tbody>
</table>
MCS 9, Spatial Streams = 3 : Disabled
MCS 11, Spatial Streams = 3 : Disabled
MCS 7, Spatial Streams = 4 : Supported
MCS 9, Spatial Streams = 4 : Supported
MCS 11, Spatial Streams = 4 : Supported
MCS 7, Spatial Streams = 5 : Supported
MCS 9, Spatial Streams = 5 : Supported
MCS 11, Spatial Streams = 5 : Supported
MCS 7, Spatial Streams = 6 : Supported
MCS 9, Spatial Streams = 6 : Supported
MCS 11, Spatial Streams = 6 : Supported
MCS 7, Spatial Streams = 7 : Supported
MCS 9, Spatial Streams = 7 : Supported
MCS 11, Spatial Streams = 7 : Supported
MCS 7, Spatial Streams = 8 : Supported
MCS 9, Spatial Streams = 8 : Supported
MCS 11, Spatial Streams = 8 : Supported
Beacon Interval : 100
.
.
Maximum Number of Clients per AP Radio : 200

Device# show ap dot11 24ghz network

802.11b Network : Enabled
.
.
802.11axSupport................................. Enabled
  dynamicFrag................................ Disabled
  multiBssid................................. Disabled
802.11ax : Enabled
  DynamicFrag : Enabled
  MultiBssid : Enabled
802.11ax MCS Settings:
  MCS 7, Spatial Streams = 1 : Supported
  MCS 9, Spatial Streams = 1 : Supported
  MCS 11, Spatial Streams = 1 : Supported
  MCS 7, Spatial Streams = 2 : Supported
  MCS 9, Spatial Streams = 2 : Supported
  MCS 11, Spatial Streams = 2 : Supported
  MCS 7, Spatial Streams = 3 : Supported
  MCS 9, Spatial Streams = 3 : Supported
  MCS 11, Spatial Streams = 3 : Supported
  MCS 7, Spatial Streams = 4 : Disabled
  MCS 9, Spatial Streams = 4 : Disabled
  MCS 11, Spatial Streams = 4 : Disabled
Beacon Interval : 100
.
.
Maximum Number of Clients per AP Radio : 200

Device# show wlan ID <wlan-id>

WLAN Profile Name : ax-wlc

Identifier : 1
Network Name (SSID) : ax-wlc
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

802.11ac MU-MIMO: Disabled
802.11ax parameters:
  - OFDMA Downlink: Enabled
  - OFDMA Uplink: Enabled
  - MU-MIMO Downlink: Enabled
  - MU-MIMO Uplink: Enabled
  - BSS Color: Enabled
  - Partial BSS Color: Enabled
  - BSS Color Code: 0
  - BSS Target Wake Up Time: Enabled

Device# `show ap led-brightness-level summary`

<table>
<thead>
<tr>
<th>AP Name</th>
<th>LED Brightness level</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP00FC.BA01.CC00</td>
<td>Not Supported</td>
</tr>
<tr>
<td>AP70DF.2FA2.72EE</td>
<td>8</td>
</tr>
<tr>
<td>AP7069.5A74.6678</td>
<td>2</td>
</tr>
<tr>
<td>APb838.6159.e184</td>
<td>Not Supported</td>
</tr>
</tbody>
</table>
PART III

Radio Resource Management

- Radio Resource Management, on page 205
- Coverage Hole Detection, on page 235
- Optimized Roaming, on page 241
- Cisco Flexible Radio Assignment, on page 245
- XOR Radio Support, on page 249
- Cisco Receiver Start of Packet, on page 255
- Client Limit, on page 257
- IP Theft, on page 259
- Unscheduled Automatic Power Save Delivery, on page 263
- USB Power Support, on page 265
- Dynamic Frequency Selection, on page 269
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
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 60 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

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. An RF group exists for each 802.11 network type. 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 MC.

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 $\pm 80$ 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.
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**

The RF Group Leader can be configured in two ways as follows:

- Auto Mode—In this mode, the members of an RF group elect an RF group leader to maintain a master power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or 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.

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

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

The main cause of both pinning and cascading is 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 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.

Rogue Access Point Detection in RF Groups

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

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 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, no access point will transmit above 11 dBm, unless the access point is configured manually.

Dynamic Channel Assignment

Two adjacent access points on the same channel can cause either signal contention or signal collision. In a collision, data is not received by the access point. This functionality can become a problem, for example, when someone reading an e-mail in a café affects the performance of the access point in a neighboring business. Even though these are separate networks, someone sending traffic to the café on channel 1 can disrupt communication in an enterprise using the same channel. 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.
Dynamic Channel Assignment

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.
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.

How to Configure RRM

Configuring Neighbor Discovery Type (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Radio Configurations &gt; RRM.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Radio Resource Management page, click either the 5 GHz Band or the 2.4 GHz Band tab.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Save the configuration.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Neighbor Discovery Type (CLI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ap dot11 24ghz</td>
<td>5ghz rrm ndp-type {protected</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)#ap dot11 24ghz rrm</td>
<td>• protected—Sets the neighbor discover type to protected. Packets are encrypted.</td>
</tr>
</tbody>
</table>
### 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**

1. **Step 1** Choose **Configuration > Radio Configurations > RRM**.
2. **Step 2** On the **RRM** page, click the relevant band's tab: either **5 GHz Band** or **2.4 GHz Band**.
3. **Step 3** Click the **RF Grouping** tab.
4. **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
5. **Step 5** Save the configuration.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ndp-type protected</td>
<td><strong>transparent</strong>—Sets the neighbor discover type to transparent. Packets are sent as is.</td>
</tr>
</tbody>
</table>

**Step 3**

Example:

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

Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
## Configuring RF Group Selection Mode (CLI)

### Procedure

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

### Step 2

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ap dot11 24ghz</td>
<td>5ghz rrm group-mode {auto</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# ap dot11 24ghz rrm group-mode leader</td>
<td></td>
</tr>
</tbody>
</table>

- **auto**—Sets the 802.11 RF group selection to automatic update mode.
- **leader**—Sets the 802.11 RF group selection to leader mode.
- **off**—Disables the 802.11 RF group selection.

### Step 3

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

## Configuring an RF Group Name (CLI)

### Procedure

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

### Step 2

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>wireless rf-network name</code></td>
<td>Creates an RF group. The group name should be ASCII String up to 19 characters and is case sensitive.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device (config)# wireless rf-network test1</td>
<td></td>
</tr>
</tbody>
</table>

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

### Step 3

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
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 master power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or if RF group members experience major changes).

- **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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> ap dot11 24ghz</td>
<td>5ghz rrm group-member&lt;br&gt;<strong>group_name ip_addr</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config)#ap dot11 24ghz rrm group-member Gpmmem01 10.1.1.1</td>
</tr>
<tr>
<td><strong>Step 3</strong> end&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config)# end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
</tbody>
</table>
Configuring Transmit Power Control

Configuring Transmit Power (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Radio Configurations &gt; RRM.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>In either the 5 GHz Band or 2.4 GHz Band tab, click the TPC tab.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose of the following dynamic transmit power assignment modes:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Automatic (default): The transmit power is periodically updated for all APs that permit this operation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fixed: No dynamic transmit power assignments occur and values are set to their global default.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Apply.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the Tx-Power Control Threshold (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
</tbody>
</table>
## Configuring the Tx-Power Level (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
| Step 2 | ap dot11 24ghz | 5ghz rrm txpower 
\{trans_power_level\ | auto | max | min | once\} | 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. |
| Example: | Device(config)#ap dot11 24ghz rrm txpower auto |
| Step 3 | end | Returns to privileged EXEC mode.  
Alternatively, you can also press Ctrl-Z to exit global configuration mode. |
| Example: | Device(config)# end |
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 Anchor Time 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 ignore persistent non-WiFi interference.

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 5 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 30 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)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ap dot11 {24ghz</td>
<td>5ghz} rrm channel cleanair-event sensitivity {high</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ap dot11 {24ghz</td>
<td>5ghz} rrm channel dca {add channel-number</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)#ap dot11 24ghz rrm channel dca interval 2</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>• Once</td>
<td>Enables auto-RF only once.</td>
<td></td>
</tr>
<tr>
<td>• Interval</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>• Min-metric</td>
<td>Configures the DCA minimum RSSI energy metric. The range is between -100 and -60.</td>
<td></td>
</tr>
<tr>
<td>• Remove channel-number</td>
<td>Enter the channel number to be removed from the DCA list. The range is between 1 to 14.</td>
<td></td>
</tr>
<tr>
<td>• Sensitivity</td>
<td>Configures the DCA sensitivity level to changes in the environment.</td>
<td></td>
</tr>
<tr>
<td>• High</td>
<td>Specifies the most sensitivity.</td>
<td></td>
</tr>
<tr>
<td>• Low</td>
<td>Specifies the least sensitivity.</td>
<td></td>
</tr>
<tr>
<td>• Medium</td>
<td>Specifies medium sensitivity.</td>
<td></td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>ap dot11 {24ghz\</td>
<td>Configures the foreign AP 802.11 interference avoidance in the channel assignment.</td>
</tr>
<tr>
<td></td>
<td>5ghz} rrm channel foreign</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)#ap 24ghz rrm</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>channel foreign</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>ap dot11 {24ghz\</td>
<td>Configures the Cisco AP 802.11 load avoidance in the channel assignment.</td>
</tr>
<tr>
<td></td>
<td>5ghz} rrm channel load</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)#ap 24ghz rrm</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>channel load</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>ap dot11 {24ghz\</td>
<td>Configures the 802.11 noise avoidance in the channel assignment.</td>
</tr>
<tr>
<td></td>
<td>5ghz} rrm channel noise</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)#ap 24ghz rrm</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>channel noise</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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:*  
Device(config)#ap dot11 24ghz rrm coverage data fail-percentage 60 | Configures the 802.11 coverage hole detection for data packets.  
*fail-percentage*—Configures the 802.11 coverage failure-rate threshold for uplink data packets as a percentage that ranges from 1 to 100%.  
*packet-count*—Configures the 802.11 coverage minimum failure count threshold for uplink data packets that ranges from 1 to 255.  
*rssi-threshold*—Configures the 802.11 minimum receive coverage level for data packets that range from –90 to –60 dBm. |
| **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:* | Configures the 802.11 coverage hole detection for voice packets.  
*fail-percentage*—Configures the 802.11 coverage failure-rate threshold for uplink packets.  
*packet-count*—Configures the 802.11 coverage minimum failure count threshold for 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. |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device(config)#ap dot11 24ghz rrm coverage voice packet-count 10</strong></td>
<td>voice packets as a percentage that ranges from 1 to 100%.</td>
</tr>
<tr>
<td>• <strong>packet-count</strong>—Configures the 802.11 coverage minimum failure count threshold for uplink voice packets that ranges from 1 to 255.</td>
<td></td>
</tr>
<tr>
<td>• <strong>rssi-threshold</strong>—Configures the 802.11 minimum receive coverage level for voice packets that range from –90 to –60 dBm.</td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| **configure terminal** | Enters global configuration mode. |
| **Example:**
| Device# configure terminal | |
| **Step 2**
| **ap dot11 24ghz | 5ghz rrm logging {channel | coverage | foreign | load | noise | performance | txpower}** | Configures event-logging for various parameters. |
| **Example:**
| Device(config)#ap dot11 24ghz rrm logging channel
| **Device(config)#ap dot11 24ghz rrm logging coverage** | • **channel**—Configures the 802.11 channel change logging mode. |
| **Device(config)#ap dot11 24ghz rrm logging foreign** | • **coverage**—Configures the 802.11 coverage profile logging mode. |
| **Device(config)#ap dot11 24ghz rrm logging load** | • **foreign**—Configures the 802.11 foreign interference profile logging mode. |
| **Device(config)#ap dot11 24ghz rrm logging noise** | • **load**—Configures the 802.11 load profile logging mode. |
| **Device(config)#ap dot11 24ghz rrm logging performance** | • **noise**—Configures the 802.11 noise profile logging mode. |
| **Device(config)#ap dot11 24ghz rrm logging txpower** | • **performance**—Configures the 802.11 performance profile logging mode. |
| **Device(config)#ap dot11 24ghz rrm logging txpower** | • **txpower**—Configures the 802.11 transmit power change logging 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 3600 secs) 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# <code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong> `ap dot11 24ghz</td>
<td>5ghz rrm monitor channel-list {all</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# <code>ap dot11 24ghz rrm monitor channel-list all</code></td>
</tr>
<tr>
<td></td>
<td>• all — Monitors all channels.</td>
</tr>
<tr>
<td></td>
<td>• country — Monitor channels used in configured country code.</td>
</tr>
<tr>
<td></td>
<td>• dca — Monitor channels used by dynamic channel assignment.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>`ap dot11 24ghz</td>
<td>5ghz rrm monitor coverage interval`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)#ap dot11 24ghz rrm monitor coverage 600</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>`ap dot11 24ghz</td>
<td>5ghz rrm monitor load interval`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)#ap dot11 24ghz rrm monitor load 180</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>`ap dot11 24ghz</td>
<td>5ghz rrm monitor noise interval`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)#ap dot11 24ghz rrm monitor noise 360</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>`ap dot11 24ghz</td>
<td>5ghz rrm monitor signal interval`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)#ap dot11 24ghz rrm monitor signal 480</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring the 802.11 Performance Profile (GUI)

**Procedure**

1. **Step 1** Choose **Configuration** > **Tags & Profiles** > **AP Join**.<br>
2. **Step 2** On the **AP Join** page, click the name of the profile or click **Add** to create a new one.<br>
3. **Step 3** In the **Add/Edit RF Profile** window, click the **RRM** tab.<br>
4. **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.<br>
   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**

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

**Step 2** ap dot11 24ghz | 5ghz rrm profile clients cli_threshold_value

Example:

Device(config)#ap dot11 24ghz rrm profile clients 20

Sets the threshold value for 802.11 Cisco AP clients that range between 1 and 75 clients.

**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:

Sets the threshold value for 802.11 RF utilization that ranges between 0 to 100%.
### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# enable</td>
<td>Enables the 802.11 channel selection update for each of the Cisco access points.</td>
</tr>
<tr>
<td><strong>Step 2</strong> `ap dot11 {24ghz</td>
<td>5ghz} rrm channel-update`</td>
</tr>
</tbody>
</table>
Restarting DCA Operation

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ap dot11 {24ghz</td>
<td>5ghz} rrm dca restart</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# ap dot11 24ghz rrm dca restart</td>
<td></td>
</tr>
</tbody>
</table>

Updating Power Assignment Parameters (GUI)

<table>
<thead>
<tr>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
</tr>
</tbody>
</table>

Updating Power Assignment Parameters (CLI)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ap dot11 {24ghz</td>
<td>5ghz} rrm txpower update</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# ap dot11 24ghz rrm txpower update</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
</tbody>
</table>
| ap name *Cisco_AP* mode { monitor | clear | sensor | sniffer } | 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. |
| Example: Device# ap name ap1 mode clear |         |
| **Step 2**        |         |
| end | Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode. |
| Example: Device(config)# end |         |
| **Step 3**        |         |
| configure terminal | Enters global configuration mode. |
| Example: Device# configure terminal |         |
| **Step 4**        |         |
| wireless wps ap-authentication | Enables Rogue access point detection. |
| Example: Device (config)# wireless wps ap-authentication |         |
| **Step 5**        |         |
| wireless wps ap-authentication threshold value | Specifies when a Rogue access point alarm is generated. An alarm occurs when the threshold value (which specifies the number of access |
Purpose

Command or Action

Device (config)# wireless wps
ap-authentication threshold 50

Purpose

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

Enablerogue 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

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ap dot11 24ghz channel</td>
<td>Displays the configuration and statistics of the 802.11b channel assignment.</td>
</tr>
<tr>
<td>show ap dot11 24ghz coverage</td>
<td>Displays the configuration and statistics of the 802.11b coverage.</td>
</tr>
<tr>
<td>show ap dot11 24ghz group</td>
<td>Displays the configuration and statistics of the 802.11b grouping.</td>
</tr>
<tr>
<td>show ap dot11 24ghz logging</td>
<td>Displays the configuration and statistics of the 802.11b event logging.</td>
</tr>
<tr>
<td>show ap dot11 24ghz monitor</td>
<td>Displays the configuration and statistics of the 802.11b monitoring.</td>
</tr>
<tr>
<td>show ap dot11 24ghz profile</td>
<td>Displays 802.11b profiling information for all Cisco APs.</td>
</tr>
<tr>
<td>show ap dot11 24ghz summary</td>
<td>Displays the configuration and statistics of the 802.11b Cisco APs.</td>
</tr>
<tr>
<td>show ap dot11 24ghz txpower</td>
<td>Displays the configuration and statistics of the 802.11b transmit power control.</td>
</tr>
<tr>
<td>show ap dot11 5ghz channel</td>
<td>Displays the configuration and statistics of the 802.11a channel assignment.</td>
</tr>
<tr>
<td>show ap dot11 5ghz coverage</td>
<td>Displays the configuration and statistics of the 802.11a coverage.</td>
</tr>
<tr>
<td>show ap dot11 5ghz group</td>
<td>Displays the configuration and statistics of the 802.11a grouping.</td>
</tr>
<tr>
<td>show ap dot11 5ghz logging</td>
<td>Displays the configuration and statistics of the 802.11a event logging.</td>
</tr>
</tbody>
</table>
Commands | Description
---|---
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ap dot11 5ghz group</td>
<td>Displays the controller name which is the RF group leader for the 802.11a RF network.</td>
</tr>
<tr>
<td>show ap dot11 24ghz group</td>
<td>Displays the controller name which is the RF group leader for the 802.11b/g RF network.</td>
</tr>
</tbody>
</table>

### 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 apl 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
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
Additions to Clea 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
Coverage Hole Detection

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.

Follow the procedure given below to configure CHD:

**Before you begin**

Disable the 802.11 network before applying the configuration.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} rrm coverage<code>&lt;br&gt;</code>Device(config)# ap dot11 24ghz rrm coverage`</td>
</tr>
<tr>
<td>Step 2</td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} rrm coverage data {fail-percentage</td>
</tr>
<tr>
<td>Step 3</td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} rrm coverage exception global exception level<code>&lt;br&gt;</code>Device(config)# ap dot11 24ghz rrm coverage exception global 50`</td>
</tr>
<tr>
<td>Step 4</td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} rrm coverage level global cli_min exception level<code>&lt;br&gt;</code>Device(config)# ap dot11 24ghz rrm coverage level global 10`</td>
</tr>
</tbody>
</table>
### Command or Action

| 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
```

**Purpose:**

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.

<table>
<thead>
<tr>
<th>Step 6</th>
<th>end</th>
</tr>
</thead>
</table>

**Example:**

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

**Purpose:**

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
```

**Purpose:**

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Configuration</strong> &gt; <strong>Radio Configurations</strong> &gt; <strong>RRM</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>On the <strong>Coverage</strong> tab, select the <strong>Enable Coverage Hole Detection</strong> check box.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Data Packet Count</strong> field, enter the number of data packets.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the <strong>Data Packet Percentage</strong> field, enter the percentage of data packets.</td>
</tr>
</tbody>
</table>
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 Tag Profile (CLI)

Follow the procedure given below to configure Coverage Hole Detection (CHD) for RF tag profile.

**Before you begin**

Ensure that the RF tag profile is already created.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap dot11 {24ghz</td>
<td>5ghz} rf-profile rf-profile-tag</td>
</tr>
<tr>
<td>Example: Device(config)# ap dot11 24ghz rf-profile alpha-rfprofile-24ghz</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> coverage data rssi threshold threshold-value</td>
<td>Configures the minimum RSSI value for data packets received by the access point. Valid values range from -90 to -60 in dBm.</td>
</tr>
<tr>
<td>Example: Device(config-rf-profile)# coverage data rssi threshold -80</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device(config-rf-profile)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>show ap dot11 24ghz rf-profile summary</td>
</tr>
</tbody>
</table>

Example:

```
Device# show ap dot11 24ghz rf-profile summary
```
Configuring CHD for RF Tag Profile (CLI)
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 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.

### 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.

**Step 5** Save the configuration.

### Configuring Optimized Roaming (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** `ap dot11 5ghz rrm optimized-roam` | Configures 802.11a or 802.11b optimized roaming. By default, optimized roaming is disabled. Example:  
Device(config)# ap dot11 5ghz rrm optimized-roam |
<p>| <strong>Step 2</strong> <code>ap dot11 5ghz rrm optimized-roam reporting-interval interval-seconds</code> | 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. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>ap dot11 5ghz rrm optimized-roam data-rate-threshold mbps</strong></td>
</tr>
</tbody>
</table>
| **Step 4** | **show ap dot11 5ghz optimized-roaming**  
**Example:**  
Device# show ap dot11 5ghz optimized-roaming  
802.11a OptimizedRoaming  
  Mode : Disabled  
  Reporting Interval : 90 seconds  
  Rate Threshold : Disabled  
  Hysteresis : 6 db | Displays information about optimized roaming for each band. |
| **Step 5** | **show ap dot11 5ghz optimized-roaming statistics**  
**Example:**  
Device# show ap dot11 5ghz optimized-roaming statistics  
802.11a OptimizedRoaming statistics  
  Disassociations | Displays information about optimized roaming statistics. |
| **Step 6** | **show wireless statistics ap dot11 5ghz optimized-roaming statistics**  
**Example:**  
Device# show wireless statistics ap dot11 5ghz optimized-roaming statistics  
802.11a OptimizedRoaming statistics  
  Disassociations | Displays optimized roaming statistics for each band. |

**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.
### Configuring Optimized Roaming (CLI)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>: 0</td>
<td>Rejections : 0</td>
</tr>
</tbody>
</table>
Information About Flexible Radio Assignment

Flexible Radio Assignment (FRA) takes advantage of the dual-band radios included in APs like 4800, 3800, 2800 and the new 11AX APs. FRA is a new feature added to the RRM to analyze the 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 slot0= 802.11b,g,n and slot1=802.11a,n,ac.

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 Feature**

- Solves the problem of 2.4–GHz over coverage.
- Creating 2 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 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)**

Follow the procedure given below to configure an FRA radio.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
</tr>
<tr>
<td>3</td>
<td>[no] ap fra</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config)# [no] ap fra</td>
</tr>
<tr>
<td>4</td>
<td>ap fra interval</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ap fra interval 3</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td>5</td>
<td>ap fra sensitivity {high</td>
</tr>
<tr>
<td></td>
<td>• high—Sets the FRA Coverage Overlap Sensitivity to <strong>high</strong>.</td>
</tr>
<tr>
<td></td>
<td>• medium—Sets the FRA Coverage Overlap Sensitivity to <strong>medium</strong>.</td>
</tr>
<tr>
<td></td>
<td>• low—Sets the FRA Coverage Overlap Sensitivity to <strong>low</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ap fra sensitivity high</td>
</tr>
<tr>
<td>6</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config)# end</td>
</tr>
<tr>
<td>7</td>
<td>ap fra revert {all</td>
</tr>
<tr>
<td></td>
<td>{auto</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device# ap fra revert all auto</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device# show ap dot11 24ghz summary</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device# show ap dot11 5ghz summary</td>
</tr>
<tr>
<td>9</td>
<td>Device# show ap fra</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device# show ap fra</td>
</tr>
<tr>
<td></td>
<td>FRA State</td>
</tr>
<tr>
<td></td>
<td>: Disabled</td>
</tr>
</tbody>
</table>
### Configuring an FRA Radio (GUI)

#### Procedure

**Step 1** Choose Configuration > Radio Configurations > RRM > FRA.

**Step 2** On the Flexible Radio Assignment page, 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** 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** Click Apply.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FRA Sensitivity</strong></td>
<td>medium (95%)</td>
</tr>
<tr>
<td><strong>FRA Interval</strong></td>
<td>1 Hour(s)</td>
</tr>
<tr>
<td><strong>AP Name</strong></td>
<td>MAC Address</td>
</tr>
<tr>
<td><strong>Slot ID</strong></td>
<td>Current-Band</td>
</tr>
<tr>
<td><strong>Suggested Mode</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AP00A6.CA36.295A</th>
<th>006b.f09c.8290</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2.4GHz</td>
</tr>
<tr>
<td>2.4GHz</td>
<td></td>
</tr>
</tbody>
</table>

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`

Displays the current 802.11 dual-band parameters in a given AP.
XOR Radio Support

- Information About Dual-Band Radio Support, on page 249
- Configuring Default XOR Radio Support, on page 249
- Configuring XOR Radio Support for the Specified Slot Number (GUI), on page 252
- Configuring XOR Radio Support for the Specified Slot Number, on page 252

Information About Dual-Band Radio Support

The Dual-Band (XOR) radio in APs like Cisco 2800, 3800, 4800, and the 9100 series AP models offers 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 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. When a radio moves between bands (from 2.4GHz to 5GHz 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, the radios operate as a macro cell and micro cell. Macro-micro client steering is used to steer a client between macro and micro.

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 steering of the band on the radio—The band on the XOR radio is changed by the Flexible Radio Assignment (FRA) feature that monitors and changes the band as per site requirements.

Configuring Default XOR Radio Support

Before you begin

Note

The default radio points to the XOR radio hosted on slot 0.
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Device# enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ap name ap-name dot11 dual-band antenna ext-ant-gain antenna_gain_value</td>
</tr>
<tr>
<td></td>
<td>antenna_gain_value—The valid range is from 0 to 40.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device# ap name ap-name dot11 dual-band antenna ext-ant-gain 2</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ap name ap-name [no] dot11 dual-band shutdown</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device# ap name ap-name dot11 dual-band shutdown</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ap name ap-name dot11 dual-band txpower {transmit_power_level</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device# ap name ap-name dot11 dual-band txpower 2</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ap name ap-name dot11 dual-band role manual client-serving</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device# ap name ap-name dot11 dual-band role manual client-serving</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>ap name ap-name dot11 dual-band band 24ghz</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device# ap name ap-name dot11 dual-band band 24ghz</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>ap name ap-name dot11 dual-band channel channel-number</td>
</tr>
<tr>
<td></td>
<td>channel-number—The valid range is from 1 to 173.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device# ap name ap-name dot11 dual-band channel 2</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>ap name ap-name dot11 dual-band channel auto</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device# ap name ap-name dot11 dual-band channel auto</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| 9    | `ap name ap-name dot11 dual-band channel width {20 MHz | 40 MHz | 80 MHz | 160 MHz}` | Chooses the channel width for the dual band. **Example:**

Device# ap name ap-name dot11 dual-band channel width 20 MHz |

| 10   | `ap name ap-name dot11 dual-band cleanair` | Enables the Cisco CleanAir feature on the dual-band radio. **Example:**|

Device# ap name ap-name dot11 dual-band cleanair |

| 11   | `ap name ap-name dot11 dual-band cleanair band {24 GHz | 5 GHz}` | Selects a band for the Cisco CleanAir feature. Use the **no** form of this command to disable the Cisco CleanAir feature. **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 |

| 12   | `ap name ap-name dot11 dual-band dot11n antenna {A | B | C | D}` | Configures the 802.11n dual-band parameters for a specific access point. **Example:**

Device# ap name ap-name dot11 dual-band dot11n antenna A |

| 13   | `show ap name ap-name auto-rf dot11 dual-band` | Displays the auto-RF information for the Cisco access point. **Example:**

Device# show ap name ap-name auto-rf dot11 dual-band |

| 14   | `show ap name ap-name wlan dot11 dual-band` | Displays the list of BSSIDs for the Cisco access point. **Example:**

Device# show ap name ap-name wlan dot11 dual-band |
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap name ap-name dot11 dual-band slot 0 antenna ext-ant-gain external_antenna_gain_value</td>
<td>Configures dual-band antenna for the XOR radio hosted on slot 0 for a specific access point.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 antenna ext-ant-gain 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ap name ap-name dot11 dual-band slot 0 band {24ghz</td>
<td>5ghz}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 band 24ghz</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ap name ap-name dot11 dual-band slot 0 channel {channel_number</td>
<td>auto</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>channel_number</em>- The valid range is from 1 to 165.</td>
</tr>
</tbody>
</table>

#### Step 5

**Example:**

```
Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 channel 3
```

**Enables CleanAir features for dual-band radios hosted on slot 0 for a specific access point.**

#### Step 6

**Example:**

```
Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 cleanair band {24Ghz | 5Ghz}
```

**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.
- C - Enables antenna port C.
- D - Enables antenna port D.

#### Step 7

**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

**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

**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.
Configuring XOR Radio Support for the Specified Slot Number
Cisco Receiver Start of Packet

- Information About Receiver Start of Packet Detection Threshold, on page 255
- Restrictions for Rx SOP, on page 255
- Configuring Rx SOP (CLI), on page 256

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.

The following table shows the permitted range for the Rx SOP threshold.

<table>
<thead>
<tr>
<th>Radio Band</th>
<th>Threshold High</th>
<th>Threshold Medium</th>
<th>Threshold Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4 GHz</td>
<td>-79 dBm</td>
<td>-82 dBm</td>
<td>-85 dBm</td>
</tr>
<tr>
<td>5 GHz</td>
<td>-76 dBm</td>
<td>-78 dBm</td>
<td>-80 dBm</td>
</tr>
</tbody>
</table>
## Configuring Rx SOP (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} rx-sop threshold {auto</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# ap dot11 5ghz rx-sop threshold high</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>`show ap dot11 {24ghz</td>
<td>5ghz} high-density`</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# show ap dot11 5ghz high-density</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>show ap summary</code></td>
<td>Displays a summary of all the connected Cisco APs.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# show ap summary</code></td>
<td></td>
</tr>
</tbody>
</table>
Client Limit

This feature enforces a limit to the number of clients that can be associated with an access point. Further, you can configure the number of clients that can be associated with each access point radio.

Configuring Client Limit (CLI)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>wlan wlan-name</td>
<td>Specifies the WLAN name.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>client association limit maximum-clients-per-WLAN</td>
<td>Configures the maximum limit of clients that can be associated to the given WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Client Limit (CLI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td><code>client association limit ap maximum-clients-per-AP-per-WLAN(0—400)</code></td>
<td>Configures the maximum limit of clients that can be associated to an AP in the WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device (config-wlan) # client association limit ap 120</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>client association limit radio maximum-clients-per-AP-radio-per-WLAN(0—200)</code></td>
<td>Configures the maximum limit of clients that can be associated to an AP radio in the WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device (config-wlan) # client association limit radio 100</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>show wlan id wlan-id</code></td>
<td>Displays the current configuration of the WLAN and the corresponding client association limits.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# show wlan id 2</td>
<td></td>
</tr>
</tbody>
</table>
**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 blacklisting 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

Follow the procedure given below to configure the IP Theft feature:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless wps client-exclusion ip-theft</td>
<td>Configures the client exclusion policy.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless wps client-exclusion ip-theft</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the IP Theft Exclusion Timer

Follow the procedure given below to configure the IP theft exclusion timer:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless profile policy profile-policy</td>
<td>Configures a WLAN policy profile and enters wireless policy configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless profile policy default-policy-profile</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>exclusionlist timeout time-in-seconds</td>
<td>Specifies the timeout, in seconds. The valid range is from 0-2147483647. Enter zero (0) for no timeout.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-policy)# exclusionlist timeout 5</td>
<td></td>
</tr>
</tbody>
</table>

Adding Static Entries for Wired Hosts

Follow the procedure given below to create static wired bindings:
The statically configured wired bindings and locally configured SVI IP addresses have a higher precedence than DHCP.

### Procedure

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

| **Step 2**        | Configures IPv4 or IPv6 static entry. |
| 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:**      |         |
| 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

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>AP Name</th>
<th>WLAN State</th>
<th>Protocol</th>
<th>Method</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>000b.bbb1.0001</td>
<td>SimAP-1</td>
<td>2</td>
<td>Run</td>
<td>11a</td>
<td>None</td>
</tr>
</tbody>
</table>

Number of Excluded Clients: 1

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>AP Name</th>
<th>WLAN State</th>
<th>Protocol</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>10da.4320.cce9</td>
<td>charlie2</td>
<td>2 Excluded</td>
<td>11ac</td>
<td>None</td>
</tr>
</tbody>
</table>

Device# show wireless device-tracking database ip

<table>
<thead>
<tr>
<th>IP</th>
<th>VLAN</th>
<th>STATE</th>
<th>DISCOVERY</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.20.20.2</td>
<td>20</td>
<td>Reachable</td>
<td>Local</td>
<td>001e.14cc.cbff</td>
</tr>
<tr>
<td>20.20.20.6</td>
<td>20</td>
<td>Reachable</td>
<td>IPv4 DHCP</td>
<td>000b.bbb1.0001</td>
</tr>
</tbody>
</table>

Device# show wireless exclusionlist

Excluded Clients

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Description</th>
<th>Exclusion Reason</th>
<th>Time Remaining</th>
</tr>
</thead>
<tbody>
<tr>
<td>10da.4320.cce9</td>
<td>IP address theft</td>
<td>59</td>
<td></td>
</tr>
</tbody>
</table>

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
Unscheduled Automatic Power Save Delivery

- Information About Unscheduled Automatic Power Save Delivery, on page 263
- Configuring Unscheduled Automatic Power Save Delivery (CLI), on page 263

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.

Configuring Unscheduled Automatic Power Save Delivery (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: show wireless client mac-address</td>
<td>Show detailed information of a client by MAC</td>
</tr>
<tr>
<td>client_mac detail</td>
<td>address.</td>
</tr>
</tbody>
</table>

**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
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>VI : Video</td>
<td></td>
</tr>
<tr>
<td>VO : Voice</td>
<td></td>
</tr>
<tr>
<td>T: UAPSD Trigger Enabled</td>
<td></td>
</tr>
<tr>
<td>D: UAPSD Delivery Enabled</td>
<td></td>
</tr>
<tr>
<td>T/D : UAPSD Trigger and Delivery Enabled</td>
<td></td>
</tr>
</tbody>
</table>
USB Power Support

- Configuring an AP Profile, on page 265
- Enabling or Disabling USB for a Cisco AP Profile, on page 265
- Enabling or disabling USB Port to Override for Each Access Point, on page 266
- Enabling or disabling USB Port on an Access Point, on page 266
- Verifying USB for Cisco Access Point Configurations, on page 267

Configuring an AP Profile

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap profile ap-profile</td>
<td>Configures an AP profile and enters the AP profile configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# ap profile xyz-ap-profile</td>
<td>Note: When you delete a named profile, the APs associated with that profile will not revert to the default profile.</td>
</tr>
</tbody>
</table>

Enabling or Disabling USB for a Cisco AP Profile

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> usb-enable</td>
<td>Enables USB for each AP profile.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-ap-profile)# usb-enable</td>
<td>Note: By default, the USB for each AP profile is enabled.</td>
</tr>
</tbody>
</table>
Enabling or disabling USB Port to Override for Each Access Point

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables USB override to override the USB status of an AP profile and force the AP to take its local configuration.</td>
</tr>
<tr>
<td>ap name ap-name usb-module override</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# ap name AP44d3.ca52.48b5 usb-module override</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Disables USB override to override the USB status of an AP profile and force the AP to take its local configuration.</td>
</tr>
<tr>
<td>ap name ap-name no usb-module override</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# ap name AP44d3.ca52.48b5 no usb-module override</td>
<td></td>
</tr>
</tbody>
</table>

Enabling or disabling USB Port on an Access Point

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# enable</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>ap name <em>ap-name</em> usb-module</td>
<td>Enables the USB port on an access point.</td>
</tr>
<tr>
<td>Device# ap name AP44d3.ca52.48b5</td>
<td></td>
</tr>
<tr>
<td>usb-module</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>ap name <em>ap-name</em> no usb-module</td>
<td>Disables the USB port on an access point.</td>
</tr>
<tr>
<td>Device# ap name AP44d3.ca52.48b5</td>
<td></td>
</tr>
<tr>
<td>no usb-module</td>
<td></td>
</tr>
</tbody>
</table>

### Verifying USB for Cisco Access Point Configurations

To view the inventory details for Cisco APs, use the following command:

```bash
Device# show ap name <> inventory
```

NAME: AP2800 , DESCR: Cisco Aironet 2800 Series (IEEE 802.11ac) Access Point
PID: AIR-AP2802I-D-K9 , VID: 01, SN: FGL2135A4GSAP2800
NAME: SanDisk , DESCR: Cruzer Blade
PID: SanDisk , SN: 4C530001151, MaxPower: 224

To view the summary of an AP module, use the following command:

```bash
Device# show ap module summary
```

<table>
<thead>
<tr>
<th>AP Name</th>
<th>External Module</th>
<th>External Module PID</th>
<th>External Module Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP500F.8059.1620</td>
<td>Enable</td>
<td>SanDisk</td>
<td>Cruzer Blade</td>
</tr>
</tbody>
</table>

To view the configuration details for each AP, use the following command:

```bash
Device# show ap config general
```

USB Module Type:................................. USB Module
USB Module Status:.............................. Disabled
USB Module Operational State:............... Enabled
USB Override .............................. Enabled

To view the configuration details, use the following command:

```bash
Device# show ap name < > 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:

```bash
Device# show ap profile xyz detailed
```

USB Module : ENABLED
Dynamic Frequency Selection

- Information About Dynamic Frequency Selection, on page 269
- Configuring Dynamic Frequency Selection, on page 269
- Verifying DFS, on page 270

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 one of the channels in the 40 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

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>no ap dot11 5ghz dtpc</td>
<td>Disables the 802.11a Dynamic Transmit Power Control (DTPC) setting.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Device(config)# no ap dot11 5ghz dtpc</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong>  ap dot11 5ghz channelswitch mode <code>mode-num</code></td>
<td>Configures the 802.11h channel switch mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# ap dot11 5ghz channelswitch mode 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong>  ap dot11 5ghz power-constraint <code>value</code></td>
<td>Configures the 802.11h power-constraint value.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# ap dot11 5ghz power-constraint 12</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong>  ap dot11 5ghz smart-dfs</td>
<td>Configures nonoccupancy time for the radar</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>interference channel.</td>
<td></td>
</tr>
<tr>
<td>Device(config)# ap dot11 5ghz smart-dfs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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 273
• DHCP Option82, on page 277
• RADIUS Realm, on page 301
• Introduction to Accounting of AP Events, on page 309
• Cisco StadiumVision, on page 311
• Persistent SSID Broadcast, on page 315
• Network Monitoring, on page 317
• Creating a Lobby Ambassador Account, on page 321
• Configuring Guest User Accounts, on page 325
AP Packet Capture

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.
Enabling Packet Capture (CLI)

Follow the procedure given below to enable packet capture:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ap packet-capture start client-mac-address auto</td>
<td>Enables packet capture for the specified client on a set of nearby access points.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# ap packet-capture start 0011.0011.0011 auto</td>
<td></td>
</tr>
</tbody>
</table>

Create AP Packet Capture Profile and Map to an AP Join Profile (GUI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Click <strong>Configuration &gt; Tags &amp; Profiles &gt; AP Join Profile.</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>Add</strong> to create a new AP Join Profile and enter the requisite details.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Add AP Join Profile</strong> area, click <strong>AP &gt; Packet Capture.</strong></td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the <strong>Plus</strong> icon to create a new Packet Capture profile or select one from the drop-down menu.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Save.</strong></td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless profile ap packet-capture packet-capture-profile-name</td>
<td>Configures an AP profile.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# wireless profile ap packet-capture test1</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ap profile profile-name</td>
<td>Configures an AP packet capture profile.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# ap profile default-ap-profile</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>packet-capture profile-name</td>
<td>Enables packet capture on the AP profile.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-ap-profile)# packet-capture capture-test</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Exits the AP profile configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-ap-profile)# end</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>show wireless profile ap packet-capture detailed profile-name</td>
<td>Displays detailed information of the selected AP packet capture profile.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# show wireless profile ap packet-capture detailed test1</td>
<td></td>
</tr>
</tbody>
</table>

**Start or Stop Packet Capture**

Perform either of these tasks to start or stop a packet capture procedure.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>ap packet-capture start client-mac-address { auto</td>
<td>static ap-name }</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Device# ap packet-capture start&lt;br&gt;0011.0011.0011 auto</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ap packet-capture stop</strong> <em>client-mac-address</em>&lt;br&gt;{all</td>
<td>static <em>ap-name</em>}</td>
<td>Enables packet capture for a client.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Device# ap packet-capture stop&lt;br&gt;0011.0011.0011 all</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DHCP Option 82

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 Policy Tag
• DHCP AP Location
• DHCP VLAN ID

Configuring DHCP Option 82 Global Interface

Configuring Globally Through Server Override (CLI)

Procedure

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

Step 2 ip dhcp-relay information option server-override

Example: Device(config)# ip dhcp-relay information option server-override

Inserts global server override and link selection suboptions.

Configuring Globally Through Different SVIs (GUI)

Procedure

Step 1 Choose Configuration > VLAN > .
Step 2 Select a VLAN from the list. The Edit SVI screen appears.
Step 3  Click the Advanced tab.
Step 4  Choose the desired option from the IPv4 Inbound ACL drop-down list.
Step 5  Choose the desired option from the IPv4 Outbound ACL drop-down list.
Step 6  Choose the desired option from the IPv6 Inbound ACL drop-down list.
Step 7  Choose the desired 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 wish to enable the Relay Information Option setting.
Step 10 Enter the Subscriber ID.
Step 11 Set the status to Enabled if you wish to enable the Server ID Override setting.
Step 12 Set the status to Enabled if you wish to enable the Option Insert setting.
Step 13 Choose the desired option from the Source-Interface Vlan drop-down list.
Step 14 Click the Update & Apply to Device button.

### Configuring Globally Through Different SVIs (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ip dhcp-relay source-interface vlan vlan-id</td>
<td>Sets global source interface for relayed messages.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip dhcp-relay source-interface vlan 74</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring DHCP Option 82 Through Profile Policy

### Configuring DHCP Option 82 with the ap_ethmac Command (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td>Enables configuration for the specified policy profile.</td>
</tr>
<tr>
<td>Step 2 wireless profile policy  <em>policy-name</em></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless profile policy pp7</td>
<td></td>
</tr>
<tr>
<td>Step 3 shutdown</td>
<td>Shuts down the profile policy profile.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# shutdown</td>
<td></td>
</tr>
<tr>
<td>Step 4 vlan vlan-name</td>
<td>Assigns the profile policy to a VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# vlan 72</td>
<td></td>
</tr>
<tr>
<td>Step 5 session-timeout value-btwn-20-86400</td>
<td>(Optional) Sets the session timeout value in seconds. The range is between 20-86400.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)#</td>
<td></td>
</tr>
<tr>
<td>session-timeout 300</td>
<td></td>
</tr>
<tr>
<td>Step 6 idle-timeout value-btwn-15-100000</td>
<td>(Optional) Sets the idle-timeout value in seconds. The range is between 15-100000.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# idle-timeout 15</td>
<td></td>
</tr>
<tr>
<td>Step 7 central switching</td>
<td>Enables central switching.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# central</td>
<td></td>
</tr>
<tr>
<td>switching</td>
<td></td>
</tr>
<tr>
<td>Step 8 ipv4 dhcp opt82</td>
<td>Enables DHCP Option 82 for the wireless clients.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# ipv4 dhcp opt82</td>
<td></td>
</tr>
<tr>
<td>Step 9 ipv4 dhcp opt82 ascii</td>
<td>Enables ASCII on the DHCP Option 82 feature.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# ipv4 dhcp opt82 ascii</td>
<td></td>
</tr>
<tr>
<td>Step 10 ipv4 dhcp opt82 rid</td>
<td>(Optional) Supports the addition of Cisco 2 byte Remote ID (RID) for the DHCP Option 82 feature.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# ipv4 dhcp opt82 rid</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring DHCP Option 82 with the ap_location Command (CLI)

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Example:</em> Device(config-wireless-policy)# ipv4 dhcp opt82 format ap_ethmac</td>
<td>Enables DHCP Option 82 on the Ethernet port of the corresponding AP.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 12</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Example:</em> Device(config-wireless-policy)# no shutdown</td>
<td>Enables the profile policy.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring DHCP Option 82 with the apmac Command (CLI)

**Purpose**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>Enables central switching.</td>
</tr>
<tr>
<td>central switching</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# central switching</td>
<td></td>
</tr>
</tbody>
</table>

| Step 8            | Enables the DHCP Option 82 for the wireless clients. |
| ipv4 dhcp opt82   |         |
| Example:          |         |
| Device(config-wireless-policy)# ipv4 dhcp opt82 |         |

| Step 9            | (Optional) Enables ASCII on the DHCP Option 82 feature. |
| ipv4 dhcp opt82 ascii |         |
| Example:          |         |
| Device(config-wireless-policy)# ipv4 dhcp opt82 ascii |         |

| Step 10           | (Optional) Supports the addition of Cisco 2 byte Remote ID (RID) for the DHCP Option 82 feature. |
| ipv4 dhcp opt82 rid |         |
| Example:          |         |
| Device(config-wireless-policy)# ipv4 dhcp opt82 rid |         |

| Step 11           | Enables DHCP Option 82 on the corresponding AP. |
| ipv4 dhcp opt82 format ap_location |         |
| Example:          |         |
| Device(config-wireless-policy)# ipv4 dhcp opt82 format ap_location |         |

| Step 12           | Enables the profile policy. |
| no shutdown       |         |
| Example:          |         |
| Device(config-wireless-policy)# no shutdown |         |

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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-btw-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-btw-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: `Device(config-wireless-policy)# ipv4 dhcp opt82 ascii` | (Optional) Enables ASCII on the DHCP Option 82 feature. |
| **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 apmac`  
Example: `Device(config-wireless-policy)# ipv4 dhcp opt82 format apmac` | Enables DHCP Option 82 on the corresponding AP. |
| **Step 12** | `no shutdown`  
Example: | Enables the profile policy. |
### Configuring DHCP Option 82 with the apname Command (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wireless profile policy policy-name</code></td>
<td>Enables configuration for the specified profile policy.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# wireless profile policy pp7</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>shutdown</code></td>
<td>Shuts down the profile policy.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-wireless-policy)# shutdown</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>vlan vlan-name</code></td>
<td>Assigns the profile policy to the VLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-wireless-policy)# vlan 72</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>session-timeout value-btwn-20-86400</code></td>
<td>(Optional) Sets the session timeout value in seconds. The range is between 20-86400.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-wireless-policy)# session-timeout 300</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>idle-timeout value-btwn-15-100000</code></td>
<td>(Optional) Sets the idle timeout value in seconds. The range is between 15-100000.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-wireless-policy)# idle-timeout 15</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>central switching</code></td>
<td>Enables central switching.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-wireless-policy)# central switching</code></td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>ipv4 dhcp opt82</code></td>
<td>Enables DHCP Option 82 for the wireless clients.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-wireless-policy)# ipv4 dhcp opt82</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring DHCP Option 82 with a Policy Tag Command (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables configuration for the specified profile policy.</td>
</tr>
<tr>
<td>wireless profile policy policy-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless profile policy pp5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Shuts down the profile policy.</td>
</tr>
<tr>
<td>shutdown</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Assigns the profile policy to a VLAN.</td>
</tr>
<tr>
<td>vlan vlan-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# vlan vlan-name</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>vlan 72</code></td>
<td>Enables the creation of a VLAN.</td>
</tr>
<tr>
<td><code>session-timeout value-btwn-20-86400</code></td>
<td>Sets the session timeout value in seconds. The range is between 20-86400.</td>
</tr>
<tr>
<td><code>idle-timeout value-btwn-15-100000</code></td>
<td>Sets the idle timeout value in seconds. The range is between 15-100000.</td>
</tr>
<tr>
<td><code>central switching</code></td>
<td>Enables central switching.</td>
</tr>
<tr>
<td><code>ipv4 dhcp opt82</code></td>
<td>Enables DHCP Option 82 for the wireless clients.</td>
</tr>
<tr>
<td><code>ipv4 dhcp opt82 ascii</code></td>
<td>Enables ASCII on the DHCP Option 82 feature.</td>
</tr>
<tr>
<td><code>ipv4 dhcp opt82 rid</code></td>
<td>Supports the addition of Cisco 2 byte Remote ID (RID) for the DHCP Option 82 feature.</td>
</tr>
<tr>
<td><code>ipv4 dhcp opt82 format policy_tag</code></td>
<td>Enables DHCP Option 82 on the policy tag.</td>
</tr>
<tr>
<td><code>no shutdown</code></td>
<td>Enables the profile policy.</td>
</tr>
</tbody>
</table>
## Configuring DHCP Option 82 with the SSID Command (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>wireless profile policy policy-name</td>
<td>Enables configuration for the specified profile policy.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# wireless profile policy pp6</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>shutdown</td>
<td>Shuts down the profile policy.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)# shutdown</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>vlan vlan-name</td>
<td>Assigns the profile policy to a VLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)# vlan 72</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>session-timeout value-btwn-20-86400</td>
<td>(Optional) Sets the session timeout value in seconds. The range is between 20-86400.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)# session-timeout 300</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>idle-timeout value-btwn-15-100000</td>
<td>(Optional) Sets the idle timeout value in seconds. The range is between 15-100000.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)# idle-timeout 15</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>central switching</td>
<td>Enables central switching.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)# central switching</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>ipv4 dhcp opt82</td>
<td>Enables DHCP Option 82 for the wireless clients.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)# ipv4 dhcp opt82</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>ipv4 dhcp opt82 ascii</td>
<td>(Optional) Enables ASCII on the DHCP Option 82 feature.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring DHCP Option 82 with ap_ethmac and SSID Commands (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>wireless profile policy policy-name</code></td>
<td>Enables configuration for the specified profile policy.</td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# wireless profile policy pp7</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>shutdown</code></td>
<td>Shuts down the profile policy.</td>
</tr>
<tr>
<td></td>
<td><code>Device(config-wireless-policy)# shutdown</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>vlan vlan-name</code></td>
<td>Configures a VLAN.</td>
</tr>
<tr>
<td></td>
<td><code>Device(config-wireless-policy)# vlan 72</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>session-timeout value-between-20-86400</code></td>
<td>(Optional) Sets the session timeout value in seconds. The range is between 20-86400.</td>
</tr>
<tr>
<td></td>
<td><code>Device(config-wireless-policy)# session-timeout 800</code></td>
<td></td>
</tr>
</tbody>
</table>

#### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv4 dhcp opt82 ascii</code></td>
<td>(Optional) Supports the addition of Cisco 2 byte Remote ID (RID) for the DHCP Option 82 feature.</td>
</tr>
<tr>
<td><code>ipv4 dhcp opt82 rid</code></td>
<td>Enables DHCP Option 82 on the SSID.</td>
</tr>
<tr>
<td><code>ipv4 dhcp opt82 format ssid</code></td>
<td>Enables the profile policy.</td>
</tr>
</tbody>
</table>
### Configuring DHCP Option 82 with `ap_ethmac` and SSID Commands (CLI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td><code>idle-timeout value-btwn-15-100000</code></td>
<td><em>(Optional)</em> Sets the idle timeout value in seconds. The range is between 15-100000.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# <code>idle-timeout 15</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>central switching</code></td>
<td>Enables central switching.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# <code>central switching</code></td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>ipv4 dhcp opt82</code></td>
<td>Enables DHCP Option 82 for the wireless clients.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# <code>ipv4 dhcp opt82</code></td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td><code>ipv4 dhcp opt82 ascii</code></td>
<td><em>(Optional)</em> Enables ASCII on the DHCP Option 82 feature.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# <code>ipv4 dhcp opt82 ascii</code></td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td><code>ipv4 dhcp opt82 rid</code></td>
<td><em>(Optional)</em> Supports the addition of Cisco 2 byte Remote ID (RID) for the DHCP Option 82 feature.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# <code>ipv4 dhcp opt82 rid</code></td>
<td></td>
</tr>
<tr>
<td>Step 11</td>
<td><code>ipv4 dhcp opt82 format ap_ethmac</code></td>
<td>Enables DHCP Option 82 on the AP Ethernet MAC.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# <code>ipv4 dhcp opt82 format ap_ethmac</code></td>
<td></td>
</tr>
<tr>
<td>Step 12</td>
<td><code>ipv4 dhcp opt82 format ssid</code></td>
<td>Enables DHCP Option 82 on an SSID.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# <code>ipv4 dhcp opt82 format ssid</code></td>
<td></td>
</tr>
<tr>
<td>Step 13</td>
<td><code>no shutdown</code></td>
<td>Enables the profile policy.</td>
</tr>
</tbody>
</table>
## Configuring DHCP Option 82 with the `ap_mac` and `vlan_id` Commands (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> &lt;br&gt;Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>wireless profile policy</code> <code>policy-name</code></td>
<td>Enables configuration for the specified profile policy.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> &lt;br&gt;Device(config)# <code>wireless profile policy pp8</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>shutdown</code></td>
<td>Shuts down the profile policy.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> &lt;br&gt;Device(config-wireless-policy)# <code>shutdown</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>vlan</code> <code>vlan-name</code></td>
<td>Assigns the profile policy to a VLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> &lt;br&gt;Device(config-wireless-policy)# <code>vlan 72</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>session-timeout</code> <code>value-btwn-20-86400</code></td>
<td>(Optional) Sets the session timeout value in seconds. The range is between 20-86400.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> &lt;br&gt;Device(config-wireless-policy)# <code>session-timeout 300</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>idle-timeout</code> <code>value-btwn-15-100000</code></td>
<td>(Optional) Sets the idle timeout value in seconds. The range is between 15-100000.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> &lt;br&gt;Device(config-wireless-policy)# <code>idle-timeout 15</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>central switching</code></td>
<td>Enables central switching.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> &lt;br&gt;Device(config-wireless-policy)# <code>central switching</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>ipv4 dhcp opt82</code></td>
<td>Enables DHCP Option 82 for the wireless clients.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> &lt;br&gt;Device(config-wireless-policy)# <code>ipv4 dhcp opt82</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>ipv4 dhcp opt82 ascii</code></td>
<td>(Optional) Enables ASCII on the DHCP Option 82 feature.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring DHCP Option 82 with the `ap_name` Command and a VLAN ID (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables configuration for the specified profile policy.</td>
</tr>
<tr>
<td><code>wireless profile policy policy-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# wireless profile policy pp9</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Shuts down the profile policy.</td>
</tr>
<tr>
<td><code>shutdown</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-wireless-policy)# shutdown</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Assigns the profile policy to a VLAN.</td>
</tr>
<tr>
<td><code>vlan vlan-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Device(config-wireless-policy)# vlan 72</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

**Purpose:** (Optional) Sets the session timeout value in seconds. The range is between 20-86400.

**Example:**

```plaintext
Device(config-wireless-policy)# session-timeout value-between-20-86400
```

**Step 6**

**Purpose:** (Optional) Sets the idle timeout value in seconds. The range is between 15-100000.

**Example:**

```plaintext
Device(config-wireless-policy)# idle-timeout value-between-15-100000
```

**Step 7**

**Purpose:** Enables central switching.

**Example:**

```plaintext
Device(config-wireless-policy)# central switching
```

**Step 8**

**Purpose:** Enables DHCP Option 82 for the wireless clients.

**Example:**

```plaintext
Device(config-wireless-policy)# ipv4 dhcp opt82
```

**Step 9**

**Purpose:** (Optional) Enables ASCII on the DHCP Option 82 feature.

**Example:**

```plaintext
Device(config-wireless-policy)# ipv4 dhcp opt82 ascii
```

**Step 10**

**Purpose:** (Optional) Supports the addition of Cisco 2 byte Remote ID (RID) for the DHCP Option 82 feature.

**Example:**

```plaintext
Device(config-wireless-policy)# ipv4 dhcp opt82 rid
```

**Step 11**

**Purpose:** Enables DHCP Option 82 on the AP.

**Example:**

```plaintext
Device(config-wireless-policy)# ipv4 dhcp opt82 format apname
```

**Step 12**

**Purpose:** Enables DHCP Option 82 on the VLAN.

**Example:**

```plaintext
Device(config-wireless-policy)# ipv4 dhcp opt82 format vlan_id
```

**Step 13**

**Purpose:** Enables the profile policy.

**Example:**

```plaintext
Device(config-wireless-policy)# no shutdown
```
## Configuring DHCP Option 82 with the ap_ethmac Command and server override enabled (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>wireless profile policy policy-name</code></td>
<td>Enables configuration for the specified profile policy.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Device(config)# <code>wireless profile policy ppi0</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>shutdown</code></td>
<td>Shuts down the profile policy.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# <code>shutdown</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>vlan vlan-name</code></td>
<td>Assigns the profile policy to a VLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# <code>vlan 72</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>session-timeout value=btwn-20-86400</code></td>
<td>(Optional) Sets the session timeout value in seconds. The range is between 20-86400.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# <code>session-timeout 300</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>idle-timeout value=btwn-15-100000</code></td>
<td>(Optional) Sets the idle timeout value in seconds. The range is between 15-100000.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# <code>idle-timeout 15</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>central switching</code></td>
<td>Enables central switching.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# <code>central switching</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>ipv4 dhcp opt82</code></td>
<td>Enables DHCP Option 82 for the wireless clients.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# <code>ipv4 dhcp opt82</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring DHCP Option 82 Through a VLAN Interface

#### Configuring DHCP Option 82 Through Option-Insert Command (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface vlan vlan-id</td>
<td>Configures a VLAN ID.</td>
</tr>
<tr>
<td>Example: Device(config)# interface vlan 72</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring DHCP Option 82 Through the server-ID-override Command (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures a VLAN ID.</td>
</tr>
<tr>
<td>interface vlan vlan-id</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface vlan 72</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Inserts the server id override and link selection suboptions.</td>
</tr>
<tr>
<td>ip dhcp relay information option server-id-override</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ip dhcp relay information option server-id-override</td>
<td></td>
</tr>
</tbody>
</table>

---

### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Inserts relay information in BOOTREQUEST.</td>
</tr>
<tr>
<td>ip dhcp relay information option-insert</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ip dhcp relay information option-insert</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures the IP address for the interface.</td>
</tr>
<tr>
<td>ip address ip-address</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ip address 9.3.72.38 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures the destination address for UDP broadcasts.</td>
</tr>
<tr>
<td>ip helper-address ip-address</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ip helper-address 9.3.72.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Disables the MOP for an interface.</td>
</tr>
<tr>
<td>[no] mop enabled</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# no mop enabled</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Disables the task of sending MOP periodic system ID messages.</td>
</tr>
<tr>
<td>[no] mop sysid</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-apgroup)# [no] mop sysid</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring DHCP Option 82 Through a Subscriber-ID (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>interface vlan vlan-id</td>
<td>Configures a VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# interface vlan 72</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ip dhcp relay information option subscriber-id subscriber-id</td>
<td>Inserts the subscriber identifier suboption.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# ip dhcp relay information option subscriber-id test10</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>ip address ip-address</td>
<td>Configures the IP address for the interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# ip address 9.3.72.38 255.255.255.0</td>
<td></td>
</tr>
</tbody>
</table>
**Configuring DHCP Option 82 Through server-ID-override and subscriber-ID Commands (CLI)**

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>interface vlan <code>vlan-id</code></td>
<td>Configures a VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# interface vlan 72</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>ip dhcp relay information option server-id-override</code></td>
<td>Inserts server ID override and link selection suboptions.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# ip dhcp relay information option server-id-override</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>ip dhcp relay information option subscriber-id subscriber-id</code></td>
<td>Inserts the subscriber identifier suboption.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# ip dhcp relay information option subscriber-id test10</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>ip address ip-address</code></td>
<td>Configures the IP address for the interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**
- **Step 5**
  ```
  Device(config-if)# ip helper-address 9.3.72.1
  ```
- **Step 6**
  ```
  Device(config-if)# no mop enabled
  ```
- **Step 7**
  ```
  Device(config-apgroup)# [no] mop sysid
  ```
### Configuring DHCP Option 82 Through Different SVIs (CLI)

**Purpose**

**Command or Action**

<table>
<thead>
<tr>
<th><strong>Step</strong></th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface vlan vlan-id</code></td>
<td>Configures a VLAN ID.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# interface vlan 72</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip dhcp relay source-interface vlan vlan-id</code></td>
<td>Configures a source interface for relayed messages on a VLAN ID.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-if)# ip dhcp relay source-interface vlan 74</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>ip address ip-address</code></td>
<td>Configures the IP address for the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-if)# ip address 9.3.72.38 255.255.255.0</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>ip helper-address ip-address</code></td>
<td>Configure the destination address for UDP broadcasts.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-if)# ip helper-address 9.3.72.1</code></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>6</td>
<td>[no] mop enabled</td>
<td>Disables the MOP for an interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# no mop enabled</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>[no] mop sysid</td>
<td>Disables the task of sending MOP periodic system ID messages.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-apgroup)# [no] mop sysid</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 36

RADIUS Realm

- Information About RADIUS Realm, on page 301
- Enabling RADIUS Realm, on page 302
- Configuring Realm to Match the RADIUS Server for Authentication and Accounting, on page 302
- Configuring the AAA Policy for a WLAN, on page 303
- Verifying the RADIUS-Realm Configuration, on page 305

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:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless aaa policy aaa-policy</td>
<td>Creates a new AAA policy.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# wireless aaa policy policy-1</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>aaa-realm enable</td>
<td>Enables AAA RADIUS realm selection.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-aaa-policy)# aaa-realm enable</td>
<td></td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
Configuring the AAA Policy for a WLAN

Follow the procedure given below to configure the AAA policy for a WLAN:

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless aaa policy aaa-policy-name</td>
<td>Creates a new AAA policy for wireless.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wireless aaa policy aaa-policy-1</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>3</td>
<td>aaa-realm enable</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-aaa-policy)# aaa-realm enable</td>
</tr>
<tr>
<td>4</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-aaa-policy)# exit</td>
</tr>
<tr>
<td>5</td>
<td>wireless profile policy wlan-policy-profile</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless profile policy wlan-policy-a</td>
</tr>
<tr>
<td>6</td>
<td>aaa-policy aaa-policy</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# aaa-policy aaa-policy-1</td>
</tr>
<tr>
<td>7</td>
<td>accounting-list acct-config-realm</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# accounting-list cisco.com</td>
</tr>
<tr>
<td>8</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# exit</td>
</tr>
<tr>
<td>9</td>
<td>wlan wlan-name wlan-id ssid</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wlan wlan2 14 wlan-aaa</td>
</tr>
<tr>
<td>10</td>
<td>security dot1x authentication-list auth-list-realm</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# security dot1x authentication-list cisco.com</td>
</tr>
<tr>
<td>11</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# exit</td>
</tr>
<tr>
<td>12</td>
<td>wireless tag policy policy</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless tag policy tag-policy-1</td>
</tr>
</tbody>
</table>
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 : sactoma@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

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 13</strong> wlan wlan-name policy policy-profile</td>
<td>Maps a policy profile to the WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-policy-tag)# wlan Abc-wlan policy wlan-policy-a</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-policy-tag)# exit</td>
<td></td>
</tr>
</tbody>
</table>
NPU 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: 09770490000000DF4607B3B
  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
Client Statistics:
  Number of Bytes Received : 0
  Number of Bytes Sent : 0
  Number of Packets Received : 0
  Number of Packets Sent : 0
  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
Verifying the RADIUS-Realm Configuration
Introduction to Accounting of AP Events

This section describes the configuration of the RADIUS server to monitor the network with regards to APs. Earlier, during times of network issues, the controller would not send accounting messages when APs join and disjoin from the controller. Currently, if an AP goes down and comes up again, the RADIUS server keeps a record of all the APs that were down and have come up.

- Configuring Accounting Method-List for an AP Profile, on page 309
- Verifying the AP Accounting Information, on page 310

Configuring Accounting Method-List for an AP Profile

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Configure terminal</strong>&lt;br&gt;<strong>Example:</strong> Device#Configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>ap profile</strong> ap-profile-name&lt;br&gt;<strong>Example:</strong> Device(config)# ap profile ap-profile-name</td>
<td>Configures the AP profile. The default AP join profile name is default-ap-profile.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>[no] accounting method-list</strong> method-list-name&lt;br&gt;<strong>Example:</strong> Device(config-ap-profile)# [no] accounting method-list method-list-name</td>
<td>Configures accounting method-list for the AP profile. Use the <strong>no</strong> form of the command to disable the command.</td>
</tr>
</tbody>
</table>

**Example**

Device#Configure terminal
Device(config)# ap profile ap-profile-name
Device(config-ap-profile)# accounting method-list ap-method-list-name
Verifying the AP Accounting Information

To verify the AP accounting information, use the following command:

```plaintext
Device#show wireless stats ap accounting
Base MAC    Total packet Send  Total packet Received Methodlist
------------------------------------------------------------------------
00b0.e192.0f20  4    3   abc
38ed.18cc.5788  8    8   ML_M
70ea.1ae0.af08  0    0   ML_A
```

To view the details of the method-list configured to an ap profile, use the following command:

```plaintext
Device#sh ap profile name Method-list name detailed
Method-list name: "Method-list name"
```
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 Wireless Controller Parameters for Cisco StadiumVision (GUI)

**Procedure**

1. **Step 1** Choose **Configuration > Wireless > Advanced**.
2. **Step 2** Click the **High Density** tab.
3. **Step 3** In the **Multicast Data Rate** section, set the data rate for 5 GHz radio or 2.4 GHz radio using the drop downs.
4. **Step 4** Click **Apply**.

Configure Wireless Controller Parameters for Cisco StadiumVision (CLI)

**Note**

Multicast buffer and data rate configurations are supported for all AP models.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>wlan wlan-name wlan-id</strong></td>
<td>Configures a WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wlan wlan1 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>multicast buffer multicast-buffer-number</strong></td>
<td>Configures enhanced multicast buffer size between 30 (default) and 60 on a WLAN.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You can enable only two out of the possible 512 WLANs configured on Controller embedded wireless controller for enhanced multicast buffers.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# multicast buffer 45</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**ap dot11 [5ghz</td>
<td>24ghz] multicast data-rate rate**</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap dot11 [5ghz</td>
<td>24ghz] rx-sop threshold custom -70</td>
</tr>
<tr>
<td><strong>By default, the configuration is disabled and it’s value is set to auto. If the RxSOP value of</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 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 Size : Enabled
Multicast Buffer Size : 45

Device#

Device#sh wlan name vwlc-OpenAuth | inc Buffer
Multicast Buffer Size : Enabled
Multicast Buffer Size : 45

Device#

#### Multicast Data Rate

Device#sh ap dot11 24ghz high-density

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Mac Address</th>
<th>Slot</th>
<th>Rx sop</th>
</tr>
</thead>
<tbody>
<tr>
<td>test-1800-AP</td>
<td>aaaa.bbbb.cccc</td>
<td>0</td>
<td>auto</td>
</tr>
<tr>
<td>0</td>
<td>54</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AP4001.7AB2.BEB6</td>
<td>aabb.bbbb.cccc</td>
<td>2</td>
<td>auto</td>
</tr>
<tr>
<td>0</td>
<td>54</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AP70DF.2FA2.72EE</td>
<td>aaac.bbbb.cccc</td>
<td>0</td>
<td>auto</td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Device#show ap dot11 5ghz high-density

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Mac Address</th>
<th>Slot</th>
<th>Rx sop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saji-1800-AP</td>
<td>aaab.bbbb.cccc</td>
<td>1</td>
<td>auto</td>
</tr>
<tr>
<td>0</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Saji-2802I-AP</td>
<td>aaab.bbbb.cccc</td>
<td>0</td>
<td>custom</td>
</tr>
<tr>
<td>-82</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Saji-2802I-AP</td>
<td>aaac.bbbb.cccc</td>
<td>1</td>
<td>custom</td>
</tr>
<tr>
<td>-82</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AP4001.7AB2.BEB6</td>
<td>aaad.bbbb.cccc</td>
<td>0</td>
<td>custom</td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Device# 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#
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.

Configuring Persistent SSID Broadcast

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ap profile ap-profile-name</td>
<td>Configures the AP profile.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# ap profile ap-profile-name</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>[no]ssid broadcast persistent</td>
<td>The ssid broadcast command configures the SSID broadcast mode. The persistent keyword enables a persistent SSID broadcast, where the</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Device(config-ap-profile)# [no] ssid broadcast persistent</td>
<td>associated APs will re-join. Use the [no] command to disable the feature.</td>
<td></td>
</tr>
</tbody>
</table>

**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
```
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
```

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>
</site-cfg-data>
```

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>  # show ap summary "Country Code"
                <name>AP_A-1</name>  # show ap summary "AP Name"
                ...
            </capwap-data>
        </radio-oper-data>
    </access-point-oper-data>
</data>
```
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:**

```
  <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"
  </common-oper-data>
</client-oper-data>
```

---

**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"
    <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'
  <subscription-id xmlns='urn:ietf:params:xml:ns:yang:ietf-event-notifications'>2147483652</subscription-id>
</rpc-reply>
```
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>
          <wtb-mac>00ab11006600</wtb-mac>
        </capwap-data>
      </value>
    </edit>
  </yang-patch>
</datastore-changes-xml>
<<--
Creating a Lobby Ambassador Account

Information About Lobby Ambassador Account

An administrator can create a lobby ambassador user for creating guest users only.

A lobby ambassador sets the following parameters on the guest user:

- Guest user creation and deletion.
- Password.
- Lifetime of the user.
- Guest role profiles (QoS profiles that should be applied on the guest using AAA attribute list).

Note

You can create a lobby admin from a RADIUS or TACACS server, instead of locally creating one.

Only the admin can create WLAN and web authentication policies. Also, the admin can create AAA attribute list, which the lobby administrator can use to map it to its guest user.

Creating a Lobby Ambassador Account (GUI)

You can configure administrator or lobby usernames and passwords to prevent unauthorized users from reconfiguring the controller and viewing configuration information.
Creating a User Account

Procedure

Step 1  On the Administration > User Administration page, click Add.
Step 2  Enter a user name for the new account.
Step 3  Specify the policy that you want to associate with the user.
Step 4  Specify the privilege level that you want to associate with the user. The privilege level defines what commands the user can enter using the CLI after they have logged into the device. Privilege 1 allows access in User Exec mode, privilege 15 allows access in Privileged Exec mode.

Note  To create a lobby admin user, specify the privilege as lobby-admin.

Step 5  Specify a password with which to authenticate access to the device.
Step 6  Specify the password again to re-confirm.
Step 7  Click Save & 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>user-name user-name</strong></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>Device(config)# user-name lobby</code></td>
<td></td>
</tr>
</tbody>
</table>
| **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 lobby` | Creates a password for the lobby administrator account. |
| **Step 5** exit **Example:**  
  `Device(config-user-name)# exit` | Returns to global configuration mode. |
Configuring Guest User Accounts

- Information About Creating Guest User Accounts, on page 325
- Creating a Guest User Account (GUI), on page 325
- Creating a Guest User Account (CLI), on page 326
- Verifying Guest User Account, on page 327

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.

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.
Creating a Guest User Account (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>user-name guest-user-name</td>
<td>Creates a guest user account.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# user-name guest</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>type network-user description description guest-user max-login-limit number of simultaneous logins lifetime year y y month mm day day hour hour minute minute second second</td>
<td>Specifies the account type as guest user account.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-user-name)# type network-user description sample-description guest-user max-login-limit 3 lifetime year 2 month 3 day 23 hour 6 minute 30 second 15</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>password 0 password</td>
<td>Creates a password for the guest user account.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-user-name)# password 0 guest</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>aaa attribute list aaa-attribute-list-name</td>
<td>Creates a AAA attribute list to apply QoS profiles on the guest user account.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-user-name)# aaa attribute list aaa-attribute-list-name</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Device(config-user-name)# exit | 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`

<table>
<thead>
<tr>
<th>User-Name</th>
<th>Type</th>
<th>Password</th>
<th>Is_passwd_encrypted</th>
<th>Attribute-List</th>
<th>Viewname</th>
<th>Lobby Admin Name</th>
<th>Max Login Limit</th>
<th>Description</th>
<th>Start-Time</th>
<th>Lifetime</th>
<th>Expiry-Time</th>
<th>Remaining Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>new4</td>
<td>GUEST USER</td>
<td>*</td>
<td>No</td>
<td>Not-Configured</td>
<td>Not-Configured</td>
<td>NEW_LOBBY_ADMIN</td>
<td>0</td>
<td>guest</td>
<td>07:56:39 IST Jan 25 2019</td>
<td>1 years 0 months 0 days 0 hours 0 mins 0 secs</td>
<td>07:56:39 IST Jan 30 2020</td>
<td>0 years 11 months 29 days 22 hours 52 mins 49 secs</td>
</tr>
</tbody>
</table>

To verify a specific guest user account, use the following command:

Device# `show aaa local guest_user new_guest3`

<table>
<thead>
<tr>
<th>User-Name</th>
<th>Type</th>
<th>Password</th>
<th>Is_passwd_encrypted</th>
<th>Attribute-List</th>
<th>Viewname</th>
<th>Lobby Admin Name</th>
<th>Max Login Limit</th>
<th>Description</th>
<th>Start-Time</th>
<th>Lifetime</th>
<th>Expiry-Time</th>
<th>Remaining Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>new_guest3</td>
<td>GUEST USER</td>
<td>*</td>
<td>No</td>
<td>Not-Configured</td>
<td>Not-Configured</td>
<td>INVALID_ADMIN</td>
<td>9</td>
<td>new</td>
<td>04:39:01 IST Feb 4 2019</td>
<td>1 years 0 months 0 days 0 hours 0 mins 0 secs</td>
<td>04:39:01 IST Jan 30 2020</td>
<td>0 years 11 months 11 days 21 hours 16 mins 34 secs</td>
</tr>
</tbody>
</table>
Verifying Guest User Account
PART V

System Management

• Network Mobility Services Protocol, on page 331
• Application Visibility and Control, on page 345
• Cisco Hyperlocation, on page 367
• FastLocate for Cisco Catalyst Series Access Points, on page 379
• BLE Beacons in CiscoWave 2 Access Points, on page 383
• Cisco DNA Spaces, on page 389
• EDCA Parameters, on page 393
• 802.11 parameters and Band Selection, on page 397
• Predownloading an Image to an Access Point, on page 419
• Efficient Image Upgrade, on page 423
• Hitless Upgrade, on page 429
• Wireless Sub-Package for Switch, on page 433
• NBAR Protocol Discovery, on page 439
• NBAR Dynamic Protocol Pack Upgrade, on page 441
• Conditional Debug, Radioactive Tracing, and Packet Tracing, on page 445
• Aggressive Client Load Balancing, on page 457
• Accounting Identity List, on page 461
• Wireless Multicast, on page 465
• Map-Server Per-Site Support, on page 485
• Volume Metering, on page 493
• Enabling Syslog Messages in Access Points and Controller for Syslog Server, on page 495
• Login Banner, on page 505
• Software Maintenance Upgrade, on page 507
• In-Service Software Upgrade, on page 521
• WiFi Alliance Agile Multiband, on page 529
Cisco Network Mobility Services Protocol (NMSP) is a secure two-way protocol that can be run over a connection-oriented (TLS) or connection-less (DTLS) 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 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.

NMSP essentially provides a way to the applications in the controller to talk to the outside world. The NMSP in Cisco Catalyst 9800 Series Wireless Controller also provides the flexibility to change the protocol to talk to the outside world.

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.
• When web sockets are used, 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>nmsp enable</td>
<td>Enables NMSP on premises services.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# nmsp enable</td>
<td></td>
</tr>
</tbody>
</table>

Note: By default, the NMSP is enabled on the controller.

Step 3 | end                     | Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode. |
|        | Example:                |                                              |
|        | Device(config)# end     |                                              |
Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues

NMSP manages communication between the Cisco Mobility Services Engine (Cisco MSE) 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.

The TCP port (16113) that the controller and Cisco MSE communicate over must be open (not blocked) on any firewall that exists between the controller and the Cisco MSE for NMSP to function.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>`nmsp notification interval {rssi</td>
<td>clients</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# nmsp notification interval rssi rfid 50</code></td>
<td><code>interval</code>-NMSP notification interval value, in seconds for RSSI measurement. Valid range is from 1 to 180.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

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

Procedure

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>nmmsp strong-cipher</code></td>
<td>Enable strong ciphers for NMSP server.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# <code>nmmsp strong-cipher</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>

### Verifying NMSP Settings

To view the NMSP capabilities of the controller, use the following command:

```
Device# show nmssp 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 nmssp 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:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Echo Request</td>
<td>6076</td>
</tr>
<tr>
<td>7</td>
<td>Capability Notification</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>Measurement Request</td>
<td>5</td>
</tr>
<tr>
<td>16</td>
<td>Information Request</td>
<td>3</td>
</tr>
<tr>
<td>20</td>
<td>Statistics Request</td>
<td>2</td>
</tr>
<tr>
<td>30</td>
<td>Service Subscribe Request</td>
<td>1</td>
</tr>
</tbody>
</table>

Tx Message Counters:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Echo Response</td>
<td>6076</td>
</tr>
<tr>
<td>7</td>
<td>Capability Notification</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>Measurement Response</td>
<td>13</td>
</tr>
<tr>
<td>15</td>
<td>Measurement Notification</td>
<td>91120</td>
</tr>
<tr>
<td>17</td>
<td>Information Response</td>
<td>6</td>
</tr>
<tr>
<td>18</td>
<td>Information Notification</td>
<td>7492</td>
</tr>
<tr>
<td>21</td>
<td>Statistics Response</td>
<td>2</td>
</tr>
<tr>
<td>22</td>
<td>Statistics Notification</td>
<td>305</td>
</tr>
<tr>
<td>31</td>
<td>Service Subscribe Response</td>
<td>1</td>
</tr>
<tr>
<td>67</td>
<td>AP Info Notification</td>
<td>304</td>
</tr>
</tbody>
</table>

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
Verifications failures: 6
Verifications 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
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-address
```

CMX IP address: 127.0.0.1
CMX Group name: Group1
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-address
```

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 00:00:00:60:00:02 00:00:00:02:00:02 00:00:00:00:40:02
- 00:00:00:00:00:02 00:00:00:00:a0:02 00:00:77:00:00:02 00:22:00:00:00:02
- 00:00:00:00:00:02 00:00:00:00:00:82 00:00:00:00:03:02 aa:00:00:00:00:02
- 00:00:00:00:00:02 00:00:00:00:00:02 00:00:00:00:00:02 01:00:00:00:00:02
- 00:00:00:00:00:02 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:
- 00:00:00:00:03:00 00:00:00:00:02:00 00:00:00:00:01:00

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

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

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>wireless probe filter</td>
<td>Enables filtering of unacknowledged probe requests from AP to improve the location accuracy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless probe filter</td>
<td>Use the no form of the command to disable the feature. This will forward both acknowledged and unacknowledged probe requests to the controller.</td>
</tr>
</tbody>
</table>
### Command or Action

| Step 3 | wireless probe limit *limit-value interval*  
|        | Example:  
|        | Device(config)# wireless probe limit 10  
|        | 100  

**Purpose:** 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 | location algorithm rssi-average  
|        | Example:  
|        | Device(config)# location algorithm rssi-average  

**Purpose:** Sets the probe RSSI measurement updates to a more accurate algorithm but with more CPU overhead.

| Step 5 | 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 6 | location expiry client *interval*  
|        | Example:  
|        | Device(config)# location expiry client 300  

**Purpose:** Configures the timeout for RSSI values. The `no` form of the command sets it to a default value of 15.

| Step 7 | location notify-threshold client *threshold-db*  
|        | Example:  
|        | Device(config)# location notify-threshold client 5  

**Purpose:** Configures the notification threshold for clients. The `no` form of the command sets it to a default value of 0.

| Step 8 | location rssi-half-life client *time-in-seconds*  
|        | Example:  
|        | Device(config)# location rssi-half-life client 20  

**Purpose:** 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 RFID tags 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

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless rfid</td>
<td>Enables RFID tag tracking.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless rfid</td>
<td>The default value is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the no form of this command to disable RFID tag tracking.</td>
</tr>
<tr>
<td>Step 3</td>
<td>wireless rfid timeout timeout-value</td>
<td>Configures the RFID tag data timeout value to cleanup the table.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless rfid timeout 90</td>
<td>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 (approximately three times the beacon value). The default value is 1200 seconds.</td>
</tr>
</tbody>
</table>

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>
To view the summary information for all known RFID tags, use the following command:

```
Device# show wireless rfid summary
```

To view the location-based system RFID statistics, use the following command:

```
Device# show wireless rfid stats
```
RFID smallest rssi expired 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
Application Visibility and Control

- Information About Application Visibility and Control, on page 345
- Create a Flow Monitor, on page 348
- Create a Flow Record, on page 349
- Create a Flow Exporter, on page 351
- Configure a WLAN for AVC, on page 352
- Configuring a Policy Tag, on page 353
- Attaching a Policy Profile to a WLAN Interface (GUI), on page 354
- Attaching a Policy Profile to a WLAN Interface (CLI), on page 354
- Attaching a Policy Profile to an AP, on page 355
- Verify the AVC Configuration, on page 356
- Default DSCP on AVC, on page 357
- AVC-Based Selective Reanchoring, on page 359
- Restrictions for AVC-Based Selective Reanchoring, on page 359
- Configuring the Flow Exporter, on page 359
- Configuring the Flow Monitor, on page 360
- Configuring the AVC Reanchoring Profile, on page 360
- Configuring the Wireless WLAN Profile Policy, on page 361
- Verifying AVC Reanchoring, on page 362

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.
- Provides only limited support for NetFlow exporter.
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.

<table>
<thead>
<tr>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# flow monitor fm_avc</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
</tbody>
</table>
### Command or Action

**Device(config-flow-monitor)# record wireless avc ipv6 basic**

### Purpose

**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 4

**cache timeout active value**

**Example:**

Device(config-flow-monitor)# cache timeout active 60

Sets the active flow timeout in seconds.

### Step 5

**cache timeout inactive value**

**Example:**

Device(config-flow-monitor)# cache timeout inactive 60

Sets the inactive flow timeout in seconds.

---

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> flow record <code>flow_record_name</code></td>
<td>Creates a flow record.</td>
</tr>
<tr>
<td>Example: Device(config)# flow record record1</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 2</strong> description <code>string</code></td>
<td>(Optional) Describes the flow record as a maximum 63-character string.</td>
</tr>
<tr>
<td>Example: Device(config-flow-record)# description IPv4 flow</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> match ipv4 protocol</td>
<td>Specifies a match to the IPv4 protocol.</td>
</tr>
<tr>
<td>Example: Device(config-flow-record)# match ipv4 protocol</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> match ipv4 source address</td>
<td>Specifies a match to the IPv4 source address-based field.</td>
</tr>
<tr>
<td>Example: Device(config-flow-record)# match ipv4 source address</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> match ipv4 destination address</td>
<td>Specifies a match to the IPv4 destination address-based field.</td>
</tr>
<tr>
<td>Example: Device(config-flow-record)# match ipv4 destination address</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> match transport source-port</td>
<td>Specifies a match to the transport layer's source port field.</td>
</tr>
<tr>
<td>Example: Device(config-flow-record)# match transport source-port</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> match transport destination-port</td>
<td>Specifies a match to the transport layer's destination port field.</td>
</tr>
<tr>
<td>Example: Device(config-flow-record)# match transport destination-port</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> match flow direction</td>
<td>Specifies a match to the direction the flow was monitored in.</td>
</tr>
<tr>
<td>Example: Device(config-flow-record)# match flow direction</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> match application name</td>
<td>Specifies a match to the application name.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
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.

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.
## Configure a WLAN for AVC

Follow the procedure given below to configure a WLAN for AVC:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>flow exporter</strong> flow-export-name</td>
<td>Creates a flow monitor.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# flow exporter export-test</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>description</strong> string</td>
<td>Describes the flow record as a maximum 63-character string.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-flow-exporter)# description IPv4flow</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>destination</strong> {hostname/ipv4address</td>
<td>hostname/ipv6address</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-flow-exporter) # destination local wlc</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>transport udp</strong> port-value</td>
<td>Configures a port value for the UDP protocol.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-flow-exporter) # transport udp 2</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>option application-table timeout</strong> seconds</td>
<td>(Optional) Specifies the application table timeout option, in seconds. The valid range is from 1 to 86400.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-flow-exporter)# option application-table timeout 500</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>option usermac-table timeout</strong> seconds</td>
<td>(Optional) Specifies the wireless usermac-to-username table option, in seconds. The valid range is from 1 to 86400.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-flow-exporter)# option usermac-table timeout 1000</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><strong>show flow exporter</strong></td>
<td>(Optional) Verifies your configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device # show flow exporter</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Policy Tag

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>wireless tag policy policy-tag-name</code></td>
<td>Configures policy tag and enters policy tag</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>configuration mode.</td>
</tr>
<tr>
<td>Device(config-policy-tag)# wireless tag policy policy</td>
<td></td>
</tr>
<tr>
<td>rr-xyz-policy-tag</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Saves the configuration and exits configuration</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Device(config-policy-tag)# end</td>
<td></td>
</tr>
</tbody>
</table>
Attaching a Policy Profile to a WLAN Interface (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configuration &gt; Tags &amp; Profiles &gt; Tags</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the <strong>Manage Tags</strong> page, click <strong>Policy</strong> tab.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Add</strong> to view the <strong>Add Policy Tag</strong> window.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter a name and description for the policy tag.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Add</strong> to map WLAN and policy.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click <strong>Save &amp; Apply to Device</strong>.</td>
</tr>
</tbody>
</table>

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:

```plaintext
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:

```plaintext
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
```
In this example, a policy profile with and without AVC is applied to the same WLAN in different tags.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 wireless tag policy avc-tag</td>
<td>Creates a policy tag.</td>
</tr>
<tr>
<td>Example: Device(config)# wireless tag policy avc-tag</td>
<td></td>
</tr>
<tr>
<td>Step 2 wlan wlan-avc policy avc-policy</td>
<td>Attaches a policy profile to a WLAN profile.</td>
</tr>
<tr>
<td>Example: Device(config-policy-tag)# wlan wlan_avc policy avc_pol</td>
<td></td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 ap ap-ether-mac</td>
<td>Enters AP configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# ap 34a8.2ec7.4cf0</td>
<td></td>
</tr>
<tr>
<td>Step 2 policy-tag policy-tag</td>
<td>Specifies the policy tag that is to be attached to the access point.</td>
</tr>
<tr>
<td>Example: Device(config)# policy-tag avc-tag</td>
<td></td>
</tr>
</tbody>
</table>
## Verify the AVC Configuration

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `show avc wlan wlan-name top num-of-applications applications {aggregate | downstream | upstream}` | 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. |
| **Example:** | Device# show avc wlan wlan_avc top 2 applications aggregate |
| Step 2 | `show avc client mac top num-of-applications applications {aggregate | downstream | upstream}` | 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. |
| **Example:** | Device# show avc client 9.3.4 top 3 applications aggregate |
| Step 3 | `show avc wlan wlan-name application app-name top num-of-clients aggregate` | Displays information about top applications and users using these applications. |
| **Example:** | Device# show avc wlan wlan_avc application app top 4 aggregate |
| Step 4 | `show ap summary` | Displays a summary of all the access points attached to the controller. |
| **Example:** | Device# show ap summary |
| Step 5 | `show ap tag summary` | Displays a summary of all the access points with policy tags. |
| **Example:** | Device# show ap tag summary |
Default DSCP on AVC

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

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Configure Terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>class class-map-name</strong></td>
<td>Creates a class map.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-pmap)# class-map avc-class</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>match protocol</strong></td>
<td>Specifies match to the application name, category name, subcategory name, or application group.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# class-map avc-class</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-cmap)# match protocol avc-media</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# class-map class-avc-category</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-cmap)# match protocol attribute category avc-media</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# class-map class-avc-sub-category</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-cmap)# match protocol attribute sub-category avc-media</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# class-map avcS-webex-application-group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-cmap)# match protocol attribute application-group webex-media</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>end</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
## Creating Policy Map

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Configure Terminal</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>policy-map</strong> &lt;br&gt;<strong>policy-map-name</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config)#policy-map avc-policy</td>
<td>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. <strong>Note</strong> To delete an existing policy map, use the <code>no policy-map policy-map-name</code> global configuration command.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>class</strong> [ <strong>class-map-name</strong></td>
<td><strong>class-default</strong> ]&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-pmap)# class-map avc-class</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>set dscp</strong> &lt;br&gt;<strong>new-dscp</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-pmap-c)# set dscp 45</td>
<td>Classifies IP traffic by setting a new value in the packet. For <code>dscp new-dscp</code>, enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>class</strong> &lt;br&gt;<strong>class-default</strong></td>
<td>Specifies the default class so that you can configure or modify its policy.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Step 6 set dscp default</td>
<td>Configures the default DSCP.</td>
<td></td>
</tr>
<tr>
<td>Step 7 end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 flow exporter name</td>
<td>Creates a flow exporter and enters flow exporter configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# flow exporter avc-reanchor</td>
<td>Note You can use this command to modify an existing flow exporter too.</td>
</tr>
<tr>
<td>Step 3 destination local wlc</td>
<td>Sets the exporter as local.</td>
</tr>
<tr>
<td>Example: Device(config-flow-exporter)# destination local wlc</td>
<td></td>
</tr>
</tbody>
</table>
Configuring the Flow Monitor

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> flow monitor monitor-name</td>
<td>Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# flow monitor fm_avc</td>
<td><strong>Note</strong> You can use this command to modify an existing flow monitor too.</td>
</tr>
<tr>
<td><strong>Step 3</strong> exporter exporter-name</td>
<td>Specifies the name of an exporter.</td>
</tr>
<tr>
<td>Example: Device(config-flow-monitor)# exporter avc-reanchor</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> record wireless avc basic</td>
<td>Specifies the flow record to use to define the cache.</td>
</tr>
<tr>
<td>Example: Device(config-flow-monitor)# record wireless avc basic</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> cache timeout active value</td>
<td>Sets the active flow timeout, in seconds.</td>
</tr>
<tr>
<td>Example: Device(config-flow-monitor)# cache timeout active 60</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> cache timeout inactive value</td>
<td>Sets the inactive flow timeout, in seconds.</td>
</tr>
<tr>
<td>Example: Device(config-flow-monitor)# cache timeout inactive 60</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> class-map cmap-name</td>
<td>Configures the class map.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# class-map AVC-Reanchor-Class</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> match any</td>
<td>Instructs the device to match with any of the protocols that pass through it.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-cmap)# match any</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> match protocol jabber-audio</td>
<td>Specifies a match to the application name.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-cmap)# match protocol jabber-audio</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Configuring the Wireless WLAN Profile Policy

Follow the procedure given below to configure the WLAN profile policy:

**Note** Starting with Cisco IOS XE Amsterdam 17.1.1, IPv6 flow monitor is supported on Wave 2 APs. You can attach two flow monitors in a policy profile per direction (input and output) and per IP version (IPv4 and IPv6) in local (central switching) mode, when NBAR runs in the controller. However, only one flow monitor is supported per direction (input and output) and per IP version (IPv4 and IPv6) in flexconnect and fabric modes on Wave 2 APs, when NBAR runs on the corresponding AP.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| 2    | wireless profile policy policy-name | Configures the WLAN policy profile and enters wireless policy configuration mode.  
**Example:**  
Device(config)# wireless profile policy default-policy-profile |
| 3    | shutdown | Disables the policy profile.  
**Example:**  
Device(config-wireless-policy)# shutdown |
| 4    | no central switching | Disables central switching.  
**Example:**  
Device(config-wireless-policy)# no central switching |
| 5    | ipv4 flow monitor monitor-name input | Specifies the name of the IPv4 ingress flow monitor.  
**Example:**  
Device(config-wireless-policy)# ipv4 flow monitor fm_avc input |
| 6    | ipv4 flow monitor monitor-name output | Specifies the name of the IPv4 egress flow monitor.  
**Example:**  
Device(config-wireless-policy)# ipv4 flow monitor fm_avc output |
| 7    | ipv6 flow monitor monitor-name input | Specifies the name of the IPv6 ingress flow monitor.  
**Example:**  
Device(config-wireless-policy)# ipv6 flow monitor fm_v6_avc input |
| 8    | ipv6 flow monitor monitor-name output | Specifies the name of the IPv6 egress flow monitor.  
**Example:**  
Device(config-wireless-policy)# ipv6 flow monitor fm_v6_avc output |
| 9    | no shutdown | Enables the policy profile.  
**Example:**  
Device(config-wireless-policy)# no shutdown |

**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

<table>
<thead>
<tr>
<th>Counter Name</th>
<th>Thread ID</th>
<th>Counter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reanch_deassociated_clients</td>
<td>28340</td>
<td>1</td>
</tr>
<tr>
<td>Reanch_tracked_clients</td>
<td>28340</td>
<td>4</td>
</tr>
<tr>
<td>Reanch_deleted_clients</td>
<td>28340</td>
<td>3</td>
</tr>
</tbody>
</table>

Device# show platform software trace counter tag wncd chassis active R0 avc-afc debug

<table>
<thead>
<tr>
<th>Counter Name</th>
<th>Thread ID</th>
<th>Counter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reanch_co_ignored_clients</td>
<td>30063</td>
<td>1</td>
</tr>
<tr>
<td>Reanch_co_anchored_clients</td>
<td>30063</td>
<td>5</td>
</tr>
<tr>
<td>Reanch_co_deauthed_clients</td>
<td>30063</td>
<td>4</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>FSM State</th>
<th>Event</th>
<th>RC</th>
<th>Ctx</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/12/2018 16:45:30.630342</td>
<td>:ZOMBIE</td>
<td>1 :FSM_AFM_BIND</td>
<td>0 2</td>
<td></td>
</tr>
<tr>
<td>06/12/2018 16:45:28.822780</td>
<td>:READY</td>
<td>2 :FSM_AFM_UNBIND</td>
<td>0 0</td>
<td></td>
</tr>
<tr>
<td>06/12/2018 16:45:28.822672</td>
<td>:READY</td>
<td>2 :FSM_AFM_UNBIND</td>
<td>0 0</td>
<td></td>
</tr>
<tr>
<td>06/12/2018 16:45:15.172073</td>
<td>:ZOMBIE</td>
<td>1 :FSM_AFM_BIND</td>
<td>0 2</td>
<td></td>
</tr>
<tr>
<td>06/12/2018 16:45:12.738367</td>
<td>:READY</td>
<td>2 :FSM_AFM_UNBIND</td>
<td>0 0</td>
<td></td>
</tr>
<tr>
<td>06/12/2018 16:45:12.738261</td>
<td>:READY</td>
<td>2 :FSM_AFM_UNBIND</td>
<td>0 0</td>
<td></td>
</tr>
<tr>
<td>06/12/2018 16:45:01.162689</td>
<td>:ZOMBIE</td>
<td>1 :FSM_AFM_BIND</td>
<td>0 2</td>
<td></td>
</tr>
</tbody>
</table>
### Verifying AVC Reanchoring

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

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>FSM State</th>
<th>Event</th>
<th>RC</th>
<th>Ctx</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/12/2018 16:45:30.664772</td>
<td>3</td>
<td>ZOMBIE</td>
<td>1</td>
<td>FSM_AFM_BIND</td>
</tr>
<tr>
<td>06/12/2018 16:45:28.822499</td>
<td>2</td>
<td>READY</td>
<td>2</td>
<td>FSM_AFM_UNBIND</td>
</tr>
<tr>
<td>06/12/2018 16:45:15.207605</td>
<td>3</td>
<td>ZOMBIE</td>
<td>1</td>
<td>FSM_AFM_BIND</td>
</tr>
<tr>
<td>06/12/2018 16:45:12.738105</td>
<td>2</td>
<td>READY</td>
<td>2</td>
<td>FSM_AFM_UNBIND</td>
</tr>
<tr>
<td>06/12/2018 16:45:12.737997</td>
<td>2</td>
<td>READY</td>
<td>2</td>
<td>FSM_AFM_UNBIND</td>
</tr>
<tr>
<td>06/12/2018 16:45:01.164225</td>
<td>3</td>
<td>ZOMBIE</td>
<td>1</td>
<td>FSM_AFM_BIND</td>
</tr>
<tr>
<td>06/12/2018 16:44:55.757266</td>
<td>2</td>
<td>READY</td>
<td>2</td>
<td>FSM_AFM_UNBIND</td>
</tr>
<tr>
<td>06/12/2018 16:44:55.757181</td>
<td>2</td>
<td>READY</td>
<td>2</td>
<td>FSM_AFM_UNBIND</td>
</tr>
<tr>
<td>06/12/2018 16:44:04.472778</td>
<td>3</td>
<td>ZOMBIE</td>
<td>1</td>
<td>FSM_AFM_BIND</td>
</tr>
<tr>
<td>06/12/2018 16:44:02.154130</td>
<td>2</td>
<td>READY</td>
<td>2</td>
<td>FSM_AFM_UNBIND</td>
</tr>
<tr>
<td>06/12/2018 16:44:02.152630</td>
<td>2</td>
<td>READY</td>
<td>2</td>
<td>FSM_AFM_UNBIND</td>
</tr>
</tbody>
</table>

AVC key: [1,wlan_avc.fm_avc,v4-Out,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

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>FSM State</th>
<th>Event</th>
<th>RC</th>
<th>Ctx</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/12/2018 16:45:30.630764</td>
<td>3</td>
<td>ZOMBIE</td>
<td>1</td>
<td>FSM_AFM_BIND</td>
</tr>
<tr>
<td>06/12/2018 16:45:28.822621</td>
<td>2</td>
<td>READY</td>
<td>2</td>
<td>FSM_AFM_UNBIND</td>
</tr>
<tr>
<td>06/12/2018 16:45:15.172357</td>
<td>3</td>
<td>ZOMBIE</td>
<td>1</td>
<td>FSM_AFM_BIND</td>
</tr>
<tr>
<td>06/12/2018 16:45:12.738212</td>
<td>2</td>
<td>READY</td>
<td>2</td>
<td>FSM_AFM_UNBIND</td>
</tr>
<tr>
<td>06/12/2018 16:45:12.738167</td>
<td>2</td>
<td>READY</td>
<td>2</td>
<td>FSM_AFM_UNBIND</td>
</tr>
<tr>
<td>06/12/2018 16:45:10.164048</td>
<td>3</td>
<td>ZOMBIE</td>
<td>1</td>
<td>FSM_AFM_BIND</td>
</tr>
<tr>
<td>06/12/2018 16:44:55.757403</td>
<td>2</td>
<td>READY</td>
<td>2</td>
<td>FSM_AFM_UNBIND</td>
</tr>
<tr>
<td>06/12/2018 16:44:55.757361</td>
<td>2</td>
<td>READY</td>
<td>2</td>
<td>FSM_AFM_UNBIND</td>
</tr>
<tr>
<td>06/12/2018 16:44:04.472561</td>
<td>3</td>
<td>ZOMBIE</td>
<td>1</td>
<td>FSM_AFM_BIND</td>
</tr>
<tr>
<td>06/12/2018 16:44:02.186602</td>
<td>2</td>
<td>READY</td>
<td>2</td>
<td>FSM_AFM_UNBIND</td>
</tr>
<tr>
<td>06/12/2018 16:44:02.185882</td>
<td>2</td>
<td>READY</td>
<td>2</td>
<td>FSM_AFM_UNBIND</td>
</tr>
<tr>
<td>06/12/2018 16:38:20.164293</td>
<td>2</td>
<td>READY</td>
<td>3</td>
<td>FSM_AFM_SWEEP</td>
</tr>
<tr>
<td>06/12/2018 16:35:20.163799</td>
<td>1</td>
<td>INIT</td>
<td>1</td>
<td>FSM_AFM_BIND</td>
</tr>
<tr>
<td>06/12/2018 16:35:20.163773</td>
<td>1</td>
<td>INIT</td>
<td>24</td>
<td>CREATE_FSM</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>FSM State Event</th>
<th>RC</th>
<th>Ctx</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/12/2018 16:45:30.629278</td>
<td>:WLAN_READY</td>
<td>3</td>
<td>:BIND_WNCD 24</td>
</tr>
<tr>
<td>06/12/2018 16:45:30.629223</td>
<td>:WLAN_READY</td>
<td>3</td>
<td>:FSM_BIND_ACK</td>
</tr>
<tr>
<td>06/12/2018 16:45:30.629179</td>
<td>:WLAN_READY</td>
<td>3</td>
<td>:FSM_BIND_ACK</td>
</tr>
<tr>
<td>06/12/2018 16:45:30.510867</td>
<td>:PLUMB_READY</td>
<td>2</td>
<td>:BIND_IOSD</td>
</tr>
<tr>
<td>06/12/2018 16:45:30.510411</td>
<td>:PLUMB_READY</td>
<td>2</td>
<td>:FSM_WLAN_UP</td>
</tr>
<tr>
<td>06/12/2018 16:45:30.510371</td>
<td>:PLUMB_READY</td>
<td>2</td>
<td>:FSM_WLAN_FM_PLUMB</td>
</tr>
<tr>
<td>06/12/2018 16:45:28.866377</td>
<td>:PLUMB_READY</td>
<td>2</td>
<td>:UNBIND_ACK_IOSD</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>FSM State Event</th>
<th>RC</th>
<th>Ctx</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/12/2018 16:45:30.664032</td>
<td>:WLAN_READY</td>
<td>3</td>
<td>:BIND_WNCD 24</td>
</tr>
<tr>
<td>06/12/2018 16:45:30.663958</td>
<td>:WLAN_READY</td>
<td>3</td>
<td>:FSM_BIND_ACK</td>
</tr>
<tr>
<td>06/12/2018 16:45:30.663921</td>
<td>:WLAN_READY</td>
<td>3</td>
<td>:FSM_BIND_ACK</td>
</tr>
<tr>
<td>06/12/2018 16:45:30.511151</td>
<td>:PLUMB_READY</td>
<td>2</td>
<td>:BIND_IOSD</td>
</tr>
<tr>
<td>06/12/2018 16:45:30.510624</td>
<td>:PLUMB_READY</td>
<td>2</td>
<td>:FSM_WLAN_UP</td>
</tr>
<tr>
<td>06/12/2018 16:45:30.510608</td>
<td>:PLUMB_READY</td>
<td>2</td>
<td>:FSM_WLAN_FM_PLUMB</td>
</tr>
<tr>
<td>06/12/2018 16:45:28.807239</td>
<td>:READY</td>
<td>4</td>
<td>:UNBIND_WNCD</td>
</tr>
<tr>
<td>06/12/2018 16:45:28.807205</td>
<td>:READY</td>
<td>4</td>
<td>:UNBIND_IOSD</td>
</tr>
<tr>
<td>06/12/2018 16:45:28.806734</td>
<td>:READY</td>
<td>4</td>
<td>:FSM_WLAN_DOWN</td>
</tr>
</tbody>
</table>

AVC key: [1,wlan_avc,fm_avc,v4-Out,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

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>FSM State Event</th>
<th>RC</th>
<th>Ctx</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/12/2018 16:45:30.629414</td>
<td>:WLAN_READY</td>
<td>3</td>
<td>:BIND_WNCD 24</td>
</tr>
<tr>
<td>06/12/2018 16:45:30.629392</td>
<td>:WLAN_READY</td>
<td>3</td>
<td>:FSM_BIND_ACK</td>
</tr>
<tr>
<td>06/12/2018 16:45:30.629380</td>
<td>:WLAN_READY</td>
<td>3</td>
<td>:FSM_BIND_ACK</td>
</tr>
<tr>
<td>06/12/2018 16:45:30.629179</td>
<td>:WLAN_READY</td>
<td>3</td>
<td>:FSM_BIND_ACK</td>
</tr>
</tbody>
</table>
Verifying AVC Reanchoring

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 23:UNBIND_IOSD 0 0
06/12/2018 16:45:28.807795 4 :READY 25:UNBIND_WNCD 0 0
06/12/2018 16:45:28.806990 4 :READY 3 :FSM_WLAN_DOWN 0 0
Cisco Hyperlocation

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:

- **WiSM or WiSM2 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.

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

<table>
<thead>
<tr>
<th>Attribute</th>
<th>BLE Configuration Per AP Profile</th>
<th>BLE Configuration Per AP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributes with per-AP granularity (global for all the beacons)</td>
<td>• Interval&lt;br&gt;• Advertised transmission power</td>
<td>• Interval&lt;br&gt;• Advertised transmission power</td>
</tr>
<tr>
<td>Attributes with per-AP per-beacon granularity</td>
<td>• Transmission power&lt;br&gt;• UUID&lt;br&gt;• Status</td>
<td>• Transmission power&lt;br&gt;• UUID&lt;br&gt;• Status&lt;br&gt;• Major&lt;br&gt;• Minor</td>
</tr>
</tbody>
</table>

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

- 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.
Support for IPv6 in Cisco Hyperlocation or BLE Configuration

Until Release 16.12, IPv4 was the only valid configuration. From Release 17.1 onwards, IPv6 is also supported for specific deployments.

CMX accepts only one IP configuration at a time (either IPv4 or IPv6).

The configuration combinations listed in the following tables are the valid deployments.

Table 9: Flex Deployment Mode

<table>
<thead>
<tr>
<th>Controller Management Interface and AP</th>
<th>CMX</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>IPv4</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv6</td>
</tr>
</tbody>
</table>

Table 10: Fabric Deployment Mode

<table>
<thead>
<tr>
<th>Controller Management Interface and AP</th>
<th>CMX</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>IPv4</td>
</tr>
</tbody>
</table>

Any other combination of IPv4 or IPv6 is not supported.

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.
### Configuring Cisco Hyperlocation (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | `configure terminal` | Enters global configuration mode.  
    Example:  
    `Device# configure terminal` |
| 2    | `ap profile profile-name` | Enables configuration for all APs that are associated with the specified AP profile name.  
    Example:  
    `Device(config)# ap profile profile-name` |
| 3    | `[no] hyperlocation` | Enables Hyperlocation on all the supported APs that are associated with this AP profile.  
    Use the `no` form of the command to disable the Hyperlocation feature.  
    Example:  
    `Device(config-ap-profile)# [no] hyperlocation` |
| 4    | `[no] hyperlocation threshold detection value-in-dBm` | 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.  
    Example:  
    `Device(config-ap-profile)# [no] hyperlocation threshold detection -100` |
| 5    | `[no] hyperlocation threshold reset value-btwn-0-99` | Resets the value of scan cycles after a trigger. The `no` form of this command resets the threshold to its default value.  
    Example:  
    `Device(config-ap-profile)# [no] hyperlocation threshold reset 8` |
| 6    | `[no] hyperlocation threshold trigger value-btwn-1-100` | 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.  
    Example:  
    `Device(config-ap-profile)# [no] hyperlocation threshold trigger 10` |
| 7    | `[no] ntp ip ipv4-address-of-ntp-server` | Sets the IPv4 address of the NTP server, directly reachable by the access points. The `no` form of this command removes the NTP server.  
    Example:  
    `Device(config-ap-profile)# [no] ntp ip 9.0.0.4` |
Verifying Cisco Hyperlocation

To display values for Hyperlocation status 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 overall and per-AP config values and operational status. The values displayed for Hyperlocation status and parameters reflect the values for all the AP profiles, 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: 0.0.0.0
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -90
Hyper location trigger threshold: 8
Hyperlocation reset threshold: 7

```
+--------------------------------+----------------+------------+----------+-----------------------------+----------------+----------+
| AP Name                        | Radio MAC      | Method     | CMX IP   | AP Profile                  |
|--------------------------------|----------------|------------|----------|-----------------------------|----------------|----------|
| APe865.49d9.bfe0               | e865.49ea.a4b0 | WSM2+Ant   | 10.0.0.1 | house24                     |
| APA89d.21b9.69d0               | a89d.21b9.69d0 | Local      | 10.0.0.1 | house24                     |
| APe4aa.5d3f.d750               | e4aa.5d5f.3630 | WSM        | 10.0.0.1 | house24                     |
+--------------------------------+----------------+------------+----------+-----------------------------+----------------+----------+
```

To display the overall (profile specific) configuration values and operational status for the 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 overall (profile specific) and per-AP configuration values and operational status for the 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

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Radio MAC</th>
<th>Method</th>
<th>CMX IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP07f.0635.2d40</td>
<td>f07f.0635.2d40</td>
<td>WSM2+Ant</td>
<td>1.2.3.4</td>
</tr>
<tr>
<td>AP07f.0635.2d41</td>
<td>f07f.0635.2d41</td>
<td>Local</td>
<td>1.2.3.4</td>
</tr>
<tr>
<td>AP07f.0635.2d42</td>
<td>f07f.0635.2d42</td>
<td>WSM</td>
<td>1.2.3.4</td>
</tr>
</tbody>
</table>

To display configuration values for the AP profile. There is a section for Hyperlocation configuration where values of Hyperlocation threshold parameters such as PAK RSSI are shown. 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 CMXs that are correctly joined and used by Hyperlocation, use the following command:

Device# show ap hyperlocation cmx summary

Hyperlocation-enabled CMXs

<table>
<thead>
<tr>
<th>IP</th>
<th>Port</th>
<th>Dest MAC</th>
<th>Egress src MAC</th>
<th>Egress VLAN</th>
<th>Ingress src MAC</th>
<th>Join time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.4</td>
<td>2003</td>
<td>aaaa.bbbb.cccc</td>
<td>aabb.ccdd.eeff</td>
<td>2</td>
<td>0000.0001.0001</td>
<td>12/14/18 09:27:14</td>
</tr>
</tbody>
</table>

To display the Cisco 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  0XFO000001  0000.0001.0001  9  HL  0  RN  LC  N  NULL

To display the interface handle value to start 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

<table>
<thead>
<tr>
<th>Pkts</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>3628</td>
</tr>
</tbody>
</table>

To stop the 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 APs requested by CMX with AP groups support, use the following commands:

Device# show nmsp subscription group summary

CMX IP address: 10.0.0.1
  Groups subscribed by this CMX server:
    Group name: CMX_10.0.0.1

Device# show nmsp subscription group detail ap-list CMX_10.0.0.1 10.0.0.1

CMX IP address: 10.0.0.1
CMX Group name: CMX_10.0.0.1
CMX Group AP MACs:
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 (CLI)

Before you begin

For Hyperlocation BLE to be enabled, CMX must be fully joined and enabled for Hyperlocation.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ap profile <em>profile-name</em></td>
<td>Enables configuration for all the APs that are associated with the specified AP profile name.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device(config)# ap profile <em>profile-name</em></td>
</tr>
<tr>
<td>2</td>
<td>hyperlocation ble-beacon <em>beacon-id</em></td>
<td>Specifies the BLE beacon parameters and enters BLE configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device(config-ap-profile)# hyperlocation ble-beacon <em>beacon-id</em></td>
</tr>
<tr>
<td>3</td>
<td>enabled</td>
<td>Enables BLE for the beacon ID specified.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device(config-halo-ble)# enabled</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>4</td>
<td>exit</td>
<td>Returns to AP profile configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-halo-ble)# exit</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><strong>hyperlocation ble-beacon interval</strong> value-in-hertz</td>
<td>Configures the BLE beacon interval as 1 Hz for the selected profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-profile)# hyperlocation ble-beacon interval 1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><strong>hyperlocation ble-beacon advpwr</strong> value-in-dBm</td>
<td>Configures the BLE beacon-advertised attenuation level. Valid range is between –40 dBm and –100 dBm. The default value is –59 dBm.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-profile)# hyperlocation ble-beacon advpwr 40</td>
<td></td>
</tr>
</tbody>
</table>

### 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
```

**Example:**

```
B 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-bbbbbbbbbbb 0 Enabled
2 ffffffff-gggg-gggg-gggg-gggggggggggg 0 Enabled
3 ffffffff-dddd-dddd-dddd-ddddddd44 0 Enabled
4 ffffffff-eeee-eeee-eeee-eeeeeeeee 0 Enabled
```

### Configuring Hyperlocation BLE Beacon Parameters for AP (CLI)

Follow the procedure given below to configure hyperlocation BLE beacon parameters for an AP:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>ap name ap-name hyperlocation ble-beacon</strong> <strong>beacon-id</strong> enable</td>
<td>Configures Hyperlocation and related parameters for an AP, and the specified beacon ID:</td>
</tr>
<tr>
<td></td>
<td><strong>major major-value</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>minor minor-value</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>txpwr value-in-dBm</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>uuid uuid-value</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# ap name test-ap hyperlocation ble-beacon 3 major 65535</td>
<td></td>
</tr>
</tbody>
</table>

- **enable**—Enables BLE beacon on the AP.
- **major major-value**—Configures BLE beacon’s major parameter. Valid value is
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>between 0 and 65535; the default value is 0.</td>
</tr>
<tr>
<td>• <strong>minor</strong> minor-value</td>
<td>Configures BLE beacon's minor parameter. Valid value is between 0 and 65535; the default value is 0.</td>
</tr>
<tr>
<td>• <strong>txpwr</strong> value-in-dBm</td>
<td>Configures BLE beacon attenuation level. Valid value is between –52 dBm and 0 dBm.</td>
</tr>
<tr>
<td>• <strong>uuid</strong> uuid-value</td>
<td>Configures a UUID.</td>
</tr>
</tbody>
</table>

### Step 2

<table>
<thead>
<tr>
<th>Step 2</th>
<th>ap name ap-name hyperlocation ble-beacon advpwr value-in-dBm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device# ap name test-ap hyperlocation ble-beacon advpwr 90</td>
</tr>
</tbody>
</table>

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).

---

### 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
```

<table>
<thead>
<tr>
<th>ID</th>
<th>Status</th>
<th>UUID</th>
<th>Major</th>
<th>Minor</th>
<th>TXPower(dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Enabled</td>
<td>99999999-9999-9999-9999-999999999999</td>
<td>8</td>
<td>0</td>
<td>-0</td>
</tr>
<tr>
<td>1</td>
<td>Enabled</td>
<td>bbbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbb</td>
<td>8</td>
<td>1</td>
<td>-0</td>
</tr>
<tr>
<td>2</td>
<td>Enabled</td>
<td>88888888-8888-8888-8888-888888888888</td>
<td>8</td>
<td>2</td>
<td>-0</td>
</tr>
<tr>
<td>3</td>
<td>Enabled</td>
<td>ddddddddd-dddd-dddd-dddd-dddddddddddd</td>
<td>8</td>
<td>3</td>
<td>-0</td>
</tr>
<tr>
<td>4</td>
<td>Enabled</td>
<td>eeeeeeee-eeee-eeee-eeee-eeee-eeee</td>
<td>8</td>
<td>4</td>
<td>-0</td>
</tr>
</tbody>
</table>
Verifying Hyperlocation BLE Beacon Configuration for AP
CHAPTER 46

FastLocate for Cisco Catalyst Series Access Points

- Information About FastLocate, on page 379
- Supported Access Points, on page 379
- FastLocate Network Components, on page 380
- Configuring FastLocate (GUI), on page 380
- Verifying FastLocate on Cisco Catalyst APs, on page 381

Information About FastLocate

Current Wi-Fi location technology relies on mobile devices sending received signal strength indication (RSSI) or location information, based on probe request messaging, to access points. This information is sent on most channels by the mobile device and received by neighbor APs on different channels. This helps in location estimation.

Wi-Fi clients are moving towards lesser probing to discover an AP. This helps to conserve battery power. Depending on the client, operating system, driver, battery, current, and client activity, device probing frequency varies anywhere from 10 seconds to 5 minutes. This variation results in inadequate data points to represent real-world movement.

Since data packets are more frequent than probe request packets, they can be aggregated better. FastLocate enables higher location refresh rates by collecting RSSI or location information through data packets received by the APs. Using these data packets, location-based services (LBS) updates are initiated by the network and are available more frequently.

Supported Access Points

Beginning with IOS XE 17.1.1, FastLocate is supported on the Cisco Catalyst 9120 Series APs.

When FastLocate is enabled, the RHL radios of these APs act as a WSSI module and transform into a monitoring role and off-channel scanning mode. The RHL radios scan through all the 2.4-GHz channels and 5-GHz channels in a linear fashion, with each channel scanned for 150 milliseconds. This period is called the dwell time.
The RHL radios of the APs are synchronized with the NTP server. Using FastPath, all data packet RSSI records that are collected during one off-channel dwell is sent in a specific packet format to the Cisco controller, at the end of the dwell time.

FastLocate Network Components

For successful packet RSSI location computation, the following components with necessary functionalities are needed:

- Wireless client
  - Send data, management, and control packets
- Cisco Catalyst 9800 Series Wireless Controller
  - Configure NTP server information and location parameters on AP
  - Forward clients' RSSI related information to CMX/MSE via FastPath/datapath
- Cisco Catalyst 9120 Series AP
  - Location radio in monitor or equivalent role
  - Time synchronized with NTP server
  - Collect RSSI related data sent by clients (both associated and unassociated)
  - Send clients' RSSI data to the Cisco controller through CAPWAP
- Cisco CMX
  - Parse fastpath location data received by WLC
  - Calculate exact physical location of the client and render on GUI using algorithms

Configuring FastLocate (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Step Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configuration &gt; Tags &amp; Profiles &gt; AP Join.</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td>On the <strong>AP Join</strong> page, click the <strong>default-ap-profile</strong> AP join profile.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Edit AP Join Profile</strong> window, click the <strong>AP</strong> tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Under <strong>Hyperlocation</strong>, select the <strong>Enable Hyperlocation</strong> check box.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Update &amp; Apply to Device.</strong></td>
</tr>
</tbody>
</table>
Verifying FastLocate on Cisco Catalyst APs

To verify FastLocate, use the below commands on the AP:

```
Device# show ntp
Stratum  Version  Last Received  Delay  Offset  Jitter  NTP server
1        4         123sec ago  1.169ms -3.262ms 10.050ms 7.7.7.2

Device# show ap fast-path statistics
total packets sent : 90001
invalid app ID drops : 0
application : 0 (HALO)
packets sent (CAPWAP) : 90001
packets sent (APP HOST INTF) : 0
admin state drops : 0
no dest IP drops : 0
```

To view FastLocate admin status details on the AP, use the following command:

```
Device# show capwap client rcb
Hyperlocation Admin State : Enabled
MSE Gateway MAC : 00:50:56:86:0F:9D
WLC Hyperlocation Source Port: 9999
MSE IP Address : 10.0.0.1
```

To view FastPath-related parameters on the AP like source and destination IP addresses, port numbers, and the gateway MAC address, use the following command:

```
Device# show ap fastpath configuration hyperlocation
source IP address : 10.0.0.2
destination IP address: 10.0.0.1
source port (WLC) : 9999
destination port (MSE): 2003
gateway MAC : 00:50:56:86:0F:9D
ewlc hyperlocation MAC: 00:00:00:01:00:01
```

To verify FastLocate on the Cisco Catalyst controller, use the appropriate command given below.

```
To view the summary of applications that send fastpath or datapath data, use the below command. The hexcode for the HyperLocation and BLE port numbers are displayed.

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   DPIIDX  MAC Address VLAN CT MCVL AS MS E WLAN POA
-----------------------------------------------------------------------
0X31 0XF0000002 0000.0003.0001 122 BL 0 RN LC N NULL 0X32 0XF0000001 0000.0001.0001 122
HL 0 RN LC N NULL
```

To capture statistics of a selected application, use the below command:
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
cpp-if-handle register-code statistics start

The hex-value of the register-code is obtained from the `show platform hardware chassis active qfp feature wireless wlclient cpp-client summary` command mentioned earlier.

Device# show platform hardware chassis active qfp feature wireless wlclient datapath cpp-if-handle 0x32 statistics start

To display the statistics of the selected application, use the below command:

Device# show platform hardware chassis active qfp feature wireless wlclient datapath cpp-if-handle register-code statistics

The hex-value of the register-code is obtained from the `show platform hardware chassis active qfp feature wireless wlclient cpp-client summary` command mentioned earlier.

Device# show platform hardware chassis active qfp feature wireless wlclient datapath cpp-if-handle 0x32 statistics

<table>
<thead>
<tr>
<th>Pkts</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx</td>
<td>232</td>
</tr>
</tbody>
</table>
CHAPTER 47

BLE Beacons in CiscoWave 2 Access Points

- Managing BLE Beacons in Cisco Wave 2 and 802.11ax Access Points, on page 383
- Monitoring BLE Management, on page 385

Managing BLE Beacons in Cisco Wave 2 and 802.11ax Access Points

Some Cisco Wave 2 (Aironet series) and 802.11ax (Catalyst series) access points (APs) are Bluetooth Low-Energy (BLE) enabled. The BLE Management feature enables standardized management for third-party beacon vendors to interoperate with these Cisco APs over BLE. The BLE Management feature supports both sending of beacons and listening to beacons from small battery-powered devices to allow better control and management.

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 11: Feature Support in AP Models**

<table>
<thead>
<tr>
<th>AP Platform</th>
<th>SKU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Catalyst 9115AX Access Point</td>
<td>I</td>
</tr>
<tr>
<td>Cisco Catalyst 9117AX Access Point</td>
<td>I</td>
</tr>
<tr>
<td>Cisco Catalyst 9120AX Access Point</td>
<td>I, E, P</td>
</tr>
<tr>
<td>Cisco Aironet 1542 Access Point</td>
<td>I</td>
</tr>
<tr>
<td>Cisco Aironet 1810 Access Point</td>
<td>W, T</td>
</tr>
<tr>
<td>Cisco Aironet 1815 Access Point</td>
<td>W, T</td>
</tr>
<tr>
<td>Cisco Aironet 1800 Access Point</td>
<td>I</td>
</tr>
<tr>
<td>Cisco Aironet 4800 Access Point</td>
<td>-</td>
</tr>
</tbody>
</table>

**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 beaoning 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:
  - 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

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 BLE management feature for a specific CMX along with all the APs associated to the corresponding IPv6 IP address, use the following command:

Device# show ap ble cmx detail ip 2001:0db8:0000:85a3:0000:0000:ac1f:8001
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

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Interface</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP4001.7AB2.C39B</td>
<td>Integrated</td>
<td>Open</td>
</tr>
</tbody>
</table>
Cisco DNA Spaces

Cisco DNA Spaces is the next generation indoor location services platform. The Network Mobility Services Protocol (NMSP) cloud-service of the wireless controller communicates with Cisco DNA Spaces using HTTPS as a transport protocol.

- Configuring Cisco DNA Spaces, on page 389
- Verifying Cisco DNA Spaces Configuration, on page 390

Configuring Cisco DNA Spaces

Follow the procedure given below to configure Cisco DNA Spaces:

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 DNA Spaces is required to enable `server url` and `server token` parameters configuration which is needed to complete this setup.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Example:</strong> <code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>ip name-server namesvr-ip-addr</code></td>
<td>Configures the DNS on the controller to resolve the FQDN names used by the NMSP cloud-services.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Example:</strong> <code>Device(config)#ip name-server 10.10.10.205</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>crypto pki trustpool import url url</td>
<td>Imports the 3rd party root CA. The controller verifies the peer using the imported certificate.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# crypto pki trustpool import url <a href="http://www.cisco.com/security/pki/trs/ios.p7b">http://www.cisco.com/security/pki/trs/ios.p7b</a></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[no] nmsp cloud-services server url url</td>
<td>Configures the URL used for cloud services. Use the no form of the command to delete the server url from the configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# nmsp cloud-services server url <a href="https://cisco.com">https://cisco.com</a></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[no] nmsp cloud-services server token token</td>
<td>Configures the authentication token for the NMSP cloud service. Use the no form of the command to delete the server token from the configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# nmsp cloud-services server token test</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[no] nmsp cloud-services http-proxy proxy-server port</td>
<td>(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.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# nmsp cloud-services http-proxy 10.0.0.1 10</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[no] nmsp cloud-services enable</td>
<td>Enables NMSP cloud services. Use the no form of the command to disable the feature.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# nmsp cloud-services enable</td>
<td></td>
</tr>
</tbody>
</table>

## Verifying Cisco DNA Spaces Configuration

Use the following commands to verify the Cisco DNA Spaces configuration.

To view the status of active NMSP connections, use the following command:

```
Device# show nmsp status
```

<table>
<thead>
<tr>
<th>MSE IP Address</th>
<th>Tx Echo Resp</th>
<th>Rx Echo Resp</th>
<th>Tx Data</th>
<th>Rx Data</th>
<th>Transport</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9.71.78</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>TLS</td>
</tr>
<tr>
<td>64.103.36.133</td>
<td>0</td>
<td>0</td>
<td>1230</td>
<td>2391</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

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 nmirstatus 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 nmirstatus 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
Verifying Cisco DNA Spaces Configuration
EDCA Parameters

- Enhanced Distributed Channel Access Parameters, on page 393
- Configuring EDCA Parameters (GUI), on page 393
- Configuring EDCA Parameters (CLI), on page 394

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.
### Configuring EDCA Parameters (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;<strong>Example:</strong> Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>**ap dot11 {5ghz</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**ap dot11 {5ghz</td>
</tr>
<tr>
<td></td>
<td><strong>• custom-voice</strong>—Enables custom voice parameters for the 802.11a or 802.11b/g network.</td>
</tr>
<tr>
<td></td>
<td><strong>• fastlane</strong>—Enables the fastlane parameters for the 802.11a or 802.11b/g network.</td>
</tr>
<tr>
<td></td>
<td><strong>• optimized-video-voice</strong>—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.</td>
</tr>
<tr>
<td></td>
<td><strong>• optimized-voice</strong>—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.</td>
</tr>
<tr>
<td></td>
<td><strong>• svp-voice</strong>—Enables SpectraLink voice-priority parameters for the 802.11a or 802.11b/g network. Choose this option if SpectraLink phones are deployed on</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no ap dot11 {5ghz</td>
<td>24ghz} shutdown Example: Device(config)# no ap dot11 5ghz shutdown</td>
</tr>
<tr>
<td><strong>Step 5</strong> end Example: Device(config)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> show ap dot11 {5ghz</td>
<td>24ghz} network Example: Device# show ap dot11 5ghz network</td>
</tr>
</tbody>
</table>
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 can be used only with Cisco Aironet 1140, 1250, 1260, 1550, 1800, 2600, 2800, 3500, 3600, 3800 Series access points.

- Mid-RSSI is not supported on Cisco Aironet 1600 Series access points.

- Band selection is not supported in Cisco Aironet 1040, OEAP 600 Series access points.

- Band selection operates only on access points that are connected to a controller. A FlexConnect access point without a controller connection does not perform band selection after a reboot.

- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.

- You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.

- It is not possible to enable or disable band selection and client load balancing globally through the controller GUI or CLI. You can, however, enable or disable band selection and client load balancing for a particular WLAN. Band selection and client load balancing are enabled globally by default.
Information About Configuring Band Selection, 802.11 Bands, and Parameters

Band Selection

Band selection enables client radios that are capable of dual-band (2.4 and 5-GHz) 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 selection works by regulating probe responses to clients and it can be enabled on a per-WLAN basis. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels. In an access point, the band select table can be viewed by running the `show dot11 band-select` command. It can also be viewed by running the `show cont d0/d1 | begin Lru` command.

Note

The WMM default configuration is not shown in the `show running-config` command output.

Band Selection Algorithm

The band selection algorithm affects clients that use 2.4-GHz band. Initially, when a client sends a probe request to an access point, the corresponding client probe’s Active and Count values (as seen from the band select table) become 1. The algorithm functions based on the following scenarios:

- **Scenario 1** — Client RSSI (as seen from `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.

- **Scenario 2** — 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.
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.

When a controller is configured to allow only 802.11g traffic, 802.11b client devices are able to successfully connect to an access point, but cannot pass traffic. When you configure the controller only for 802.11g traffic, you must mark 11g rates as mandatory.

The Block Acks in a Cisco 2800, 3800, 1560 APs are sent at configured mandatory data rates in controller for 2.4 GHz radio.

This section contains the following subsections:

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.

Some Cisco 802.11n APs may intermittently emit incorrect beacon frames, which can trigger false wIPS alarms. We recommend that you ignore these alarms. The issue is observed in the following Cisco 802.11n APs: 2600, 3500, and 3600.

802.11h Parameters

802.11h informs client devices about channel changes and can limit the transmit power of those client devices.
How to Configure 802.11 Bands and Parameters

Configuring Band Selection (GUI)

Before you begin

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Wireless Advanced &gt; Band Select.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Client RSSI (dbm) field, enter a value between -90 to -20. This is the average of the client packets received.</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>In the Client Mid RSSI (dbm) field, enter a value between -90 to -20. This the instantaneous RSSI value of the probe packets.</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>On the AP Join Profile page, click the AP Join Profile name.</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td>Click Apply.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Band Selection (CLI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless client band-select cycle-count cycle_count</td>
<td>Sets the probe cycle count for band select. Valid range is between 1 and 10.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wireless client band-select cycle-count 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> wireless client band-select cycle-threshold milliseconds</td>
<td>Sets the time threshold for a new scanning cycle period. Valid range is between 1 and 1000.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wireless client band-select cycle-threshold 5000</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> wireless client band-select expire suppression seconds</td>
<td>Sets the suppression expire to the band select. Valid range is between 10 and 200.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wireless client band-select expire suppression 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> wireless client band-select expire dual-band seconds</td>
<td>Sets the dual band expire. Valid range is between 10 and 300.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wireless client band-select expire dual-band 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> wireless client band-select client-rssi client_rssi</td>
<td>Sets the client RSSI threshold. Valid range is between 20 and 90.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wireless client band-select client-rssi 40</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# end</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> wlan wlan_profile_name wlan_ID SSID_network_name band-select</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wlan wlan1 25 ssid12 Device(config-wlan)# band-select</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the 802.11 Bands (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configuration &gt; Radio Configurations &gt; Network.</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td>Click either <strong>5 GHz Band</strong> or <strong>2.4 GHz Band.</strong></td>
</tr>
<tr>
<td>Step 3</td>
<td>Uncheck the <strong>Network Status</strong> check box to disable the network in order to be able to configure the network parameters.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the <strong>Beacon Interval</strong> field, enter the rate at which the SSID is broadcast by the APs, from 100 to 600 milliseconds. The default is 100 milliseconds.</td>
</tr>
<tr>
<td>Step 5</td>
<td>For 802.11b/g/n (2.4-GHz) radios, to enable short preamble on the radio, check the <strong>Short Preamble</strong> check box. A short preamble improves throughput performance.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the <strong>Fragmentation Threshold (in bytes)</strong> field, enter a value between 256 to 2346 bytes. Packets larger than the size you specify here will be fragmented.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Check the <strong>DTPC Support</strong> 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 <strong>DTPC Support</strong> check box is checked.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Click <strong>Apply.</strong></td>
</tr>
<tr>
<td>Step 9</td>
<td>In the <strong>CCX Location Measurement</strong> section, check the <strong>Mode</strong> 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.</td>
</tr>
<tr>
<td>Step 10</td>
<td>In the <strong>Interval</strong> field, enter a value to specify how often the APs must issue broadcast radio measurement requests.</td>
</tr>
<tr>
<td>Step 11</td>
<td>Click <strong>Apply.</strong></td>
</tr>
<tr>
<td>Step 12</td>
<td>In the <strong>Data Rates</strong> section, choose a value to specify the rates at which data can be transmitted between the access point and the client:</td>
</tr>
<tr>
<td></td>
<td>• Mandatory: Clients must support this data rate in order to associate to an access point on the controller embedded wireless controller.</td>
</tr>
<tr>
<td></td>
<td>• Supported: Any associated clients that support this data rate may communicate with the access point using that rate.</td>
</tr>
<tr>
<td></td>
<td>• Disabled: The clients specify the data rates used for communication.</td>
</tr>
<tr>
<td>Step 13</td>
<td>Click <strong>Apply.</strong></td>
</tr>
<tr>
<td>Step 14</td>
<td>Save the configuration.</td>
</tr>
</tbody>
</table>

### Configuring the 802.11 Bands (CLI)

Follow the procedure given below to configure 802.11 bands and parameters:
## Configuring the 802.11 Bands (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ap dot11 5ghz shutdown</td>
<td>Disables the 802.11a band.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap dot11 5ghz shutdown</td>
<td><strong>Note</strong> You must disable the 802.11a band before configuring the 802.11a network parameters.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ap dot11 24ghz shutdown</td>
<td>Disables the 802.11b band.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap dot11 24ghz shutdown</td>
<td><strong>Note</strong> You must disable the 802.11b band before configuring the 802.11b network parameters.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ap dot11 {5ghz</td>
<td>24ghz} beaconperiod time_unit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap dot11 5ghz beaconperiod 500</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ap dot11 {5ghz</td>
<td>24ghz} fragmentation threshold</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap dot11 5ghz fragmentation 300</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>ap dot11 {5ghz</td>
<td>24ghz} dtpc</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap dot11 5ghz dtpc; Device(config)# no ap dot11 24ghz dtpc</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>wireless client association limit number interval milliseconds</td>
<td>Specifies the maximum allowed clients that can be configured.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong>                                                                 ****</td>
<td><strong>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 1000 milliseconds.</strong>&lt;br&gt;<strong>Device(config)# wireless client association limit 50 interval 1000</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>**ap dot11 {5ghz</td>
<td>24ghz} rate rate {disable</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>no ap dot11 5ghz shutdown</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<strong>Device(config)# no ap dot11 5ghz shutdown</strong></td>
<td>Enables the 802.11a band. <strong>Note</strong> The default value is enabled.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>no ap dot11 24ghz shutdown</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<strong>Device(config)# no ap dot11 24ghz shutdown</strong></td>
<td>Enables the 802.11b band. <strong>Note</strong> The default value is enabled.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>ap dot11 24ghz dot11g</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<strong>Device(config)# ap dot11 24ghz dot11g</strong></td>
<td>Enables or disables 802.11g network support. The default value is enabled. You can use this command only if the 802.11b band is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap dot11 24ghz rf-profile <em>rf-profile</em></td>
<td>Configures the RF profile name and enters RF profile configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# ap dot11 24ghz rf-profile test1</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring 802.11n Parameters (GUI)

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Tags &amp; Profiles &gt; RF.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Add to view the Add RF Profile window.</td>
<td></td>
</tr>
</tbody>
</table>
| 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

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

---

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 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. |
| 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. |
| 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. |
| 5    | `ap dot11 {5ghz | 24ghz} shutdown`  
^Example:  
Device(config)# ap dot11 5ghz shutdown | Disables the network. |
| 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  
• 1—Background  
• 2—Spare  
• 3—Excellent effort  
• 4—Controlled load  
• 5—Video, less than 100-ms latency and jitter |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| • 6—Voice, less than 100-ms latency and jitter  
• 7—Network control | You can configure each priority level independently, or you can use 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.  

**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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>ap dot11 5ghz shutdown</code></td>
<td>Disables the 802.11a network.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# <code>ap dot11 5ghz shutdown</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>`{ap</td>
<td>no ap} dot11 5ghz channelswitch mode switch_mode`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# <code>ap dot11 5ghz channelswitch mode 0</code></td>
<td><code>switch_mode</code>--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.</td>
</tr>
<tr>
<td>3</td>
<td><code>ap dot11 5ghz power-constraint value</code></td>
<td>Configures the 802.11h power constraint value in dB. The valid range is from 0 to 255. The default value is 3.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# <code>ap dot11 5ghz power-constraint 200</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>no ap dot11 5ghz shutdown</code></td>
<td>Re-enables the 802.11a network.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# <code>no ap dot11 5ghz shutdown</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>

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 12: Monitoring Configuration Settings Using Band Selection and 802.11 Band Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ap dot11 5ghz network</code></td>
<td>Displays 802.11a band network parameters, 802.11a operational rates, 802.11n MCS settings, and 802.11n status information.</td>
</tr>
</tbody>
</table>
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 Admission Control (CAC) configuration
Voice AC
Voice AC - Admission control (ACM) : Disabled
Voice Stream-Size : 84000
Voice Max-Streams : 2
Voice Max RF Bandwidth : 75
Voice Reserved Roaming Bandwidth : 6
Voice Load-Based CAC mode : Enabled
Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
SIP based CAC : Disabled
SIP Codec Type : CODEC_TYPE_G711
SIP call bandwidth : 64
SIP call bandwidth sample-size : 20
Video AC
Video AC - Admission control (ACM) : Disabled
Video max RF bandwidth : Infinite
Video reserved roaming bandwidth : 0

Example: Viewing the Configuration Settings for the 24-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
Example: Viewing the Configuration Settings for the 24-GHz Band

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
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

<table>
<thead>
<tr>
<th>Rate</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b 1M</td>
<td>Mandatory</td>
</tr>
<tr>
<td>802.11b 2M</td>
<td>Mandatory</td>
</tr>
<tr>
<td>802.11b 5.5M</td>
<td>Mandatory</td>
</tr>
<tr>
<td>802.11b 11M</td>
<td>Mandatory</td>
</tr>
<tr>
<td>802.11b 6M</td>
<td>Supported</td>
</tr>
<tr>
<td>802.11b 9M</td>
<td>Supported</td>
</tr>
<tr>
<td>802.11b 12M</td>
<td>Supported</td>
</tr>
<tr>
<td>802.11b 18M</td>
<td>Supported</td>
</tr>
<tr>
<td>802.11b 24M</td>
<td>Supported</td>
</tr>
<tr>
<td>802.11b 36M</td>
<td>Supported</td>
</tr>
<tr>
<td>802.11b 48M</td>
<td>Supported</td>
</tr>
<tr>
<td>802.11b 54M</td>
<td>Supported</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>MCS</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Enabled</td>
</tr>
<tr>
<td>1</td>
<td>Enabled</td>
</tr>
<tr>
<td>2</td>
<td>Enabled</td>
</tr>
<tr>
<td>3</td>
<td>Enabled</td>
</tr>
<tr>
<td>4</td>
<td>Enabled</td>
</tr>
<tr>
<td>5</td>
<td>Enabled</td>
</tr>
<tr>
<td>6</td>
<td>Enabled</td>
</tr>
<tr>
<td>7</td>
<td>Enabled</td>
</tr>
<tr>
<td>8</td>
<td>Enabled</td>
</tr>
<tr>
<td>9</td>
<td>Enabled</td>
</tr>
<tr>
<td>10</td>
<td>Enabled</td>
</tr>
<tr>
<td>11</td>
<td>Enabled</td>
</tr>
<tr>
<td>12</td>
<td>Enabled</td>
</tr>
<tr>
<td>13</td>
<td>Enabled</td>
</tr>
<tr>
<td>14</td>
<td>Enabled</td>
</tr>
<tr>
<td>15</td>
<td>Enabled</td>
</tr>
<tr>
<td>16</td>
<td>Enabled</td>
</tr>
<tr>
<td>17</td>
<td>Enabled</td>
</tr>
<tr>
<td>18</td>
<td>Enabled</td>
</tr>
<tr>
<td>19</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
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\nDevice(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\nDevice(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\nDevice(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 51

Predownloading an Image to an Access Point

- Information About Predownloading an Image to an Access Point, on page 419
- Restrictions for Predownloading an Image to an Access Point, on page 419
- How to Predownload an Image to an Access Point, on page 420
- Monitoring the Access Point Predownload Process, on page 421

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 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.
How to Predownload an Image to an Access Point

Predownloading an Image to Access Points (CLI)

Before you begin

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

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

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>ap image predownload</code> or <code>ap name ap-name image predownload</code></td>
<td>Downloads the new image to all the access points or a specific access point connected to the device.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# <code>ap image predownload</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# <code>ap name ap1 image predownload</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>show ap image</code></td>
<td>Verifies the access point's predownload status.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>This command initially displays the status as Predownloading and then moves to Completed, when download is complete.</td>
</tr>
<tr>
<td></td>
<td>Device# <code>show ap image</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>show ap name ap-name image</code></td>
<td>Provides image details of a particular AP.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# <code>show ap name ap1 image</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>ap image swap</code> or <code>ap name ap-name image swap</code></td>
<td>Swaps the images of the APs that have completed predownload.</td>
</tr>
<tr>
<td></td>
<td>or <code>ap image swap completed</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# <code>ap image swap</code></td>
<td></td>
</tr>
</tbody>
</table>
### 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 | Predownload Ver... | Primary Image | Backup Image | Predownload Status
--------|--------------------|--------------|--------------|---------------------
AP1     | 10.0.1.67          | 10.0.1.66    | 10.0.1.66    | Predownloading

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 | Predownload Ver... | Primary Image | Backup Image | Predownload Status
--------|--------------------|--------------|--------------|---------------------
AP1     | 10.0.1.67          | 10.0.1.67    | 10.0.1.67    | Complete

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
```

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>ap image reset</code></td>
<td>Resets the access points.</td>
</tr>
<tr>
<td>or <code>ap name ap-name reset</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>ap image reset</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>reload</code></td>
<td>Resets the system.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>reload</code></td>
<td></td>
</tr>
</tbody>
</table>
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
Efficient Image Upgrade

Efficient Image upgrade is an efficient way of predownloading the image to the APs. It works similar to Master - Slave model. An AP per model becomes the Master AP and downloads image from the controller through the WAN link. Once the Master AP has the downloaded image, the Slave APs starts downloading the image from the Master AP. In this way, WAN latency is reduced. Master AP selection is dynamic and random. A maximum of three Slave APs per AP model can download the image from the Master APs.

Note
- Efficient image upgrade works only on flex mode.
- Efficient image upgrade will not work with default-site-tag.

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)

Before you begin

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `configure terminal` | Enters the global configuration mode.  
**Example:**  
Device# configure terminal |
| **Step 2** | `wireless profile flex flex-profile` | Configures an RF profile and enters the rf profile configuration mode.  
**Example:**  
Device(config)# wireless profile flex rr-xyz-flex-profile |
| **Step 3** | `predownload` | Enables predownload of the image.  
**Example:**  
Device(config-wireless-flex-profile)# predownload |
| **Step 4** | `end` | Exits the configuration mode and returns to privileged EXEC mode.  
**Example:**  
Device(config-wireless-flex-profile)# end |

# Configuring a Site Tag (CLI)

Follow the procedure given below to configure a site tag:

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `configure terminal` | Enters global configuration mode.  
**Example:**  
Device# configure terminal |
| **Step 2** | `wireless tag site site-name` | Configures a site tag and enters site tag configuration mode.  
**Example:**  
Device(config)# wireless tag site rr-xyz-site |
| **Step 3** | `flex-profile flex-profile-name` | Configures a flex profile. |
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap mac-address</td>
<td>Configures a Cisco AP and enters AP profile configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# ap F866.F267.7DFB</td>
<td>Note: The <strong>mac-address</strong> should be a wired <strong>mac address</strong>.</td>
</tr>
</tbody>
</table>

#### 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 details.

---

### Trigger Predownload to a Site Tag

Follow the procedure given below to trigger image download to the APs:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enters the privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Example:**

Device> configure terminal
### Trigger Predownload to a Site Tag

<table>
<thead>
<tr>
<th>Step 2</th>
<th>ap image predownload site-tag site-tag start</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device# ap image predownload site-tag rr-xyz-site start</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Instructs the master APs to start image predownload.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>show ap master list</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show ap master list</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Displays the list of master APs per AP model per site tag.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>show ap image</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show ap image</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Displays the predownloading state of master and slave APs.</td>
</tr>
</tbody>
</table>

**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 master 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 master AP has started predownloading the image.

```
Device# show ap image
Total number of APs: 6
AP Name       Next Retry Time       Primary Image       Backup Image       Predownload Status       Predownload Version
APE00E.DA99.687A N/A            16.6.230.37       0.0.0.0             None                        0.0.0.0
AP188B.4500.4208 N/A            16.6.230.37       8.4.100.0           None                        0.0.0.0
AP188B.4500.4480 N/A            16.6.230.37       0.0.0.0             None                        0.0.0.0
AP188B.4500.5E28 N/A            16.6.230.37       16.4.230.35         None                        0.0.0.0
AP0896.AD9D.3124 0               16.6.230.37       8.4.100.0           Predownloading                16.6.230.36
AF2C33.1185.C4D0 N/A            16.6.230.37       8.4.100.0           None                        0.0.0.0
```

The following output shows that the master AP has completed predownload and the predownload has been initiated in the slave AP.

```
Device# show ap image
Total number of APs: 6
```
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
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
```

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Next Retry Time</th>
<th>Primary Image</th>
<th>Backup Image</th>
<th>Predownload Status</th>
<th>Predownload Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>APE00E.DA99.687A</td>
<td>N/A</td>
<td>16.6.230.37</td>
<td>0.0.0.0</td>
<td>Initiated</td>
<td>16.6.230.36</td>
</tr>
<tr>
<td>API88B.4500.4208</td>
<td>N/A</td>
<td>16.6.230.37</td>
<td>8.4.100.0</td>
<td>None</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>API88B.4500.4480</td>
<td>N/A</td>
<td>16.6.230.37</td>
<td>0.0.0.0</td>
<td>None</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>API88B.4500.5E28</td>
<td>N/A</td>
<td>16.6.230.37</td>
<td>16.4.230.35</td>
<td>None</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>AP0896.AD9D.3124</td>
<td>N/A</td>
<td>16.6.230.37</td>
<td>8.4.100.0</td>
<td>Complete</td>
<td>16.6.230.36</td>
</tr>
<tr>
<td>API2C33.1185.C4D0</td>
<td>0</td>
<td>16.6.230.37</td>
<td>8.4.100.0</td>
<td>Complete</td>
<td>16.6.230.36</td>
</tr>
</tbody>
</table>
Hitless Upgrade

- N+1 Hitless Rolling AP Upgrade, on page 429
- Configuring Hitless Upgrade, on page 430
- Verifying Hitless Upgrade, on page 431

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.
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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `ap image upgrade destination wlc-name wlc-ip` | 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.  
| Example: | `Device# ap image upgrade destination wlc2 10.7.8.9` |  
| 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` | (Optional) Moves APs to the specified destination controller with a swap and reset command.  
| Example: | `Device# ap image upgrade destination wlc2 10.7.8.9` |  
| Note | Perform Steps 2 to 4 only if you are not performing Step 1. |
| **Step 3** | `ap image move destination wlc-name wlc-ip` | Move the APs back to the parent controller.  
| Example: | `Device# ap image move destination wlc1 10.7.8.6` |  
| **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 the parent controller (without a swap and reset) after manual install activate of the new image and reloading of the parent controller.  
<p>| Example: | <code>Device# ap image upgrade destination wlc2 10.7.8.9 fallback</code> |<br />
| <strong>Step 5</strong> | <code>ap image upgrade destination wlc-name wlc-ip [reset]</code> | (Optional) Moves APs to the specified destination controller with a swap and reset command. After this, the parent controller |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# ap image upgrade destination wlc2 10.7.8.9 reset</td>
<td>activates the new image and reloads with the new image.</td>
</tr>
</tbody>
</table>

## 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
---------------------
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.

The sub-package is an optional binary that contains the entire Cisco Catalyst 9800 Series Wireless Controller software.
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.

**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 Switch 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**

```plaintext
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

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.

**Step 3**
Reload the switch.

---

**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 and triggers a reload. However, you can also rollback to the previous state after the reload.

**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 435.

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:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>install deactivate file flash:&lt;controller&gt;.bin</strong></td>
<td>Removes the package and forces the switch to reboot.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# install deactivate file flash:&lt;controller&gt;.bin</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>install commit</strong></td>
<td>Commits the switch without wireless package.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# install commit</td>
<td></td>
</tr>
</tbody>
</table>

### Enabling or Disabling Auto-Upgrade

Follow the procedure given below to enable or disable auto-upgrade:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>software auto-upgrade enable</strong></td>
<td>Enables software auto-upgrade.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# software auto-upgrade enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>software auto-upgrade disable</strong></td>
<td>Disables software auto-upgrade.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# software auto-upgrade disable</td>
<td></td>
</tr>
</tbody>
</table>
Enabling or Disabling Auto-Upgrade
CHAPTER 55

NBAR Protocol Discovery

- Introduction to NBAR Protocol Discovery, on page 439
- Configuring NBAR Protocol Discovery, on page 439
- Verifying Protocol Discovery Statistics, on page 440

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

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

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>wireless profile policy profile-policy</td>
<td>Configures a WLAN policy profile and enters wireless policy configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless profile policy nbar-proto-policy</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>central switching</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# central switching</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configures the wireless policy profile for central switching.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>NBAR Protocol Discovery is supported in local mode (central switching) and in FlexConnect (central switching) mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>ip nbar protocol-discovery</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# ip nbar protocol-discovery</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enables application recognition on the wireless policy profile by activating the NBAR2 engine.</td>
<td></td>
</tr>
</tbody>
</table>

### Verifying Protocol Discovery Statistics

To view protocol discovery statistics, use the following command:

```
Device# show ip nbar protocol-discovery wlan wlan-profile-name
```

Last clearing of “show ip nbar protocol-discovery” counters 00:07:12

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Input Packet Count</th>
<th>Input Byte Count</th>
<th>5min Input Bit Rate (bps)</th>
<th>Output Packet Count</th>
<th>Output Byte Count</th>
<th>5min Output Bit Rate (bps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp</td>
<td>3</td>
<td>1166</td>
<td>0</td>
<td>724</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ping</td>
<td>2</td>
<td>204</td>
<td>0</td>
<td>236</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>unknown</td>
<td>22</td>
<td>4173</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>27</td>
<td>5543</td>
<td>960</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2000</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Total</strong></td>
<td><strong>5563</strong></td>
<td><strong>960</strong></td>
<td><strong>0</strong></td>
<td><strong>0</strong></td>
<td><strong>0</strong></td>
</tr>
</tbody>
</table>

To clear protocol discovery statistics, use the following command:

```
Device# clear ip nbar protocol-discovery wlan wlan-profile-name
```
CHAPTER 56

NBAR Dynamic Protocol Pack Upgrade

- NBAR Dynamic Protocol Pack Upgrade, on page 441
- Upgrading the NBAR2 Protocol Pack, on page 442
- Setting a Custom Application, on page 442

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).

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ip nbar protocol-pack bootflash:pack-name</td>
<td>Loads the protocol pack.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip nbar protocol-pack bootflash:mypp.pack</td>
<td></td>
</tr>
</tbody>
</table>

Setting a Custom Application

Follow the procedure given below to set a custom application:

Note

When you add custom application rules, only the new flows matching those rules will appear. Existing flows will still be identified with the default NBAR rules.
### Setting a Custom Application

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td>2</td>
<td>ip nbar custom custom-protocol http host host-string</td>
<td>Configures the custom protocol and sets the HTTP host.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device(config)# ip nbar custom myapp</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>Custom applications take precedence over built-in protocols.</td>
</tr>
<tr>
<td>3</td>
<td>Run one of the following commands:</td>
<td>Sets the HTTP host or custom protocols based on the IP protocol.</td>
</tr>
<tr>
<td></td>
<td>• http host host-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ip address ip-address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td><em>Device(config-custom)# http host <a href="http://www.cisco.com">www.cisco.com</a></em></td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Device(config-custom)# ip address 8.9.71.50 8.9.71.11 8.9.71.14</em></td>
</tr>
<tr>
<td>4</td>
<td>port port-no</td>
<td>Sets the port number to use.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device(config-custom)# port 1111</td>
</tr>
<tr>
<td>5</td>
<td>dscp dscp-value</td>
<td>Sets the DSCP.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device(config-custom)# dscp 0</td>
</tr>
<tr>
<td>6</td>
<td>direction any</td>
<td>Sets the flow direction.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device(config-custom)# direction any</td>
</tr>
</tbody>
</table>

**What to do next**

CHAPTER 57

Conditional Debug, Radioactive Tracing, and Packet Tracing

- Introduction to Conditional Debugging, on page 445
- Introduction to Radioactive Tracing, on page 446
- Conditional Debugging and Radioactive Tracing, on page 446
- Location of Tracefiles, on page 446
- Configuring Conditional Debugging, on page 447
- Radioactive Tracing for L2 Multicast, on page 449
- Recommended Workflow for Trace files, on page 449
- Copying Tracefiles Off the Box, on page 449
- Configuration Examples for Conditional Debugging, on page 450
- Verifying Conditional Debugging, on page 451
- Example: Verifying Radioactive Tracing Log for SISF, on page 451
- Information About Packet Tracing, on page 452
- Configuring Conditional Debugging Packet Tracing, on page 452
- Configuring Conditional Debugging Packet Tracing per AP, on page 454
- Configuring Conditional Debugging Packet Tracing per Client, on page 455
- Verifying Conditional Debugging Packet Tracing Configuration, on page 455

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.

- 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 13: Components Supporting Radio Active Tracing

<table>
<thead>
<tr>
<th>Components</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>SISF or FHS</td>
<td>The first-hop security features, includes IPv6 Address Glean and IPv6 Device Tracking. For more information, see Information About IPv6 Snooping.</td>
</tr>
<tr>
<td>LISP</td>
<td>Locator or ID Separation Protocol.</td>
</tr>
</tbody>
</table>

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.

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 tracelogs directory is also decided by the process. For example, WNCD process uses a limit of 400 files 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

Follow the procedure given below to configure conditional debugging:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>debug platform condition mac {mac-address}</td>
<td>Configures conditional debugging for the MAC Address specified in wireless flows.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# debug platform condition mac bc16.6509.3314</td>
<td></td>
</tr>
<tr>
<td></td>
<td>debug platform condition feature wireless mac {mac-address}</td>
<td>Configures conditional debugging for a feature using the specified MAC address.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# debug platform condition feature wireless mac b838.61a1.5433</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>debug platform condition start</td>
<td>Starts conditional debugging (this will start radioactive tracing if there is a match on one of the conditions above).</td>
</tr>
<tr>
<td></td>
<td>Example: Device# debug platform condition start</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>show platform condition OR show debug</td>
<td>Displays the current conditions set.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# show platform condition Device# show debug</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Conditional Debugging

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>debug platform condition stop</td>
<td>Stops conditional debugging (this will stop radioactive tracing).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# debug platform condition stop</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>request platform software trace archive [last {number} days] [target {crashinfo:</td>
<td>(Optional) Displays historical logs of merged tracefiles on the system. Filter on any combination of number of days or location.</td>
</tr>
<tr>
<td></td>
<td>flashinfo:;]</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# request platform software trace archive last 2 days</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>request platform software trace filter-binary</td>
<td>(Optional) Filters the modules to collate the information (wire or wireless) and then on the context of Mac address specified. These logs can be viewed off-line.</td>
</tr>
<tr>
<td></td>
<td>{wire</td>
<td>wireless} [context {mac-address}</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# request platform software trace filter-binary wireless</td>
<td></td>
</tr>
<tr>
<td></td>
<td>context mac-address bc16.6509.3314</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td>show platform software trace filter-binary wireless</td>
<td>(Optional) Displays the consolidated log produced by all features.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show platform software trace filter-binary wireless</td>
<td></td>
</tr>
<tr>
<td></td>
<td>bc16.6509.3314</td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>show platform software trace [counter</td>
<td>filter-binary] level</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show platform software trace message</td>
<td></td>
</tr>
<tr>
<td>Step 11</td>
<td>clear platform condition all</td>
<td>Clears all conditions.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# clear platform condition all</td>
<td></td>
</tr>
</tbody>
</table>

### What to do next

#### Note

The commands `request platform software trace filter-binary` and `show platform software trace filter-binary` work in a similar way. The only difference is:

- `request platform software trace filter-binary`: Sources the data from historical logs.
- `show platform software trace filter-binary`: Sources the data from the flash Temp directory.
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 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.

```bash
deploy platform condition feature multicast controlplane mac client MAC address ip Group IP address 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:
   
   ```bash
   Device# request platform software trace archive last 1 day
   ```

2. The system generates a tar ball (.gz file) of the tracelogs in the location /flash:

3. Copy the file off the switch device. 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 (.gz) file from /flash: location. This will ensure enough space on the switch device for other operations.

**Copying Trace files Off the Box**

An example of the tracefile is shown below:

```bash
Device# dir crashinfo:/tracelogs
Directory of crashinfo:/tracelogs/
```
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
  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

```

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show platform condition</td>
<td>Displays the current conditions set.</td>
</tr>
<tr>
<td>show debug</td>
<td>Displays the current debug conditions set.</td>
</tr>
<tr>
<td>show platform software trace filter-binary</td>
<td>Displays logs merged from the latest tracefile.</td>
</tr>
<tr>
<td>request platform software trace filter-binary</td>
<td>Displays historical logs of merged tracefiles on the system.</td>
</tr>
</tbody>
</table>

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 13:46:10.667 {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): 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
Information About Packet Tracing


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

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| **Example:**  
Device> enable | 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 | Redirects all traced packets to bootflash.  
Converts the packet_trace.txt to pcap and downloads the pcap files. You can do so using the following link:  

**Example:**  
Device# show platform hardware chassis  
active qfp feature packet-trace packet  
all | redirect bootflash:packet_trace.txt
# Configuring Conditional Debugging Packet Tracing per AP

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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/n | 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  
Device# debug platform condition interface TenGigabitEthernet 0/0/0 match ipv4 192.168.1.2/32 both | Enables conditional debugging with IP filter.  
Here,  
**intf-number**—Is the GigabitEthernet interface number. Valid range is from 1 to 32. |
## Configuring Conditional Debugging Packet Tracing per Client

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td>Enter your password, if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>debug platform condition interface {intf-name</td>
<td>Enables conditional debugging for a wireless client interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>device</td>
<td>Here,</td>
</tr>
<tr>
<td></td>
<td>cpp cpp-handle-index} {mac</td>
<td>\cpp-handle-index—Valid range is from 1 to 4294967295.</td>
</tr>
<tr>
<td></td>
<td>ipv4</td>
<td>\ ipv4</td>
</tr>
<tr>
<td></td>
<td>[ipv4</td>
<td>ipv6</td>
</tr>
<tr>
<td></td>
<td>Device# debug platform condition interface cpp 0xa0000001 match ipv4 protocol icmp host 192.168.1.100 host 192.168.1.1 both</td>
<td></td>
</tr>
</tbody>
</table>

### 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
Verifying Conditional Debugging Packet Tracing Configuration
Aggressive Client Load Balancing

- Information About Configuring Aggressive Client Load Balancing, on page 457
- Configuring Aggressive Client Load Balancing (GUI), on page 458
- Configuring Aggressive Client Load Balancing (CLI), on page 458

Information About Configuring Aggressive Client Load Balancing

Enabling aggressive load balancing on the Cisco Wireless Controller 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.
For a FlexConnect AP, the association is locally handled. The load-balancing decisions are taken at Cisco WLC. A FlexConnect AP sends an initial response to the client before knowing the result of the calculations in Cisco WLC. 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.

**Configuring Aggressive Client Load Balancing (GUI)**

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Configuration &gt; Wireless &gt; WLANs &gt; Wireless Networks.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select a WLAN to view the Edit WLAN window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Advanced tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select the Load Balance check box to enable the feature.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Update &amp; Apply to Device.</td>
</tr>
</tbody>
</table>

**Configuring Aggressive Client Load Balancing (CLI)**

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device # configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>wlan wlan-name</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>wlan-name, Enter the WLAN name.</td>
</tr>
<tr>
<td>Device (config)# wlan test-wlan</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>shutdown</td>
<td>Disables the WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device (config-wlan)# shutdown</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>5</td>
<td>load-balance</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Device (config-wlan) # load-balance</code></td>
</tr>
<tr>
<td>6</td>
<td>no shutdown</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Device (config-wlan)# no shutdown</code></td>
</tr>
<tr>
<td>7</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# end</code></td>
</tr>
<tr>
<td>8</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Device # configure terminal</code></td>
</tr>
<tr>
<td>9</td>
<td>wireless load-balancing window</td>
</tr>
<tr>
<td></td>
<td>number-of-clients(0-20)</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Device (config) # wireless load-balancing window 2</code></td>
</tr>
<tr>
<td>10</td>
<td>wireless load-balancing denial</td>
</tr>
<tr>
<td></td>
<td>load-balancing-denial-count(1-10)</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Device (config) # wireless load-balancing denial 5</code></td>
</tr>
<tr>
<td>11</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Device (config-wlan) # end</code></td>
</tr>
<tr>
<td>12</td>
<td>show running-config</td>
</tr>
<tr>
<td></td>
<td>section wlan-name</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>`Device# show running-config</td>
</tr>
</tbody>
</table>
Configuring Aggressive Client Load Balancing (CLI)
Accounting Identity List

- Configuring Accounting Identity List (GUI), on page 461
- Configuring Accounting Identity List (CLI), on page 461
- Configuring Client Accounting (GUI), on page 462
- Configuring Client Accounting (CLI), on page 462

Configuring Accounting Identity List (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configuration &gt; Security &gt; AAA</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the <strong>Accounting</strong> section, click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Quick Setup: AAA Accounting</strong> window that is displayed, enter a name for your method list.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose the type of authentication as identity, in the <strong>Type</strong> drop-down list.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Choose the server groups you want to use to authenticate access to your network, from the <strong>Available Server Groups</strong> list and click &gt; icon to move them to the <strong>Assigned Server Groups</strong> list.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Save &amp; Apply to Device</strong>.</td>
</tr>
</tbody>
</table>

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.
### Configuring Client Accounting (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa accounting identity named-list start-stop group server-group-name</td>
<td>Enables accounting to send a start-record accounting notice when a client is authorized and a stop-record at the end.</td>
<td></td>
</tr>
</tbody>
</table>

#### Example:

```
Device(config)# aaa accounting identity user1 start-stop group aaa-test
```

#### 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 (CLI)

Follow the procedure given below to configure client accounting.

**Before you begin**

Ensure that RADIUS accounting is configured.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>wireless profile policy profile-policy</td>
<td>Configures WLAN policy profile and enters wireless policy configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# wireless profile policy default-policy-profile</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> shutdown</td>
<td>Disables the policy profile.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> accounting-list <code>list-name</code></td>
<td>Sets the accounting list.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# accounting-list user1-list</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no shutdown</td>
<td>Enables the policy profile.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 60

Wireless Multicast

- Information About Wireless Multicast, on page 465
- Prerequisites for Configuring Wireless Multicast, on page 469
- Restrictions on Configuring Wireless Multicast, on page 469
- Configuring Wireless Multicast, on page 470
- IPv6 Multicast over Multicast, on page 474
- Directed Multicast Service, on page 476
- Wireless Broadcast, Non-IP Multicast and Multicast VLAN, on page 478

Information About Wireless Multicast

If the network supports packet multicasting, the multicast method that the device uses can be configured. The device performs multicast routing in two modes:

- **Unicast mode**—The device unicasts every multicast packet to every access point associated to the device. 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 device sends multicast packets to a CAPWAP multicast group. This method reduces the overhead on the device 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 device receives a multicast packet from the wired LAN, the device encapsulates the packet using CAPWAP and forwards the packet to the CAPWAP multicast group address. The device 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 device 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 device 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 device then updates the access-point MGID table on the corresponding access point with the client MAC address. When the device 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 VLAN. 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 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 multicast 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.

**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 or RA guard 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.

**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

IPv6 RA Guard

The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue RA guard messages that arrive at the network device platform. RAs are used by devices to announce themselves on the link. The IPv6 RA Guard feature analyzes these RAs and filters out RAs that are sent by unauthorized devices. In host mode, all RA and router redirect messages are disallowed on the port. The RA guard feature compares configuration information on the Layer 2 (L2) device with the information found in the received RA frame. Once the L2 device has validated the content of the RA frame and router redirect
frame against the configuration, it forwards the RA to its unicast or multicast destination. If the RA frame content is not validated, the RA is dropped.

In the wireless deployment RAs coming on wireless ports are dropped as routers cannot reside on these interfaces.

**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 device, 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.

**Restrictions for IPv6 Snooping**

The IPv6 snooping feature is not supported on Etherchannel ports.

**Restrictions for IPv6 RA Guard**

- The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is tunneled.
- This feature is supported only in hardware when the ternary content addressable memory (TCAM) is programmed.
- This feature can be configured on a switch port interface in the ingress direction.
- This feature supports host mode and router mode.
- This feature is supported only in the ingress direction; it is not supported in the egress direction.
- This feature is not supported on EtherChannel and EtherChannel port members.
- This feature is not supported on trunk ports with merge mode.
- This feature is supported on auxiliary VLANs and private VLANs (PVLANs). In the case of PVLANs, primary VLAN features are inherited and merged with port features.
- Packets dropped by the IPv6 RA Guard feature can be spanned.
• If the **platform ipv6 acl icmp optimize neighbor-discovery command** is configured, the IPv6 RA Guard feature cannot be configured and an error message will be displayed. This command adds default global Internet Control Message Protocol (ICMP) entries that will override the RA guard ICMP entries.

### Configuring Wireless Multicast

The following sections provide information about the various wireless multicast configuration tasks:

#### Configuring Wireless Multicast-MCMC Mode

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable`  
**Example:**  
Device> `enable`  

Enters privileged EXEC mode.  
Enter your password, if prompted. |
| Step 2 | `configure terminal`  
**Example:**  
Device# `configure terminal`  

Enters global configuration mode. |
| Step 3 | `wireless multicast`  
**Example:**  
Device(config)# `wireless multicast`  
Device(config)# `no wireless multicast`  

Enables multicast traffic for wireless clients.  
By default, multicast traffic is in disabled state.  
Use the no form of this command to disable the multicast traffic for wireless clients. |
| Step 4 | `wireless multicast ip-addr`  
**Example:**  
Device(config)# `wireless multicast 231.1.1.1`  
Device(config)# `no wireless multicast 231.1.1.1`  

Enables multicast-over-multicast. Use the no form of this command to disable the feature. |
| Step 5 | `end`  
**Example:**  
Device(config)# `end`  

Exits configuration mode. Alternatively, press Ctrl-Z to exit configuration mode. |
# Configuring Wireless Multicast-MCUC Mode

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td>Enter your password, if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>wireless multicast</td>
<td>Enables the multicast traffic for wireless clients and enables mDNS bridging. By default, the feature is in disabled state. Use the no form of this command to disable the multicast traffic for wireless clients and disable mDNS bridging.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless multicast</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>wireless multicast ip-addr</td>
<td>Enables multicast-over-multicast. Use the no form of this command to disable the feature.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless multicast 231.1.1.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# no wireless multicast 231.1.1.1</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Exits configuration mode. Alternatively, press Ctrl-Z to exit configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

# Configuring IPv6 Snooping

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td>Enter your password, if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Configuring IPv6 Snooping Policy

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device# configure terminal</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>Enter your password, if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures an IPv6 snooping policy with a name.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Device(config)# ipv6 snooping policy mypolicy</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures the security level to inspect and drop unauthorized messages, if any.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Device(config-ipv6-snooping)# security-level guard</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures the role of the device, which is a node, to the attached port.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Device(config-ipv6-snooping)# device-role node</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Sets the protocol to glean addresses in either the DHCP or the NDP packets.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Device(config-ipv6-snooping)# protocol ndp</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Layer 2 Port as Multicast Router Port

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> ipv6 mld snooping vlan vlan-id mrouter interface Port-channel port-channel-interface-number</td>
<td>Configures a Layer 2 port as a Multicast router port. The VLAN is the client VLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# ipv6 mld snooping vlan 2 mrouter interface Port-channel 22</td>
<td></td>
</tr>
</tbody>
</table>

Configuring IPv6 RA Guard

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> ipv6 nd raguard policy policy-name</td>
<td>Configures a policy for RA guard.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# ipv6 nd raguard policy myraguardpolicy</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> trusted-port</td>
<td>Sets up a trusted port.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-nd-raguard)# trusted-port</td>
<td></td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Policy Profile Name</th>
<th>default-policy-profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>default policy profile</td>
</tr>
<tr>
<td>Status</td>
<td>ENABLED</td>
</tr>
<tr>
<td>VLAN</td>
<td>vlan-pool1</td>
</tr>
<tr>
<td>Multicast VLAN</td>
<td>84</td>
</tr>
<tr>
<td>Client count</td>
<td>0</td>
</tr>
<tr>
<td>Passive Client</td>
<td>DISABLED</td>
</tr>
</tbody>
</table>

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-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.
### Configuring IPv6 Multicast-over-Multicast

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>wireless multicast {ipv4-address</td>
<td>ipv6 ipv6-address)</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless multicast ipv6 ff45:1234::86</td>
<td></td>
</tr>
</tbody>
</table>

### 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

---

**Table 14: Multicast Support Per Platform**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Multicast Support - Multicast over Unicast</th>
<th>Multicast Support - Multicast over Multicast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Catalyst 9800-40 Wireless Controller</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Catalyst 9800-80 Wireless Controller</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Catalyst 9800 Wireless Controller for Cloud - Small Template</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Catalyst 9800 Wireless Controller for Cloud - Medium Template</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Catalyst 9800 Wireless Controller for Cloud - Large Template</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Wireless &gt; WLANs &gt; Wireless Networks.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select a WLAN to view the Edit WLAN window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Advanced tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Check the Directed Multicast Service check box to enable the feature.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Update &amp; Apply to Device.</td>
</tr>
</tbody>
</table>

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**

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

<table>
<thead>
<tr>
<th>Step 2</th>
<th>wlan profile-name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wlan test5</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Configures the WLAN profile and enters WLAN profile configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# shutdown</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Disables the WLAN profile.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>dms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# dms</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Configures DMS processing per WLAN.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>no shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# no shutdown</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Enables the WLAN profile.</td>
</tr>
</tbody>
</table>

---

### 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
```

### IEEE 802.11v Parameters

```
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 parameters
  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

Configuring Non-IP Wireless Multicast

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.
## Configuring Wireless Broadcast (GUI)

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Configuration</strong> &gt; <strong>Services</strong> &gt; <strong>Multicast</strong>.</th>
</tr>
</thead>
</table>
| 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 adjacent to the VLAN ID in the **Disabled** state to the **Enabled** state to enable broadcast packets for a VLAN.  
The default value is disabled. |
**Configuring Wireless Broadcast**

**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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>wireless broadcast</td>
<td>Enables broadcast packets for wireless clients. By default, the broadcast packets for wireless clients is in Disabled state. Enabling <strong>wireless broadcast</strong> enables broadcast traffic for each VLAN. Use the <strong>no</strong> form of this command to disable broadcasting packets.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless broadcast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# no wireless broadcast</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>wireless broadcast vlanvlanid</td>
<td>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 <strong>no</strong> form of this command to disable broadcast traffic for each VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless broadcast vlan 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# no wireless broadcast vlan 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
<td>Exits configuration mode. Alternatively, press <strong>Ctrl-Z</strong> to exit configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Multicast-over-Multicast for All the AP Multicast Groups (CLI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>ap capwap multicast IP address</strong></td>
<td>Configures an all-AP multicast group to send a single packet to all the APs.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ap capwap multicast 239.4.4.4</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>wireless multicast IP address</strong></td>
<td>Enables Multicast-over-Multicast for multicasting client multicast group traffic to all the APs through the underlying all-AP multicast group.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless multicast 239.4.4.4</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>end</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Verifying Wireless Multicast

Table 15: Commands for Verifying Wireless Multicast

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless multicast</td>
<td>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.</td>
</tr>
<tr>
<td>show wireless multicast group summary</td>
<td>Displays all (Group and VLAN) lists and the corresponding MGID values.</td>
</tr>
<tr>
<td>show wireless multicast [source source]</td>
<td>Displays details of the specified (S,G,V) and shows all the clients associated with and their MC2UC status.</td>
</tr>
<tr>
<td>group group vlan vlanid</td>
<td></td>
</tr>
<tr>
<td>show ip igmp snooping wireless mcast-ipe-count</td>
<td>Displays the number of multicast IPCs per MGID sent to the wireless controller module.</td>
</tr>
<tr>
<td>show ip igmp snooping wireless mgid</td>
<td>Displays the MGID mappings.</td>
</tr>
<tr>
<td>show ip igmp snooping igmpv2-tracking</td>
<td>Displays the client-to-SGV mappings and the SGV-to-client mappings.</td>
</tr>
</tbody>
</table>
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 multicast 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

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
</tr>
<tr>
<td>2</td>
<td>wireless profile policy <em>profile-policy</em></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless profile policy default-policy-profile</td>
</tr>
<tr>
<td>3</td>
<td>central association</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# central association</td>
</tr>
<tr>
<td>4</td>
<td>central switching</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# central switching</td>
</tr>
<tr>
<td>5</td>
<td>description <em>policy-profile-name</em></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# description &quot;default policy profile&quot;</td>
</tr>
<tr>
<td>6</td>
<td>vlan <em>vlan-name</em></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# vlan 32</td>
</tr>
<tr>
<td>7</td>
<td>multicast vlan <em>vlan-id</em></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# multicast vlan 84</td>
</tr>
<tr>
<td>8</td>
<td>no shutdown</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# no shutdown</td>
</tr>
</tbody>
</table>

**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
CHAPTER 61

Map-Server Per-Site Support

- Information About Map Server Per Site Support, on page 485
- Configuring the Default Map Server (GUI), on page 486
- Configuring the Default Map Server (CLI), on page 486
- Configuring a Map Server Per Site (GUI), on page 487
- Configuring a Map Server Per Site (CLI), on page 487
- Creating a Map Server for Each VNID (GUI), on page 488
- Creating a Map Server for Each VNID, on page 488
- Creating a Fabric Profile and Associating a Tag and VNID (GUI), on page 489
- Creating a Fabric Profile and Associating a Tag and VNID (CLI), on page 489
- Verifying the Map Server Configuration, on page 490

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 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 wireless fabric control-plane</td>
<td>Configures the control plane name.</td>
</tr>
<tr>
<td>control-plane-name</td>
<td></td>
</tr>
</tbody>
</table>
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

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Device(config)# wireless fabric control-plane test-map</td>
<td>If you do not provide a control plane name, the default-control-plane that is auto generated is used.</td>
</tr>
<tr>
<td><strong>Step 3</strong> ip address ip-address key pre-shared-key</td>
<td>Configures IP address and the key for the control plane.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wireless-cp)#ip address 10.12.13.14 key secret</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 Choose one of the following:</td>
<td></td>
</tr>
<tr>
<td>• wireless fabric name v nid-map</td>
<td>Configures a map server for each VNID in Layer 2 and Layer 3 or a map</td>
</tr>
<tr>
<td>l2-vnid l3-vnid l3vnid ip subnet-</td>
<td>server for a client VNID.</td>
</tr>
<tr>
<td>mask control-plane</td>
<td></td>
</tr>
<tr>
<td>control-plane</td>
<td></td>
</tr>
</tbody>
</table>
### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>config terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# wireless profile fabric test-fabric</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>sgt-tag value</code></td>
<td>Configures an SGT tag.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# sgt-tag cp1</code></td>
<td></td>
</tr>
</tbody>
</table>
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
--- | --- | --- | --- | ---
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
--- | --- | --- | --- | --- | ---
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
Verifying the Map Server Configuration
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.

This feature is supported only on Wave 2 APs.

* Configuring Volume Metering, on page 493

Confuguring Volume Metering

Follow the procedure given below to configure volume metering:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ap profile profile-name</td>
<td>Configures an AP profile and enters ap profile configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ap profile yy-ap-profile</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>dot11 24ghz reporting-interval reporting-interval</td>
<td>Configures the dot11 parameters.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-profile)# dot11 24ghz reporting-interval 60</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>dot11 5ghz reporting-interval reporting-interval</td>
<td>Configures the dot11 parameters.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-ap-profile)# dot11 5ghz reporting-interval 60</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Returns to global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-ap-profile)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> aaa accounting update periodic interval-in-minutes</td>
<td>Sets the time interval (in minutes) at which the controller sends interim accounting updates of the client to the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# aaa accounting update periodic 75</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Exits configuration mode and returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# exit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 495
• Configuring Syslog Server for an AP Profile, on page 497
• Configuring Syslog Server for the Controller, on page 498
• Verifying Syslog Server Configurations, on page 500

Information About Enabling Syslog Messages in Access Points and Controller for Syslog Server

You will be able to view the Syslog server messages only after an AP join.

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.
• syslog—Syslog itself.
• user—User process.
• uucp—Unix-to-Unix copy system.

Note
For more information about the usage of the syslog facilities and levels, refer to RFC 5424 (The Syslog Protocol).
## Configuring Syslog Server for an AP Profile

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ap profile ap-profile</code></td>
<td>Configures an AP profile and enters the AP profile configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ap profile xyz-ap-profile</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>syslog facility</code></td>
<td>Configures the facility parameter for Syslog messages.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-profile)# syslog facility</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>syslog host ip-address</code></td>
<td>Configures the Syslog server IP address and parameters.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-profile)# syslog host 9.3.72.1</td>
<td></td>
</tr>
</tbody>
</table>
| Step 5 | `syslog level {alerts | critical | debugging | emergencies | errors | informational | notifications | warnings}` | Configures the Syslog server logging level. The following are the Syslog server logging levels:
|        | Example:                                      |                                                                          |
|        | Device(config-ap-profile)# syslog level        |                                                                          |
|        | • `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.                                             |
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.

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

## Configuring Syslog Server for the Controller

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`logging host {hostname</td>
<td>ipv6}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# logging host 124.3.52.62</td>
<td></td>
</tr>
</tbody>
</table>
| **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` | 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. |
<p>| <strong>Example:</strong> | Device(config)# logging facility syslog |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• news—USENET news.</td>
<td></td>
</tr>
<tr>
<td>• sys10 to sys14 and sys9—System use.</td>
<td></td>
</tr>
<tr>
<td>• syslog—Syslog itself.</td>
<td></td>
</tr>
<tr>
<td>• user—User process.</td>
<td></td>
</tr>
<tr>
<td>• uucp—Unix-to-Unix copy system.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 4**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`logging trap {severity-level</td>
<td>alerts</td>
</tr>
</tbody>
</table>

- • **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.
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 join 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 Configurations 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

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x
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 Configurations
Login Banner

- Information About Login Banner, on page 505
- Configuring a Login Banner, on page 505

Information About Login Banner

Login banner is used to display a warning or message when you try to login to the controller.

To create a login banner, you must configure a delimiting character that notifies the system that the following text string must be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any single character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string for the banner.

Note

When HTTP authentication is configured using TACACS+/RADIUS, the banner message does not display on the Web UI.

Configuring a Login Banner

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Device# enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>banner login c message c</td>
<td>Specifies the login message.</td>
</tr>
</tbody>
</table>
## Configuring a Login Banner

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# banner login $</td>
<td>• c—Enters the delimiting character of your choice, for example, a pound sign (#), and press the <strong>Return</strong> key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.</td>
</tr>
<tr>
<td>Access for authorized users only. Please enter your username and password. $</td>
<td>• message—Enters a login message up to 255 characters. You cannot use the delimiting character in the message.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Device(config)# end

Device# show running-config

Device# copy running-config startup-config
Software Maintenance Upgrade

• Introduction to Software Maintenance Upgrade, on page 507
• Information About AP Device Package, on page 510
• Information About Per Site or Per AP Model AP SMU Upgrade (APSP), on page 512

Introduction to Software Maintenance Upgrade

The 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 on a per release and per component basis, and is specific to the platform.

A SMU provides a significant benefit over classic IOS software as 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 non-compatible SMUs.

All SMUs are integrated into the subsequent Cisco IOS XE software maintenance releases. A SMU is an independent and self-sufficient package and it does not have any prerequisites or dependencies. You can choose which SMUs to install or uninstall in any order.

SMU infrastructure can be used to meet the following requirements in the wireless context:

- Controller SMU: Controller bug fixes or PSIRTs
- APSP: AP bug fixes, PSIRTs, or minor features which 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 of the AP images in the controller. We recommend that you clear the statistics using clear ap predownload statistics command, before using the show ap image command to ensure correct data.

SMU Workflow

The SMU process is initiated with a request to the SMU committee. Contact your customer support to raise an SMU request. At release time, the SMU package is posted to 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 that the SMU is requested for.

SMU Reload

The SMU type describes the effect to a system after installing the SMU. SMUs can be non-traffic 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 currently). This reload ensures that all processes are started with the correct libraries and files that are installed as part of the SMU.

Controller hot patching support allows 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 SMU

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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. |
### Rollback SMU

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>install rollback to {base</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# install rollback to id 1234</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>install commit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# install commit</td>
</tr>
</tbody>
</table>

### Deactivate SMU

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>install deactivate file bootflash: filename</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# install deactivate file bootflash:&lt;Filename&gt;</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>install commit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# install commit</td>
</tr>
</tbody>
</table>

### 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 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.

Installing AP Device Package

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>install add file bootflash:&lt;filename&gt;</code></td>
<td>Extracts AP images from APDP and places them in SMU or APDP specific mount location.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device# install add file bootflash:&lt;Filename&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td>Here, the SMU does not trigger the Wireless module.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>install activate file bootflash:&lt;filename&gt;</code></td>
<td>Adds the AP software in APDP to the existing current active AP image list.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device# install activate file bootflash:&lt;Filename&gt;</code></td>
<td>Also, updates the capability information for the new AP models in the controller.</td>
</tr>
<tr>
<td>Note:</td>
<td>Even if the new AP module supports new hardware capabilities, the controller recognizes only the capability information that its base version supports.</td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td>At this point, the controller accepts the new connection from the new AP model. The new AP model then joins the controller.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>install commit</code></td>
<td>Commits the new AP software to be persistent across relogs.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device# install commit</code></td>
<td>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.</td>
</tr>
</tbody>
</table>
## Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> install deactivate file bootflash: <em>filename</em></td>
<td>(Optional) Deactivates an active APDP, updates the package status, and triggers a process to restart or reload.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# install deactivate file bootflash:&lt;<em>Filename</em>&gt;</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 5** show version | Displays the image version on the device. |
| **Example:**            |                                              |
| Device# show version    |                                              |

## Verifying APDP and APSP on the Controller

To verify the status of APDP and APSP 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
--------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Type</th>
<th>St</th>
<th>Filename/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>APDP</td>
<td>I</td>
<td>bootflash:apdp_CSCvp12345.bin</td>
</tr>
<tr>
<td>IMG</td>
<td>C</td>
<td>17.1.0.0</td>
</tr>
</tbody>
</table>
--------------------------------------------------------------------------------
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 AP SMU Upgrade (APSP)

The controller supports critical updates to the access points (APs) using Software Maintenance Update (SMU). Using the Per Site or Per AP Model AP SMU Upgrade 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 you 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 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.
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.

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.

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.
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]
```

Note: Rolling AP upgrade is not resumed after an SSO. You should run the `ap image upgrade` command to restart the rolling AP upgrade from the beginning and it affects all the APs, including the Mesh APs.

Installing APSP

Use the following procedure to roll out critical bug fixes to a subset of APs using SMU.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>install add file file-name</strong></td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
### Adding a Site to a Filter

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Adds a site tag to a site filter.</td>
</tr>
<tr>
<td><code>ap image site-filter file file-name add site-tag</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# ap image site-filter file flash:&lt;file-name&gt; add bg118</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(Optional) Removes a site tag from a site filter.</td>
</tr>
<tr>
<td><code>ap image site-filter file file-name remove site-tag</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# ap image site-filter file flash:&lt;file-name&gt; remove bg118</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Performs predownload of an AP image. This image predownload will be filtered by the site filter, set up in the previous step.</td>
</tr>
<tr>
<td><code>ap image predownload</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# ap image predownload</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Triggers the AP upgrade in rolling a staggered fashion for the APs added in site filter.</td>
</tr>
<tr>
<td><code>install activate file file-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# install activate file flash:&lt;file-name&gt;</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>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.</td>
</tr>
<tr>
<td><code>install commit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# install commit</td>
<td></td>
</tr>
</tbody>
</table>
Deactivating an Image

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>install deactivate file flash &lt;file-name&gt;</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# install deactivate file flash:&lt;file-name&gt;</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>install add profile rollback_profile-name</td>
<td>(Optional) Moves back to any rollback points in a graceful way with AP image predownload support. To get a list of available rollback profile names, use show install profile command.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# install add profile rollback_id1</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** (Optional) Performs predownload of an AP image. This image predownload will be filtered by the site filter, set up in the previous step.

| **Step 2**        |         |
| ap image predownload | (Optional) Performs rollback of the image for the affected AP models. The rollback action is not filtered by site. Therefore, rollback applies to all the sites. |
| **Example:**      |         |
| Device# ap image predownload | |

| **Step 3**        |         |
| install rollback to rollback_id | Performs rollback of the image for the affected AP models. The APs that are in the base image or in a point before the rollback action takes effect are not affected. |
| **Example:**      |         |
| Device# install rollback to rollback_id1 |
Aborting the Upgrade

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>install abort</strong></td>
<td>Aborts the upgrade by resetting the APs in rolling fashion.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# install abort</td>
<td></td>
</tr>
</tbody>
</table>

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
----------------------------------------

<table>
<thead>
<tr>
<th>AP Image Type</th>
<th>Capwap Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap1g1</td>
<td>16.11.1.19</td>
</tr>
<tr>
<td>ap1g2</td>
<td>16.11.1.19</td>
</tr>
<tr>
<td>ap1g3</td>
<td>16.11.1.19</td>
</tr>
<tr>
<td>ap1g4</td>
<td>16.11.1.19</td>
</tr>
<tr>
<td>ap1g5</td>
<td>16.11.1.19</td>
</tr>
<tr>
<td>ap1g6</td>
<td>16.11.1.19</td>
</tr>
</tbody>
</table>

AP Image Prepare List**
----------------------------------------
Install File Name: vwlc_apsp_16.11.1.0_74.bin
----------------------------------------

<table>
<thead>
<tr>
<th>AP Image Type</th>
<th>Capwap Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap1g1</td>
<td>16.11.1.19</td>
</tr>
<tr>
<td>ap1g2</td>
<td>16.11.1.19</td>
</tr>
<tr>
<td>ap1g3</td>
<td>16.11.1.19</td>
</tr>
<tr>
<td>ap1g4</td>
<td>16.11.1.19</td>
</tr>
<tr>
<td>ap1g5</td>
<td>16.11.1.19</td>
</tr>
<tr>
<td>ap1g6</td>
<td>16.11.1.19</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Site Tag</th>
<th>Prepared</th>
<th>Activated</th>
<th>Committed</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgl-18-1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>bgl-18-2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>bgl-18-3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>default-site-tag</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Type</th>
<th>St</th>
<th>Filename/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>APSP</td>
<td>I</td>
<td>bootflash:vwlc_apsp_16.11.1.0_74.bin</td>
</tr>
<tr>
<td>IMG</td>
<td>C</td>
<td>16.11.1.0.1249</td>
</tr>
</tbody>
</table>

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
<table>
<thead>
<tr>
<th>Status</th>
<th>Number of APs</th>
<th>AP Name</th>
<th>Ethernet MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgraded</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>In Progress</td>
<td>1</td>
<td>APf07f.06a5.d78c</td>
<td>f07f.06cf.b910</td>
</tr>
<tr>
<td>Remaining</td>
<td>3</td>
<td>APCC16.7EDB.6FA6</td>
<td>0081.c458.ab30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AP38ED.18CA.2FD0</td>
<td>38ed.18cb.25a0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AP881d.fce7.5ee4</td>
<td>d46d.50ee.33a0</td>
</tr>
</tbody>
</table>
Verifying of AP Upgrade on the Controller
In-Service Software Upgrade

- Information About In-Service Software Upgrade, on page 521
- Prerequisites for Performing In-Service Software Upgrade, on page 522
- Guidelines and Restrictions for In-Service Software Upgrade, on page 522
- Upgrading Software Using In-Service Software Upgrade, on page 523
- Upgrading Software Using ISSU (GUI), on page 524
- Upgrading Software Using In-Service Software Upgrade with Delayed Commit, on page 525
- Monitoring In-Service Software Upgrade, on page 525
- Troubleshooting ISSU, on page 528

Information About In-Service Software Upgrade

In-Service Software Upgrade (ISSU) is a procedure to upgrade a wireless controller image to a later release or downgrade to an earlier release on a controller while the network continues to forward packets. ISSU helps network administrators avoid a network outage when performing a software upgrade.

Attention

ISSU feature is in beta test program. It is supported only within and between major releases, for example, 17.3.x (within a release) and 17.3.x to 17.6.x (among major releases). For feedback and support, contact c9800-issu-support@external.cisco.com.

ISSU can also be used to apply cold patches without impacting the active network.

ISSU is supported only on the following Cisco Catalyst 9800 Series Wireless Controllers, and supports upgrade and downgrade.

- Cisco Catalyst 9800-80 Wireless Controller
- Cisco Catalyst 9800-40 Wireless Controller
- Cisco Catalyst 9800-L Wireless Controller
- Cisco Catalyst 9800-CL Wireless Controller (Private Cloud)

High-Level Workflow of ISSU

1. Onboard the controller software image to the flash memory.
Prerequisites for Performing In-Service Software Upgrade

- Ensure that the controller is in install mode.
- Ensure that the network or device is not being configured during the upgrade.
- Schedule the upgrade when your network is stable and steady.
- Ensure uninterrupted power supply. A power interruption during upgrade procedure might corrupt the software image.

Guidelines and Restrictions for In-Service Software Upgrade

- During ISSU upgrade, while AP rolling upgrade is in progress, the **install abort** command won’t work. You should use the **install abort issu** command, instead to abort the upgrade.
- During ISSU upgrade, the system displays a warning message similar to:
  
  > found 46 disjoint TDL objects
  
  You can ignore the warning message because it doesn’t have any functional impact.
- During ISSU upgrade, if both the controllers (active and standby) have different images after the power cycle, an auto abort of ISSU is triggered to bring both the controllers to the same version. The following is a sample scenario: Install Version1 (V1) software on the active controller and then apply a SMU hot patch and perform a commit. Now, upgrade the software to Version2 using ISSU, and then power cycle the active controller. At this point, the system has a version mismatch (V1 and V2). The active controller reloads at this stage, after the completion of bulk synchronization. Now, both the controllers come up with the same version (V1 and V1).
- An ISSU upgrade that is aborted because of configuration synchronization failure on the standby controller rolls back to V1 of the software image. However, this information isn’t available in the **show install** command log. Run the **show issu state detail** command to see the current ISSU state.
- To enable the **clear install** command, you should first run the **service internal** command in privileged EXEC mode.
- The **clear install state** command doesn’t clear an added SMU. To remove a SMU, use either the **install remove file** command or the **install remove inactive** command.
- When the new active controller comes up, after the image upgrade, it doesn’t retain the old logs on web GUI window as part of show logs.
- If a stateful switchover (SSO) or a high-availability (HA) event occurs during the rolling AP upgrade procedure of the ISSU feature, the rolling AP upgrade stops. You should then use the **ap image upgrade** command to restart the upgrade process.
- If HA fails to form after the ISSU procedure, you should reload any one chassis again to form HA again.

- When you use ISSU to downgrade the controller image to version 1 (V1) after upgrading from controller version 1 (V1) and APSP version 1 (APSP1) to controller version 2 (V2) and APSP version 2 (APSP2), wrong image may get pushed to the AP. In such instances, remove APSP1 and reinstall it. After that, APSP1 images are pushed to the AP.

- Use clear ap predownload statistics command before using the show ap image command. This ensures that you get the right data after every pre-download.

# Upgrading Software Using In-Service Software Upgrade

Use the following procedure to perform a complete image upgrade, that is, from one image to another.

**Note**

ISSU is supported only within and between major releases, for example, 17.1.x to 17.1.x (within a release) and 17.1.x to 17.3.x (among major releases), that is, for two releases before and after the current release.

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>install add file file-name</td>
<td>The controller software image is added to the flash and expanded.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# install add file &lt;&gt;</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>In Cisco Catalyst 9800 Wireless Controller for Switch, run the install add file sub-package-file-name command to expand the wireless subpackage file.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ap image predownload</td>
<td>Performs predownload of the AP image.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# ap image predownload</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To see the progress of the predownload, use the show ap image command.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>install activate issu [auto-abort-timer timer]</td>
<td>Runs compatibility checks, installs the package, and updates the package status details.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# install activate issu</td>
<td>Optionally, you can configure the time limit to abort the addition of new software without committing the image. Valid values are from 30 to 1200 minutes.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Run either of the following commands:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• install abort issu</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# install abort issu</td>
<td>Aborts the upgrade process and returns the device to the previous installation state.</td>
</tr>
</tbody>
</table>
### Upgrading Software Using ISSU (GUI)

**Before you begin**

1. The device should be in Install mode.
2. The device should have an HA pair. The standby controller should be online and is in SSO mode.
   
   You can verify the details using `show issu state detail` command.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose Administration &gt; Software Management.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Under the Software Upgrade tab, check the ISSU Upgrade (HA Upgrade) (Beta) check box.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>In the AP Upgrade Configuration section, from the AP Upgrade per Iteration drop-down list choose the percentage of APs to be upgraded.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Click Download &amp; Install. This initiates the upgrade process and you can view the progress in the Status dialog box. Click the Show Logs link to view the upgrade process details.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>The system enables the Commit and ISSU Abort buttons after the upgrade. Click Commit to commit the activation changes, or ISSU Abort to terminate the upgrade process and return the device to the previous installation state.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is applicable for both controller and the AP. • install commit Device# install commit Commits the activation changes to be persistent across reloads.</td>
<td></td>
</tr>
</tbody>
</table>
### Upgrading Software Using In-Service Software Upgrade with Delayed Commit

Use this procedure to upgrade the controller software with delayed commit, which will help you to run and test the new software without committing the image.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `install add file file-name`<br>**Example:**<br>Device# install add file <> | Adds and expands the controller software image to the flash.  
**Note** In Cisco Catalyst 9800 Wireless Controller for Switch, run the `install add file sub-package-file-name` command to expand the wireless subpackage file. |
| Step 2 | `ap image predownload`<br>**Example:**<br>Device# ap image predownload | Performs predownload of the AP image. |
| Step 3 | `install auto-abort-timer stop`<br>**Example:**<br>Device# install auto-abort-timer stop | Stops the termination timer so that the upgrade process is not terminated after the default termination time of 6-8 hours. |
| Step 4 | `install activate issu`<br>**Example:**<br>Device# install activate issu | Runs compatibility checks, installs the package, and updates the package status details. |
| Step 5 | `install commit`<br>**Example:**<br>Device# install commit | Commits the activation changes to be persistent across reloads. |

#### Monitoring In-Service Software Upgrade

To view the ISSU state after the install add ISSU and before the install activate ISSU, use the following command:

```
Device# show issu state detail
```

-- Starting local lock acquisition on chassis 1 ---
Finished local lock acquisition on chassis 1
Current ISSU Status: Enabled
Previous ISSU Operation: Abort Successful
---------------------------------------------------------------
System Check Status
-------------------------------------------------------
Platform ISSU Support Yes
Standby Online Yes
Autoboot Enabled Yes
SSO Mode Yes
Install Boot Yes
Valid Boot Media Yes
-------------------------------------------------------

No ISSU operation is in progress
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 I 17.1.1.0.432
IMG C 16.12.2.0.2707
--------------------------------------------------------------------------------

Auto abort timer: inactive

To view the ISSU state after activating ISSU, use the following command:

Device# show issu state detail

Current ISSU Status: In Progress
Previous ISSU Operation: Abort Successful

System Check Status
-------------------------------------------------------
Platform ISSU Support Yes
Standby Online Yes
Autoboot Enabled Yes
SSO Mode Yes
Install Boot Yes
Valid Boot Media Yes

Operation type: Step-by-step ISSU
Install type : Image installation using ISSU
Current state : Activated state
Last operation: Switchover
Completed operations:
Operation Start time
-------------------------------------------------------
Activate location standby Chassis 2 2019-09-17:23:41:12
Activate location active Chassis 1 2019-09-17:23:50:06
Switchover 2019-09-17:23:52:03
State transition: Added -> Standby activated -> Active switched-over
Auto abort timer: automatic, remaining time before rollback: 05:41:53
Running image: bootflash:packages.conf
Operating mode: sso, terminal state reached
show install summary

[ Chassis 1/R0 2/R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted

Type St Filename/Version
--------------------------------------------------------------------------------
IMG U 17.1.1.0.432
--------------------------------------------------------------------------------

Auto abort timer: active on install_activate, time before rollback - 05:41:49
To view the ISSU state after installing the commit, use the following command:

Device# show issu state detail

--- Starting local lock acquisition on chassis 1 ---
Finished local lock acquisition on chassis 1
Current ISSU Status: Enabled
Previous ISSU Operation: Successful

System Check Status

Platform ISSU Support Yes
Standby Online Yes
Autoboot Enabled Yes
SSO Mode Yes
Install Boot Yes
Valid Boot Media Yes

No ISSU operation is in progress

show install summary

[ Chassis 1/R0 2/R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted

Type St Filename/Version

IMG C 17.1.1.0.432

Auto abort timer: inactive

To view the ISSU state after terminating the ISSU process, use the following command:

Device# show issu state detail

Current ISSU Status: In Progress
Previous ISSU Operation: Abort Successful

System Check Status

Platform ISSU Support Yes
Standby Online Yes
Autoboot Enabled Yes
SSO Mode Yes
Install Boot Yes
Valid Boot Media Yes

Operation type: Step-by-step ISSU
Install type : Image installation using ISSU
Current state : Timeout-error state
Last operation: Commit Chassis 1
Completed operations:

--------------------------------------------
Activate location standby Chassis 2 2019-09-17:23:41:12
Activate location active Chassis 1 2019-09-17:23:50:06
Switchover 2019-09-17:23:52:03
Abort 2019-09-18:00:14:13
Commit Chassis 1 2019-09-18:00:28:23
State transition: Added -> Standby activated -> Active switched-over -> Activated -> Timeout-error
Auto abort timer: inactive
Running image: bootflash:packages.conf
Operating mode: sso, terminal state reached
To view the summary of the active packages in a system, use the following command:

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 16.12.2.0.2707
--------------------------------------------------------------------------------
Auto abort timer: inactive

Troubleshooting ISSU

Using **install activate issu** command before completing AP pre-download.

The following scenario is applicable when you run the **install activate issu** command before completing AP pre-download. In such instances, you should run the **ap image predownload** command and then proceed with the activation.

Device# install activate issu

install_activate: START Wed Jan 8 04:48:04 UTC 2020
System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q] y
Building configuration...
(OK)Modified configuration has been saved
install_activate: Activating ISSU
NOTE: Going to start Activate ISSU install process
STAGE 0: System Level Sanity Check
-----------
--- Verifying install_issu supported ---
--- Verifying standby is in Standby Hot state ---
--- Verifying booted from the valid media ---
--- Verifying AutoBoot mode is enabled ---
--- Verifying Platform specific ISSU admission criteria ---
CONSOLE: FAILED: Install operation is not allowed.
Reason -> AP pre-image download is mandatory for hitless software upgrade.
Action -> Trigger AP pre-image download.
FAILED: Platform specific ISSU admission criteria
ERROR: install_activate exit(2) Wed Jan 8 04:48:37 UTC 2020
Chapter 67

WiFi Alliance Agile Multiband

- Introduction to Wi-Fi Alliance Agile Multiband, on page 529
- Limitations of MBO, on page 531
- Configuring MBO on a WLAN, on page 531
- Verifying MBO Configuration, on page 532

Introduction to Wi-Fi Alliance Agile Multiband

The Wi-Fi Alliance Agile Multiband (MBO) feature enables better use of Wi-Fi network resources. This feature is built on the fundamental premise that both Wi-Fi networks and client devices have information that can enable better roaming decisions and improve the overall performance of Wi-Fi networks and user experience.

Note

This feature applies to MBO certified clients only.

This feature certifies the interoperability of a bundle of features that are defined by the IEEE standard amendments 802.11k, 802.11v, and 802.11u, as well as the Wi-Fi-Alliance defined specifications. These technologies are used to exchange access points (AP), band, and channel preferences, link quality, and status information between AP and client device.

MBO focuses on the following:

- Interactions between the wireless clients and APs
- Exchange of AP and client knowledge about the wireless medium (such as RF neighbors)
- Allow clients to work with APs and take intelligent decisions on the connection and improve the quality of service.

Wi-Fi Alliance Agile Multiband Topology

Multiple components form a Wi-Fi Agile Multiband wireless infrastructure network, which may vary based on the wireless network deployment.

The following figure depicts the system topology for connecting Wi-Fi Agile Multiband devices.
The following components form a Wi-Fi Agile Multiband wireless infrastructure network:

- **Access Point (AP):** A Wi-Fi Agile Multiband wireless infrastructure network contains one or more Wi-Fi Agile Multiband APs.

- **WLAN Controller:** A Wi-Fi Agile Multiband wireless infrastructure network contains zero or more WLAN controllers that provide centralized management and other features to the interconnected APs.

- **Client Station (STA):** A Wi-Fi Agile Multiband wireless infrastructure network contains zero or more STAs. These client STAs are single WLAN capable only.

- **RADIUS Server:** A Wi-Fi Agile Multiband wireless infrastructure network contains zero or more RADIUS Servers that provide Authentication, Authorization, and Accounting (AAA) services.

### Supported MBO Components

**MBO AP Capability**

A new information element is added to the Beacon, Probe Response, Association Response and Re Association Response Frames for 802.11ax APs to inform clients about MBO support.

**Note**

The new information element indicates that Cisco APs are not cellular data aware.
When an SSID is configured on an AP, the MBO AP capability is enabled.

802.11k/v/r Support

One of the prerequisites for MBO is that APs need to support 802.11k/v/r standard-based technologies. Each of the technologies has their own requirements, such as:

• 802.11k – For 802.11k, send the preferred list of AP neighbors to the client upon request and send a beacon request to a client when AP requires a beacon report from the client.

• 802.11v – For 802.11v, steer the client to a less congested AP (not in a MBO client’s non-prefer/non-operable channel list that is sent during the association request and/or WNM notification request) using BSS transition.

• 802.11r – The 802.11r MBO-related capabilities are not supported.

802.11u ANQP or GAS Support

For MBO, the 802.11ax APs must have 802.11u ANQP or GAS support.

The following are the prerequisites:

• ANQP responds to the ANQP request for a neighbor report ANQP-element.

• Before authentication, Layer 2 transport needs to be available in the network between a mobile device and server for an advertisement protocol frame.

MBO Beacon Request

Whenever an AP sends a beacon request to the client, the MBO-compliant client responds with a beacon report.

MBO Associate Disallowed IE

Cisco APs include an Associate Disallowed IE in their Beacon/Probe response/(Re) association response when they cannot accommodate any new client.

Limitations of MBO

All non-802.11ax access points are not supported.

Configuring MBO on a WLAN

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td>configure terminal</td>
<td>wlan wlan-name wlan-id ssid</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Enters global configuration mode.</td>
<td>Configures a WLAN and enters the WLAN configuration mode.</td>
</tr>
</tbody>
</table>
Verifying MBO Configuration

To view the MBO configuration, use the following command:

```
Device# show wlan id 1
WLAN Profile Name : wlan-demo
```

```
Identifier : 1
Description :
Network Name (SSID) : ssid-demo
Status : Disabled
Broadcast SSID : Enabled
802.11ax parameters
  OFDMA Downlink : Enabled
  OFDMA Uplink : Enabled
  MU-MIMO Downlink : Enabled
  MU-MIMO Uplink : Enabled
  BSS Color : Enabled
  Partial BSS Color : Enabled
  BSS Color Code : 0
  BSS Target Wake Up Time : Enabled
  BSS Target Wake Up Time Broadcast Support : Enabled
mDNS Gateway Status : Bridge
WIFI Alliance Agile Multiband : Enabled
```

To view the non-operational or non-preferred channels, use the following command:

```
Device# show wireless client mac-address 3413.e8b5.f252 detail
Client MAC Address : 3413.e8b5.f252
Client IPv4 Address : 192.165.1.53
Client IPv6 Addresses : fe80::98bb:ea89:f016:3332
Client Username: N/A
AP MAC Address : 00ee.ab18.d920
AP Name: ssap-pp
AP slot : 1
Client State : Associated
Policy Profile : prof
Flex Profile : N/A
Wireless LAN Id: 1
WLAN Profile Name: mbo_1
```
Wireless LAN Network Name (SSID): mbo_1
BSSID : 00ee.ab18.d92f
Connected For : 25 seconds
Protocol : 802.11ax - 5 GHz
Channel : 36
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Session Timeout : 1800 sec (Remaining time: 1779 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 : Enabled
U-APSD value : 0
APSD ACs : BK, BE, VI, VO
Fastlane Support : Disabled
Client Active State : Active
Power Save : OFF
Current Rate : 1.5
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 : 05/15/2019 16:03:34 IST
Client Join Time:
  Join Time Of Client : 05/15/2019 16:03:34 IST
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 26 seconds
Policy Type : N/A
Encryption Cipher : None
User Personal Network : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : default
Multicast VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Point of Attachment : capwap_90400001
  IIF ID : 0x90400001
  Authorized : TRUE
  Session timeout : 1800
  Common Session ID : 000000000000000BB92939C5
  Acct Session ID : 0x00000000
  Last Tried Aaa Server Details:
    Server IP : None
    Auth Method Status List
    Method : None
    Local Policies:
      Service Template : wlan_svc_prof_local (priority 254)
      VLAN : 165
      Absolute-Timer : 1800
      Server Policies:
      Resultant Policies:
VLAN Name : VLAN0165
VLAN : 165
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 : Implemented
  11v DMS Capable : No
  QoS Map Capable : Yes
Non-Preferred Channels : 40
Non-Operable Channels : 56
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
FlexConnect Central Association : N/A
Client Statistics:
  Number of Bytes Received : 0
  Number of Bytes Sent : 0
  Number of Packets Received : 0
  Number of Packets Sent : 0
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -34 dBm
  Signal to Noise Ratio : 56 dB
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
Nearby AP Statistics:
EoGRE : No/Simple client
PART VI

Security

- IPv4 ACLs, on page 537
- DNS-Based Access Control Lists, on page 563
- Whitelisting of Specific URLs, on page 579
- Configuring Policy Enforcement and Usage Monitoring, on page 581
- Web-Based Authentication, on page 585
- Central Web Authentication, on page 613
- ISE Simplification and Enhancements, on page 633
- Authentication and Authorization Between Multiple RADIUS Servers, on page 645
- Secure LDAP (SLDAP), on page 653
- RADIUS DTLS, on page 661
- MAC Authentication Bypass, on page 673
- IP Source Guard, on page 683
- Managing Rogue Devices, on page 685
- Classifying Rogue Access Points, on page 697
- Configuring Secure Shell, on page 707
- Private PSK, on page 715
- Multi-Preshared Key, on page 723
- Multiple Authentications for a Client, on page 731
- Configuring Cisco TrustSec, on page 739
- SGT Inline Tagging and SXPv4, on page 751
- Locally Significant Certificates, on page 757
- Cisco Umbrella WLAN, on page 771
- FIPS, on page 783
- Device Ecosystem, on page 787
• Adaptive WIPS, on page 793
• Wi-Fi Protected Access 3, on page 797
IPv4 ACLs

- Information about Network Security with ACLs, on page 537
- Restrictions for Configuring IPv4 Access Control Lists, on page 546
- How to Configure ACLs, on page 546
- Monitoring IPv4 ACLs, on page 557
- Configuration Examples for ACLs, on page 558

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 router or switch 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 switch accepts or rejects the packets. Because the switch stops testing after the first match, the order of conditions in the list is critical. If no conditions match, the switch rejects the packet. If there are no restrictions, the switch forwards the packet; otherwise, the switch drops the packet. The switch can use ACLs on all packets it forwards.

You configure access lists on a router or Layer 3 switch 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.
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 switch 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).

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 other 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 B: 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.

You cannot 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.
VLAN Maps

VLAN ACLs or VLAN maps are used to control network traffic within a VLAN. You can apply VLAN maps to all packets that are bridged within a VLAN in the switch or switch stack. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces. VACLs are not defined by direction (ingress or egress).

All non-IP protocols are access-controlled through MAC addresses and Ethertype using MAC VLAN maps. (IP traffic is not access controlled by MAC VLAN maps.) You can enforce VLAN maps only on packets going through the switch; you cannot enforce VLAN maps on traffic between hosts on a hub or on another switch connected to this switch.

With VLAN maps, forwarding of packets is permitted or denied, based on the action specified in the map.

Figure 9: Using VLAN Maps to Control Traffic

This figure shows how a VLAN map is applied to prevent a specific type of traffic from Host A in VLAN 10 from being forwarded. You can apply only one VLAN map to a VLAN.

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

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.
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 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 16: Access List Numbers**

<table>
<thead>
<tr>
<th>Access List Number</th>
<th>Type</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>1–99</td>
<td>IP standard access list</td>
<td>Yes</td>
</tr>
<tr>
<td>100–199</td>
<td>IP extended access list</td>
<td>Yes</td>
</tr>
<tr>
<td>200–299</td>
<td>Protocol type-code access list</td>
<td>No</td>
</tr>
<tr>
<td>300–399</td>
<td>DECnet access list</td>
<td>No</td>
</tr>
<tr>
<td>400–499</td>
<td>XNS standard access list</td>
<td>No</td>
</tr>
<tr>
<td>500–599</td>
<td>XNS extended access list</td>
<td>No</td>
</tr>
<tr>
<td>600–699</td>
<td>AppleTalk access list</td>
<td>No</td>
</tr>
<tr>
<td>700–799</td>
<td>48-bit MAC address access list</td>
<td>No</td>
</tr>
<tr>
<td>800–899</td>
<td>IPX standard access list</td>
<td>No</td>
</tr>
<tr>
<td>900–999</td>
<td>IPX extended access list</td>
<td>No</td>
</tr>
<tr>
<td>1000–1099</td>
<td>IPX SAP access list</td>
<td>No</td>
</tr>
<tr>
<td>1100–1199</td>
<td>Extended 48-bit MAC address access list</td>
<td>No</td>
</tr>
<tr>
<td>1200–1299</td>
<td>IPX summary address access list</td>
<td>No</td>
</tr>
<tr>
<td>1300–1999</td>
<td>IP standard access list (expanded range)</td>
<td>Yes</td>
</tr>
<tr>
<td>2000–2699</td>
<td>IP extended access list (expanded range)</td>
<td>Yes</td>
</tr>
</tbody>
</table>
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, to terminal 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`)

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, not all commands that use IP access lists accept a named access list.

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.

Downloadable Access Control List (DACL) will fail if you use a named authorization network method list that is not sent from AAA server, as part of Access-Accept.

Examples of named and default authorization network are given below:

- Default:
  ```
  aaa authorization network default AAA_EXT
  ```

- Named:
  ```
  aaa authorization network XYZ AAA_EXT
  ```

**Note**

- DACL for IPv6 is supported only from ISE 2.6
- Before configuring DACL, ensure that RADIUS and AAA configuration are in place.

To view details about DACL, use the following show commands:

- `show wireless client mac-address mac-address detail`
- `show ip access-lists dacl-name`
- `show ipv6 access-lists dacl-name`

**ACL Logging**

The switch 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.
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.

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.

If an ACL configuration cannot be implemented in hardware due to an out-of-resource condition on a switch or stack member, then only the traffic in that VLAN arriving on that switch 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 switch checks the packet against the ACL. If the ACL permits the packet, the switch continues to process the packet. If the ACL rejects the packet, the switch discards the packet.

For outbound ACLs, after receiving and routing a packet to a controlled interface, the switch checks the packet against the ACL. If the ACL permits the packet, the switch sends the packet. If the ACL rejects the packet, the switch discards the packet.

When you apply an undefined ACL to an interface, the switch acts as if the ACL has not been applied to the interface and permits all packets. Remember this behavior if you use undefined ACLs for network security.
Restrictions for Configuring IPv4 Access Control Lists

General Network Security

The following are restrictions for configuring network security with ACLs:

- Not all commands that accept a numbered ACL accept a named ACL. ACLs for packet filters and route filters on interfaces can use a name.
- 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.
- ACL wildcard is not supported in downstream client policy.

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

Follow the procedure given below to use IP ACLs on the switch:
Creating a Numbered Standard ACL (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose Configuration &gt; Security &gt; ACL.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>On the ACL page, click Add.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>In the Add ACL Setup window, enter the following parameters.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ACL Name</strong>: Enter the name for the ACL</td>
</tr>
<tr>
<td></td>
<td>• <strong>ACL Type</strong>: IPv4 Standard</td>
</tr>
<tr>
<td></td>
<td>• <strong>Sequence</strong>: The valid range is between 1 and 99 or 1300 and 1999</td>
</tr>
<tr>
<td></td>
<td>• <strong>Action</strong>: Choose Permit or Deny access from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Source Type</strong>: Choose any, Host or Network</td>
</tr>
<tr>
<td></td>
<td>• <strong>Log</strong>: Enable or disable logging, this is limited to ACLs associated to Layer 3 interface only.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Click Add.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Click Save &amp; Apply to Device.</td>
</tr>
</tbody>
</table>

Creating a Numbered Standard ACL (CLI)

Follow the procedure given below to create a numbered standard ACL:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;<strong>Example:</strong></td>
</tr>
</tbody>
</table>
### Creating a Numbered Standard ACL (CLI)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Device# configure terminal | 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. 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 3**  
**access-list access-list-number **{**deny | permit**} **source source-wildcard**  
**Example:**  
Device(config)# access-list 2 deny your_host

**Step 4**  
**end**  
**Example:**  
Device(config)# end

**Step 5**  
**show running-config**  
**Example:**  
Device# show running-config

**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: 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  Click Save & Apply to Device.

Creating a Numbered Extended ACL (CLI)

Follow the procedure given below to create a numbered extended ACL:

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>access-list access-list-number {deny</td>
<td>permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]</td>
</tr>
</tbody>
</table>
**Creating a Numbered Extended ACL (CLI)**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
| `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 IP 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 and Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>or a name: normal (0), max-reliability (2), max-throughput (4), min-delay (8).</td>
<td></td>
</tr>
<tr>
<td>• time-range—Specify the time-range name.</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Your controller must support the ability to:</td>
<td></td>
</tr>
<tr>
<td>• Mark DSCP</td>
<td></td>
</tr>
<tr>
<td>• Mark UP</td>
<td></td>
</tr>
<tr>
<td>• Map DSCP and UP</td>
<td></td>
</tr>
<tr>
<td>For more information on DSCP-to-UP Mapping, see:</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> access-list access-list-number {deny</td>
<td>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]</td>
</tr>
<tr>
<td>Defines an extended TCP access list and the access conditions.</td>
<td></td>
</tr>
<tr>
<td>The parameters are the same as those described for an extended IPv4 ACL, with these exceptions:</td>
<td></td>
</tr>
<tr>
<td>(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).</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

Example:

```
Device(config)# access-list 101 permit tcp any any eq 500
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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] | 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).  
  (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-code | icmp-message] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp] | 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] | (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, pin, or trace. |

Device(config)# access-list 101 permit udp any any eq 100

Device(config)# access-list 101 permit icmp any any 200

Device(config)# access-list 101 permit igmp any any 14

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x
Creating Named Standard ACLs (GUI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Click Configuration &gt; Security &gt; ACL.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> Click Add to create a new ACL setup.</td>
<td></td>
</tr>
</tbody>
</table>
| **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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Creating Named Standard ACLs

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ip access-list standard name</td>
<td>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.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ip access-list standard 20</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Use one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• deny {source [source-wildcard]</td>
<td>host source</td>
</tr>
<tr>
<td></td>
<td>• permit {source [source-wildcard]</td>
<td>host source</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td>Device(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-std-nacl)# end</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
Creating Extended Named ACLs

Follow the procedure given below to create an extended ACL using names:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip access-list extended name</td>
<td>Defines an extended IPv4 access list using a name, and enter access-list configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ip access-list extended 150</td>
<td>The name can be a number from 100 to 199.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>{deny</td>
<td>permit} protocol {source [source-wildcard]</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-ext-nacl)# permit 0 any any</td>
<td>• host source—A source and source wildcard of source 0.0.0.0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• host destination—A destination and destination wildcard of destination 0.0.0.0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• any—A source and source wildcard or destination and destination wildcard of 0.0.0.0 255.255.255.255.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-ext-nacl)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Device# show running-config</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
<td></td>
</tr>
<tr>
<td>Device# copy running-config</td>
<td></td>
<td></td>
</tr>
<tr>
<td>startup-config</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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**

1. Choose **Configuration > Security > ACL**.
2. Click **Associating Interfaces**.
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.
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:

---

**Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x**
Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>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).</td>
</tr>
<tr>
<td>Example: Device(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip access-group {access-list-number</td>
<td>name} {in</td>
</tr>
<tr>
<td>Example: Device(config-if)# ip access-group 2 in</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>Displays the access list configuration.</td>
</tr>
<tr>
<td>Example: Device# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example: Device# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**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 17: Commands for Displaying Access Lists and Access Groups

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show access-lists [number</td>
<td>Displays the contents of one or all current IP and MAC address access lists or a specific access list (numbered or named).</td>
</tr>
<tr>
<td>name]`</td>
<td></td>
</tr>
<tr>
<td>`show ip access-lists [number</td>
<td>Displays the contents of all current IP access lists or a specific IP access list (numbered or named).</td>
</tr>
<tr>
<td>name]`</td>
<td></td>
</tr>
<tr>
<td><code>show ip interface interface-id</code></td>
<td>Displays detailed configuration and status of an interface. If IP is enabled on the interface and ACLs have been applied by using the <code>ip access-group</code> interface configuration command, the access groups are included in the display.</td>
</tr>
<tr>
<td><code>show running-config [interface interface-id]</code></td>
<td>Displays the contents of the configuration file for the switch or the specified interface, including all configured MAC and IP access lists and which access groups are applied to an interface.</td>
</tr>
<tr>
<td><code>show mac access-group [interface interface-id]</code></td>
<td>Displays MAC access lists applied to all Layer 2 interfaces or the specified Layer 2 interface.</td>
</tr>
</tbody>
</table>

### 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
```
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 10: 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# show 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 eq 23
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 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.
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.

```plaintext
Device(config)# ip access-list standard Internet_filter
Device(config-ext-nacl)# permit 1.2.3.4
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.

```plaintext
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`:

```plaintext
Device(config)# ip access-list extended border-list
Device(config-ext-nacl)# no permit ip host 10.1.1.3 any
```
DNS-Based Access Control Lists

- Information About DNS-Based Access Control Lists, on page 563
- Restrictions on DNS-Based Access Control Lists, on page 564
- Flex Mode, on page 564
- Local Mode, on page 567
- Viewing DNS-Based Access Control Lists, on page 570
- Configuration Examples for DNS-Based Access Control Lists, on page 571
- Verifying DNS Snoop Agent (DSA), on page 572
- Information About Flex Client IPv6 Support with WebAuth Pre and Post ACL, on page 573
- Enabling Pre-Authentication ACL for LWA and EWA, on page 574
- Enabling Post-Authentication ACL for LWA and EWA, on page 576
- Enabling DNS ACL for LWA and EWA, on page 576
- Verifying Flex Client IPv6 Support with WebAuth Pre and Post ACL, on page 577

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). 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-auth or post-auth, 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.

**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.

**Flex Mode**

**Defining URL Filter List**

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>urlfilter list list-name</td>
<td>Configures the URL filter list. Here, list-name refers to the URL filter list name. The list name must not exceed 32 alphanumeric characters.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# urlfilter list urllist_flex_preauth</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>action permit</td>
<td>Configures the action: permit (Whitelist) or deny (Blacklist).</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-urlfilter-params)# action permit</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>redirect-server-ip4 IPv4-address</td>
<td>Configures the IPv4 redirect server for the URL list. Here, IPv4-address refers to the IPv4 address.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-urlfilter-params)# redirect-server-ip4 8.8.8.8</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>redirect-server-ip6 IPv6-address</td>
<td>Configures the IPv6 redirect server for the URL list. Here, IPv6-address refers to the IPv6 address.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-urlfilter-params)# redirect-server-ip6 2001:300::8::81</td>
<td></td>
</tr>
</tbody>
</table>
Applying URL Filter List to Flex Profile

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wireless profile flex default-flex-profile</code></td>
<td>Creates a new flex policy. The default flex profile name is <code>default-flex-profile</code>.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# wireless profile flex default-flex-profile</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>acl-policy acl policy name</code></td>
<td>Configures ACL policy.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-wireless-flex-profile)# acl-policy acl_name</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>urlfilter list name</code></td>
<td>Applies the URL list to the Flex profile.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-wireless-flex-profile-acl)# urlfilter list urllist_flex_preauth</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-wireless-flex-profile-acl)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

Configuring ISE for Central Web Authentication (GUI)

Perform the following steps to configure ISE for Central Web Authentication.
Configuring 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 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-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
   sessionId=SessionIdValue&portal=0ce17ad0-6d90-11e5-978e-005056bf2f0a&daysToExpire=value&action=cwa
Step 10 Verify contents in the Attributes Details section and click Save.
Local Mode

Defining URL Filter List

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> urlfilter list <em>list-name</em></td>
<td>Configures the URL filter list.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# urlfilter list</td>
<td></td>
</tr>
<tr>
<td>urllist_local_preauth</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> action permit</td>
<td>Configures the action: permit (Whitelist) or deny (Blacklist).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-urlfilter-params)# action</td>
<td></td>
</tr>
<tr>
<td>permit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> filter-type post-authentication</td>
<td>This step is applicable while configuring post-authentication URL filter only.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-urlfilter-params)# filter-type post-authentication</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> redirect-server-ip4 <em>IPv4-address</em></td>
<td>Configures the IPv4 redirect server for the URL list. Here, <em>IPv4-address</em> refers to the IPv4 address.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-urlfilter-params)# redirect-server-ip4</td>
<td></td>
</tr>
<tr>
<td>9.1.0.101</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> redirect-server-ip6 <em>IPv6-address</em></td>
<td>Configures the IPv6 redirect server for the URL list. Here, <em>IPv6-address</em> refers to the IPv6 address.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 10** Verify contents in the Attributes Details section and click Save.
Applying URL Filter List to Policy Profile

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>wireless profile policy profile-policy</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config)# wireless profile policy default-policy-profile</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**urlfilter list {pre-auth-filter name</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>end</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# end</td>
</tr>
</tbody>
</table>
Configuring ISE for Central Web Authentication

Creating Authorization Profiles

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Login to the Cisco Identity Services Engine (ISE).</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Policy, and click Policy Elements.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Results.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Expand Authorization, and click Authorization Profiles.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Add to create a new authorization profile for URL filter.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Name field, enter a name for the profile. For example, CentralWebauth.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Choose ACCESS_ACCEPT from the Access Type drop-down list.</td>
</tr>
<tr>
<td>Step 8</td>
<td>In the Advanced Attributes Setting section, choose Cisco:cisco-av-pair from the drop-down list.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Enter the following one by one and click (+) icon after each of them:</td>
</tr>
<tr>
<td></td>
<td>• url-filter-preauth=&lt;preauth_filter_name&gt;</td>
</tr>
<tr>
<td></td>
<td>• url-filter-postauth=&lt;postauth_filter_name&gt;</td>
</tr>
<tr>
<td></td>
<td>For example,</td>
</tr>
</tbody>
</table>
|        | 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Policy &gt; Authentication page, click Authentication.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter a name for your authentication rule. For example, MAB.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the If condition field, select the plus (+) icon.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose Compound condition, and choose WLC_Web_Authentication.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click the arrow located next to and ... in order to expand the rule further.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click the + icon in the Identity Source field, and choose Internal endpoints.</td>
</tr>
<tr>
<td>Step 7</td>
<td>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.</td>
</tr>
</tbody>
</table>
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:
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 IP cache address, 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 AP.

ACL definitions are pushed to AP in the following events:

- AP join.
- New ACL mapping in flex profile.
- When default External WebAuth (EWA) security ACL is pushed.
- Configuring IPv6 ACL definition in Flex profile.

---

**Note**

All the custom ACLs must be mapped in Flex profile. Only the custom ACL definitions will be pushed to AP apart from the generated default ACLs.

Custom pre-authentication ACL is mapped under WLAN profile. Whereas, custom post-authentication ACL is mapped under default policy profile. All post-authentication ACL is configured under default 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 to AP.
- Intercept ACL—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.
- AP does DNS snooping and sends the IPv4 and IPv6 addresses to the controller.
- Controller stores the snooped IPs from AP in a database and sends the message during AP-to-AP intra wncd roam.

Supported IPv6 Features in Flex Mode

Table 18: Supported IPv6 Features in Flex Mode

<table>
<thead>
<tr>
<th>Feature Parity Support</th>
<th>Feature</th>
<th>Flex Mode IPv6 Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Flex client IPv6 learning</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Pre auth IPv6 ACL</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Post auth IPv6 ACL</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Pre auth DNS ACL</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Post auth DNS ACL</td>
<td></td>
</tr>
</tbody>
</table>

Enabling Pre-Authentication ACL for LWA and EWA

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wlan wlan-name wlan-id SSID-name</td>
<td>Enters the WLAN configuration sub-mode.</td>
</tr>
<tr>
<td>Example: Device(config)# wlan wlan-demo 1 ssid-demo</td>
<td>• wlan-name—Enter the profile name. The range is from 1 to 32 alphanumeric characters.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <code>wlan-id</code>—Enter the WLAN ID. The range is from 1 to 512.</td>
</tr>
<tr>
<td>• <code>SSID-name</code>—Enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.</td>
</tr>
</tbody>
</table>

**Note** If you have already configured WLAN, enter `wlan wlan-name` command.

<table>
<thead>
<tr>
<th>Step 3</th>
<th><code>ipv6 traffic-filter web acl_name-preauth</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-wlan)# ipv6 traffic-filter web preauth_v6_acl</code></td>
</tr>
<tr>
<td>Creates a pre-authentication ACL for web authentication.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th><code>no security wpa</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-wlan)# no security wpa</code></td>
</tr>
<tr>
<td>Disables the WPA security.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th><code>no security wpa wpa2 ciphers aes</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-wlan)# no security wpa wpa2 ciphers aes</code></td>
</tr>
<tr>
<td>Disables WPA2 ciphers for AES.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th><code>no security wpa akm dot1x</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-wlan)# no security wpa akm dot1x</code></td>
</tr>
<tr>
<td>Disables security AKM for dot1x.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th><code>security dot1x authentication-list auth-list-name</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-wlan)# security dot1x authentication-list default</code></td>
</tr>
<tr>
<td>Enables security authentication list for dot1x security.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th><code>security web-auth authentication-list authenticate-list-name</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-wlan)# security web-auth authentication-list wcm_dot1x</code></td>
</tr>
<tr>
<td>Enables authentication list for WLAN.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th><code>security web-auth parameter-map parameter-map-name</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-wlan)# security web-auth parameter-map param-custom-webconsent</code></td>
</tr>
<tr>
<td>Maps the parameter map.</td>
<td></td>
</tr>
</tbody>
</table>
Enabling Post-Authentication ACL for LWA and EWA

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>wireless profile policy <em>profile-name</em></td>
<td>Creates policy profile for the WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless profile policy test1</td>
<td>The <em>profile-name</em> is the profile name of the</td>
</tr>
<tr>
<td></td>
<td>policy profile.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>ipv6 acl <em>acl_name</em></td>
<td>Creates a named WLAN ACL.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# ipv6 acl testacl</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# end</td>
<td>Alternatively, you can also press Ctrl-Z to</td>
</tr>
<tr>
<td></td>
<td>exit global configuration mode.</td>
</tr>
</tbody>
</table>

Enabling DNS ACL for LWA and EWA

Note

Post-authentication DNS ACL is not supported.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless profile policy <em>profile-name</em></td>
<td>Creates policy profile for the WLAN. The <em>profile-name</em> is the profile name of the policy profile.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wireless profile policy test1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### 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
```

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>AP Name</th>
<th>WLAN State</th>
<th>Protocol Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>1491.82b8.f8c1</td>
<td>AP4001.7A03.544C</td>
<td>Webauth Pending</td>
<td>11n(5) None</td>
</tr>
</tbody>
</table>

Local

Number of Excluded Clients: 0

To verify the IP state, discovery, and MAC, use the following command:

```
Device# show wireless dev da ip
```

<table>
<thead>
<tr>
<th>IP</th>
<th>STATE</th>
<th>DISCOVERY</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.30.0.4</td>
<td>Reachable</td>
<td>ARP</td>
<td>1491.82b8.f8c1</td>
</tr>
<tr>
<td>2001:15:30:0:d1d7:ecf3:7940:af60</td>
<td>Reachable</td>
<td>IPv6 Packet</td>
<td>1491.82b8.f8c1</td>
</tr>
<tr>
<td>fe80::595e:7c29:d7c:3c84</td>
<td>Reachable</td>
<td>IPv6 Packet</td>
<td>1491.82b8.f8c1</td>
</tr>
</tbody>
</table>
Verifying Flex Client IPv6 Support with WebAuth Pre and Post ACL
Whitelisting of Specific URLs

This feature helps you to whitelist specific URLs 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 whitelist URLs for web authentication of captive portal and walled garden. Authentication is not required to access the whitelisted URLs. When you try to access sites that are not whitelisted, you are redirected to the Login page.

Configuring URL Whitelisting

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>urlfilter list <code>&lt;urlfilter-name&gt;</code></td>
<td>Configures the URLfilter profile.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# urlfilter list</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>url-whitelist-nbn</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>action [deny</td>
<td>permit]</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-urlfilter-params)#action</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>permit</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>(redirect-server-ipv4</td>
<td>redirect-server-ipv6)</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
Purpose

Command or Action

Device(config-urlfilter-params)#redirect-server-ipv4
X.X.X.X

Step 5

url url-to-be-whitelisted

Example:

Device(config-urlfilter-params)#url www.cisco.com

Whitelist the URL.

You can associate the whitelisted URL with the ACL policy in flex profile.

Note

You must name acl-policy as preauth_v4, otherwise it will not be applied on the AP.

Example

Associating the whitelisted URL with the ACL policy in flex profile:

Device(config)#wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy preauth_v4
Device(config-wireless-flex-profile-acl)# urlfilter list url_white_list_nbn
Device(config-wireless-flex-profile-acl)# exit
Device(config-wireless-flex-profile)# description "default flex profile"

Verifying URL Whitelisting on the Controller

To verify the summary and the details of the URL whitelisting on the controller, 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-white_list 1 PRE-AUTH PERMIT 1.1.1.1

Device#

Device#show wireless urlfilter details url-white_list
List Name................ : url-white_list
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
Configuring Policy Enforcement and Usage Monitoring

You can enforce dynamic QoS policies and upstream and downstream TCP or UDP data rates on 802.11 clients seamlessly without disrupting the client’s ongoing sessions. The feature ensures that clients do not have to get dissociated from the network. All the authentication methods: 802.1X, PSK, web authentication, and so on, are supported.

The APs periodically send client statistics including bandwidth usage to the Controller. The AAA server receives Accounting-Interim messages which include the clients data utilization at the configured intervals. The AAA server accumulates information about data consumption for each client and when the client exhausts the data limit, the AAA server sends a change-of-authorization (CoA) message to the Controllers. Upon successful CoA handshakes, the Controllers apply and send new policies to the APs.

Restrictions on Policy Enforcement and Usage Monitoring

- Only FlexConnect local switching mode is supported.

Configuring Policy Enforcement and Usage Monitoring (CLI)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Example: Configuring Policy Enforcement and Usage Monitoring

Policy enforcement and usage monitoring is applied on a group where a class-map is created for QOS policies. This is done via CoA.

Given below is a sample configuration for policy enforcement and usage monitoring:

```plaintext
aaa new-model
  radius server radius_free
  address ipv4 10.0.0.1 auth-port 1812 acct-port 1813
  key cisco123
  exit
  radius server radius_free
  exit
  aaa new-model
  aaa server radius dynamic-author
  client 10.0.0.1 server-key cisco123
  aaa new-model
  aaa group server radius rad_eap
  server name radius_free
  exit
  aaa new-model
  dot1x system-auth-control
  aaa authentication dot1x eap_methods group rad_eap
  dot1x system-auth-control
  class-map client_dscp_clsmapout
  match dscp af13
  exit
  class-map client_dscp_clsmapin
  match dscp af13
  exit
  policy-map qos_new
  class client_dscp_clsmapout
  police 512000 conform-action transmit exceed-action drop
  policy-map qos_nbn
  class client_dscp_clsmapin
  police 16000000 conform-action transmit exceed-action drop
  wlan test1 3 test2
  broadcast-ssid
```

---

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa server radius dynamic-author</td>
<td>Creates a local server RADIUS profile in the controller.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# aaa server radius dynamic-author</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>client client-ip-addr server-key key</td>
<td>Configures a server key for a RADIUS client.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-locsvr-da-radius)# client 3.2.4.3 server-key testpwd</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[Optional] show aaa command handler</td>
<td>Displays the AAA CoA packet statistics.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device#show aaa command handler</td>
<td></td>
</tr>
</tbody>
</table>
Verifying Policy Usage and Enforcement

To view the detailed information about the policies applied to a specific client, use the following command:

Device# show wireless client mac-address mac-address detail

To view client-level mobility statistics, use the following command:

Device# show wireless client mac-address mac-address mobility statistics

To view client-level roaming history for an active client in a sub-domain, use the following command:

Device# show wireless client mac-address mac-address mobility history

To view detailed parameters of a given profile policy, use the following command:

Device# show wireless profile policy detailed policy-name
Verifying Policy Usage and Enforcement
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 585
- How to Configure Local Web Authentication, on page 591
- Information About Management over Wireless, on page 607
- Configuration Examples for Local Web Authentication, on page 608

Local Web Authentication Overview

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.

Note

You can configure web-based authentication on Layer 2 and Layer 3 interfaces.

When you initiate 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.
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’.

Based on where the web pages are hosted, the local web authenction can be categorozied 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-passsthrough**—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.

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.

**Device Roles**

With local web authentication, the devices in the network have these specific roles:

- **Client**—The device (workstation) that requests access to the LAN and the services and responds to requests from the switch. 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 switch that the client is authorized to access the LAN and the switch services or that the client is denied.

- **Switch**—Controls the physical access to the network based on the authentication status of the client. The switch 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.
Authentication Process

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 switch sends the login page to the user. The user enters a username and password, and the switch sends the entries to the authentication server.

- If the authentication succeeds, the switch 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 switch sends the login fail page. The user retries the login. If the maximum number of attempts fails, the switch 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 the authentication server does not respond to the switch, and if an AAA fail policy is configured, the switch applies the failure access policy to the host. The login success page is sent to the user.

- The switch reauthenticatees 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.

- The feature applies the downloaded timeout or the locally configured session timeout.

Note

Beginning with Cisco IOS XE Denali 16.1.1 and later, the default session timeout value for local web authentication on WLC is 1800 seconds. The default session timeout value was infinite seconds, prior to Cisco IOS XE Denali 16.1.1.

- If the terminate action is RADIUS, the feature sends a nonresponsive host (NRH) request to the server. The terminate action is included in the response from the server.

- If the terminate action is default, the session is dismantled, and the applied policy is removed.

Local Web Authentication Banner

With Web Authentication, you can create a default and customized web-browser banners that appears when you log in to a switch.
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 in the new-style (Session-aware) CLI mode as follows:

- New-style mode—Use the following global configuration command:

  ```
  parameter-map type webauth global
  banner text <text>
  ```

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 12: 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
    ```
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.
Customized Local Web Authentication

During the local web authentication process, the switch 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.

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 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 stack master or a member).
- You must configure all four pages.
- The banner page has no effect if it is configured with the web page.
- 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 must be 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.
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 local web authentication configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
### Configuring AAA Authentication (GUI)

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>Choose Configuration &gt; Security &gt; AAA.</strong></td>
<td>Enables AAA functionality.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the <strong>Authentication</strong> section, click <strong>Add</strong>.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Quick Setup: AAA Authentication</strong> window that is displayed, enter a name for your method list.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose the type of authentication you want to perform before allowing access to the network, in the <strong>Type</strong> drop-down list.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>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 <strong>Group</strong> Type drop-down list.</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>To configure a local server to act as a fallback method when servers in the group are unavailable, check the <strong>Fallback</strong> to local check box.</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>Choose the server groups you want to use to authenticate access to your network, from the <strong>Available Server Groups</strong> list and click &gt; icon to move them to the <strong>Assigned Server Groups</strong> list.</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>Click <strong>Save &amp; Apply to Device</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring AAA Authentication (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th><strong>aaa new-model</strong></th>
<th>Enables AAA functionality.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# aaa new-model</code></td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS server</td>
<td>• None specified</td>
</tr>
<tr>
<td>• IP address</td>
<td></td>
</tr>
<tr>
<td>• UDP authentication port</td>
<td></td>
</tr>
<tr>
<td>• Key</td>
<td></td>
</tr>
<tr>
<td>Default value of inactivity timeout</td>
<td>3600 seconds</td>
</tr>
<tr>
<td>Inactivity timeout</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
### Command or Action

| Step 2 | ```aaa authentication login {default | named_authentication_list} group AAA_group_name``` | Defines the list of authentication methods at login.  
**Example:**  
```
Device(config)# aaa authentication login default group group1
```

| Step 3 | ```aaa authorization network {default | named} group AAA_group_name``` | Creates an authorization method list for web-based authorization.  
**Example:**  
```
Device(config)# aaa authorization network default group group1
```

| Step 4 | ```tacacs server server-name``` | Specifies an AAA server.  
**Example:**  
```
Device(config)# tacacs server yourserver
```

| Step 5 | ```address {ipv4 | ipv6} ip_address``` | Configures the IP address for the TACACS server.  
**Example:**  
```
Device(config-server-tacacs)# address ipv4 10.0.1.12
```

| Step 6 | ```tacacs-server host {hostname | ip_address}``` | Specifies a AAA server.  
**Example:**  
```
Device(config)# tacacs-server host 10.1.1.1
```

---

## 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 trust points.

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 pseudo-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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ip http server</td>
<td>Enables the HTTP server. The local web authentication feature uses the HTTP server to</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Creating Parameter Maps

#### Configuring Local Web Authentication (GUI)

**Procedure**

1. **Step 1** Choose **Configuration > Security > Web Auth**.
2. **Step 2** On the **Web Auth** page, click **Add**.
3. **Step 3** In the **Create Web Auth Parameter** window that is displayed, enter a name for the parameter map.
4. **Step 4** In the **Maximum HTTP Connections** field, enter the maximum number of HTTP connections that you want to allow.
5. **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.
6. **Step 6** Choose the type of Web Auth parameter.
7. **Step 7** Click **Apply to Device**.
8. **Step 8** On the **Web Auth** page, click the name of the parameter map.
9. **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.
10. **Step 10** Enter the virtual IP addresses as required.
11. **Step 11** Set appropriate status of **WebAuth Intercept HTTPS**, **Captive Bypass Portal**, and **Watch List Enable**.
Step 12 In the **Watch List Expiry Timeout** field, enter the time in seconds after which the watch list should time out.

Step 13 Set appropriate status for **Disable Success Window**, **Disable Logout Window**, and **Login Auth Bypass for FQDN**.

Step 14 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 15 Click the **Advanced** tab.

Step 16 In the **Redirect for log-in** field, enter the name of the external server to send login request.

Step 17 In the **Redirect On-Success** field, enter the name of the external server to redirect after a successful login.

Step 18 In the **Redirect On-Failure** field, enter the name of the external server to redirect after a login failure.

Step 19 To configure external local web authentication, perform these tasks:
   a) Under **Redirect to External Server** in the **Redirect Append for AP MAC Address** field, enter the AP MAC address.
   b) In the **Redirect Append for Client MAC Address** field, enter the client MAC address.
   c) In the **Redirect Append for WLAN SSID** field, enter the WLAN SSID.
   d) In the **Portal IPV4 Address** field, enter the IPv4 address of the portal to send redirects.
   e) In the **Portal IPV6 Address** field, enter the IPv6 address of the portal to send redirects, if IPv6 address is used.

Step 20 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 21 Click **Update & Apply**.

---

**Configuring the Internal Local Web Authentication (CLI)**

Follow the procedure given below to configure the internal local web authentication:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

| **Step 2**        |         |
| configure terminal | Enters global configuration mode. |
| **Example:**      |         |
Configuring the Customized Local Web Authentication (CLI)

Follow the procedure given below to configure the customized local web authentication:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the webauth type parameter.</td>
</tr>
<tr>
<td>parameter-map type webauth</td>
<td>You need to configure a virtual IP in the global parameter map to use the customized web authentication bundle.</td>
</tr>
<tr>
<td>parameter-map-name</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# parameter-map type webauth sample</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures webauth sub-types, such as passthru, consent, webauth, or webconsent.</td>
</tr>
<tr>
<td>type {authbypass</td>
<td>consent</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-params-parameter-map)# type</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the External Local Web Authentication (CLI)

Follow the procedure given below to configure the external local web authentication:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

- **enable**
  - Example:
    ```
    Device(config)# enable
    ```

- Enter your password if prompted.

---

**Configuring the External Local Web Authentication**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures the customized login page.</td>
</tr>
</tbody>
</table>

- **custom-page login device**
  - **html-filename**
  - Example:
    ```
    Device(config-params-parameter-map)# custom-page login device bootflash:login.html
    ```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td>Configures the customized login expiry page.</td>
</tr>
</tbody>
</table>

- **custom-page login expired device**
  - **html-filename**
  - Example:
    ```
    Device(config-params-parameter-map)# custom-page login expired device bootflash:loginexpired.html
    ```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td>Configures the customized login success page.</td>
</tr>
</tbody>
</table>

- **custom-page success device**
  - **html-filename**
  - Example:
    ```
    Device(config-params-parameter-map)# custom-page success device bootflash:loginsuccess.html
    ```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong></td>
<td>Configures the customized login failure page.</td>
</tr>
</tbody>
</table>

- **custom-page failure device**
  - **html-filename**
  - Example:
    ```
    Device(config-params-parameter-map)# custom-page failure device bootflash:loginfail.html
    ```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 9</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

- **end**
  - Example:
    ```
    Device(config)# end
    ```
### Configuring the External Local Web Authentication (CLI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Device&gt; enable</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>parameter-map type webauth</td>
<td>Configures the webauth type parameter.</td>
</tr>
<tr>
<td></td>
<td>parameter-map-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# parameter-map type webauth sample</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>type {authbypass</td>
<td>consent</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-params-parameter-map)# type webauth</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>redirect [for-login</td>
<td>on-failure</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-params-parameter-map)# redirect for-login <a href="http://9.1.0.100/login.html">http://9.1.0.100/login.html</a></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>redirect portal {ipv4</td>
<td>ipv6} ip-address</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-params-parameter-map)# redirect portal ipv4 23.0.0.1</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
# 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>wlan profile-name wlan-id ssid-name</code></td>
<td>Specifies the WLAN name and ID.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# wlan mywlan 34 mywlan-ssid</code></td>
<td><code>profile-name</code> is the WLAN name which can contain 32 alphanumeric characters. <code>wlan-id</code> is the wireless LAN identifier. The valid range is from 1 to 512. <code>ssid-name</code> is the SSID which can contain 32 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>no security wpa</code></td>
<td>Disables the WPA security.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-wlan)# no security wpa</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>`security web-auth {authentication-list authentication-list-name</td>
<td>parameter-map parameter-map-name}`</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-wlan)# security web-auth authentication-list webauthlistlocal</code></td>
<td>Here,</td>
</tr>
<tr>
<td></td>
<td><code>Device(config-wlan)# security web-auth parameter-map sample</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>authentication-list authentication-list-name</code>: Sets the authentication list for IEEE 802.1x.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>parameter-map parameter-map-name</code>: Configures the parameter map.</td>
</tr>
</tbody>
</table>
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 Preauthentication 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Step 2** configure terminal  
**Example:**  
Device# configure terminal | Enters global configuration mode. |
| **Step 3** access-list access-list-number {deny | permit} source source-wildcard-bits  
**Example:**  
Device(config)# access-list 2 deny your_host | 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 4** 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 5** 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. |
Configuring the Maximum Web Authentication Request Retries

Follow these steps to configure the maximum web authentication request retries:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Configure terminal</td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>number is the maximum number of web auth request retries. The valid range is 0 to 20.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>wireless security web-auth retries number</td>
</tr>
<tr>
<td>Device(config)# wireless security web-auth retries 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>end</td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

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.
Configuring a Local Banner in Web Authentication Page (CLI)

Follow the procedure given below to configure a local banner in web authentication pages.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ip admission auth-proxy-banner http</td>
<td>Enables the local banner.</td>
</tr>
<tr>
<td></td>
<td>[banner-text</td>
<td>file-path]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip admission</td>
<td></td>
</tr>
<tr>
<td></td>
<td>auth-proxy-banner http</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C My Switch C</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Webpasssthrough

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device # configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> parameter-map type webauth parameter-map name</td>
<td>Configures the webauth type parameter.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device (config) # parameter-map type webauth webparalocal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> type consent</td>
<td>Configures webauth type as consent.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device (config-params-parameter-map) # type consent</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device (config-params-parameter-map) # end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>Displays the configuration details.</td>
</tr>
<tr>
<td></td>
<td>section parameter-map type webauth parameter-map</td>
</tr>
<tr>
<td><strong>Example:</strong> Device (config) # show running-config</td>
<td></td>
</tr>
<tr>
<td></td>
<td>section parameter-map type webauth test</td>
</tr>
</tbody>
</table>

Configuring Preauthentication ACL

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
## Configuring TrustPoint for Local Web Authentication

### Before you begin

Ensure that a certificate is installed on your controller.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> parameter-map type webauth global</td>
<td>Creates the parameter map.</td>
</tr>
</tbody>
</table>

---

### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> wlan wlan-name</td>
<td>For wlan-name, enter the profile name.</td>
</tr>
<tr>
<td><strong>Step 3</strong> shutdown</td>
<td>Disables the WLAN.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip access-group web preauthrule</td>
<td>Configures ACL that has to be applied before authentication.</td>
</tr>
<tr>
<td><strong>Step 5</strong> no shutdown</td>
<td>Enables the WLAN.</td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> show wlan name wlan-name</td>
<td>Displays the configuration details.</td>
</tr>
</tbody>
</table>
### Information About Management over Wireless

The management over wireless feature allows you to monitor and configure local controllers using a wireless client. You can perform all the management tasks except uploads to and downloads from (transfers to and from) the controller.

**Restrictions on Management over Wireless**

- Management over wireless can be disabled only if clients are on central switching.

### Configuring Management over Wireless (GUI)

**Procedure**

1. Choose **Configuration > Wireless > Wireless Global**.
2. Check the **Management Via Wireless** check box to enable the feature.
3. Click **Apply**.

### Configuring Management over Wireless (CLI)

**Procedure**

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

| **Step 3**             |                                              |
| `trustpoint trustpoint-name` | Configures trustpoint for local web authentication. |
| **Example:**            |                                              |
| `Device (config-params-parameter-map)# trustpoint trustpoint-name` |

| **Step 4**             |                                              |
| `end`                  | Returns to privileged EXEC mode.             |
| **Example:**            |                                              |
| `Device (config-params-parameter-map)# end` |
### 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
```
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
c=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:
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
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 1.1.1.1
```
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 1:1:1::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://9:1:1::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
class parameter-map type webauth
    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:loginsuccess.html
Device(config-params-parameter-map)# end
```

```
Device# show running-config | section parameter-map type webauth test
class parameter-map type webauth
    type webauth
    redirect for-login http://9.1.0.100/login.html
    redirect portal ipv4 9.1.0.100
```

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x
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 webparamlocal
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
```
Central Web Authentication

- Information About Central Web Authentication, on page 613
- How to Configure ISE, on page 613
- How to Configure Central Web Authentication on a Network Device, on page 616
- Authentication for Sleeping Clients, on page 623
- Sleeping Clients with Multiple Authentications, on page 625

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.

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.

Prerequisites for Central Web Authentication

You must be aware of the following:

- 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Click <strong>Policy &gt; Authorization</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Rule Name field, enter a name. For example: <em>Mac not known</em>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Conditions field, click the plus (+) icon.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose <strong>Compound Conditions</strong>, and choose <strong>Wireless_MAB</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>From the settings icon, select <strong>Add Attribute/Value</strong> from the options.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Description field, choose <strong>Network Access &gt; AuthenticationStatus</strong> as the attribute from the drop-down list.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Choose the <strong>Equals</strong> operator.</td>
</tr>
<tr>
<td>Step 8</td>
<td>From the right-hand field, choose <strong>UnknownUser</strong>.</td>
</tr>
<tr>
<td>Step 9</td>
<td>In the Permissions field, choose the authorization profile name that you had created earlier.</td>
</tr>
</tbody>
</table>

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.                         |
| Step 12 | The new rule must come before the **MAC not known** rule.                                      |
| Step 13 | From the settings icon, select **Add Attribute/Value** from the options.                       |
| Step 14 | In the Description field, choose **Network Access > UseCase** as the attribute from the drop-down list. |
| Step 15 | Choose the **Equals** operator.                                                                |
| Step 16 | From the right-hand field, choose **GuestFlow**.                                               |
|        | 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 a Network Device

To configure central web authentication on a network device, proceed as follows:

1. Configure WLAN.
2. Configure policy profile.
3. Configure redirect ACL.
5. Configure redirect ACL in Flex profile.

Configuring WLAN (GUI)

**Note**
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 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 General tab to configure the following parameters.

- In the Profile Name field, enter the name of the profile
- In the SSID field, enter the SSID name
  - The SSID name can be alphanumeric up to 32 characters in length.
- In the WLAN ID field, enter the ID number.
  - The valid range is between 1 and 512.
- From the Radio Policy drop-down list, choose the 802.11 radio band.
- Set the Broadcast SSID field, toggle between Enabled or Disabled status.
- Set the Status field, toggle between Enabled or Disabled status.

**Step 4** Click the Security tab, click Layer 2 tab to configure the following parameters.

- Layer 2 Security Mode: Choose None from the drop-down list. This setting disables Layer 2 security.
- MAC Filtering: Check the checkbox to enable MAC Filtering in the WLAN.
**Step 5**  
Click Save & Apply to Device.

---

## Configuring WLAN (CLI)

You need to enable MAC filtering for Layer 2 authentication to download the redirect URL and ACL.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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 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.
    - **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 3**
  - `mac-filtering [name]`
  - **Example:**
    - Device(config-wlan)# mac-filtering name | Enables MAC filtering on a WLAN by default.
    - **Note** While configuring mac-filtering the default authentication list is considered, if the authentication list is not configured earlier. |
| **Step 4**
  - `no security wpa`
  - **Example:**
    - Device(config-wlan)# no security wpa | Disable WPA security. |
| **Step 5**
  - `no shutdown`
  - **Example:**
    - Device(config-wlan)# no shutdown | Shutdown the WLAN. |
| **Step 6**
  - `end`
  - **Example:**
    - Device(config)# end | Returns to privileged EXEC mode.
    - Alternatively, you can also press Ctrl-Z to exit the global configuration mode. |
Example

```plaintext
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>wireless profile policy default-policy-profile</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config)# wireless profile policy default-policy-profile</td>
<td>Configures the default policy profile.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>vlan vlan-id</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# vlan 41</td>
<td>Maps the VLAN to a specific 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.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>aaa-override</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# aaa-override</td>
<td>Configures AAA override to apply policies coming from the AAA or ISE servers.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>nac</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# nac</td>
<td>Configures NAC in the policy profile.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>no shutdown</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# no shutdown</td>
<td>Shutdown the WLAN.</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

Step 6  
**end**

**Example:**

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

**Purpose**

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

---

### 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**  
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**
- **Central Authentication**
- **Central DHCP**
- **Central Association Enable**
- **Flex NAT/PAT**

**Step 9**  
Click **Save & Apply to Device**.
## Creating Redirect ACL

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ip access-list extended redirect</td>
<td>The HTTP and HTTPS browsing does not work without authentication (per the other ACL) as ISE is configured to use a redirect ACL (named redirect).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip access-list extended redirect</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>deny ip any host ISE-IP-add</td>
<td>Allows traffic to ISE and all other traffic is blocked.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# deny ip any host 123.123.134.112</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>deny ip host ISE-IP-add any</td>
<td>Allows traffic to ISE and all other traffic is blocked.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# deny ip host 123.123.134.112 any</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>This ACL is applicable for both local and flex mode.</td>
</tr>
<tr>
<td>5</td>
<td>permit TCP any any eq web address/port-number</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In case of HTTP:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# permit TCP any any eq www</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# permit TCP any any eq 80</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In case of HTTPS:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# permit TCP any any eq 443</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring AAA for Central Web Authentication

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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:  
Device(config-locsvr-da-radius)# client 123.123.134.112 4 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. |

### Example

```
Device# config terminal  
Device(config)# aaa server radius dynamic-author  
Device(config-locsvr-da-radius)# client 123.123.134.112 4 SECRET  
Device(config)# 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.**
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 wireless profile flex default-flex-profile</td>
<td>Creates a new flex policy. The default flex profile name is <code>default-flex-profile</code>.</td>
</tr>
<tr>
<td>Example: Device(config)# wireless profile flex default-flex-profile</td>
<td></td>
</tr>
<tr>
<td>Step 3 acl-policy acl policy name</td>
<td>Configures ACL policy.</td>
</tr>
<tr>
<td>Example: Device(config-wireless-flex-profile)# acl-policy acl1</td>
<td></td>
</tr>
<tr>
<td>Step 4 central-webauth</td>
<td>Configures central web authentication.</td>
</tr>
<tr>
<td>Example: Device(config-wireless-flex-profile-acl)# central-webauth</td>
<td></td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit the global configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
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 the sleeping clients are to be remembered for before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes, with the default being 720 minutes. You can configure the duration on WebAuth parameter map that is mapped to a WLAN. 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 controllers in a mobility group. A client that is associated with one controller goes to sleep and then wakes up and gets associated with the other controller.
- Suppose there are three controllers in a mobility group. A client that is associated with the second controller that is anchored to the first controller goes to sleep, wakes up, and gets associated with the third controller.
- A client sleeps, wakes up and gets associated with the same or different export foreign controller that is anchored to the export anchor.

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-WLAN 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> [no] parameter-map type webauth {parameter-map-name</td>
<td>global}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# parameter-map type webauth global</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> sleeping-client [timeout time]</td>
<td>Configures the sleeping client timeout to 100 minutes. Valid range is between 10 minutes and 43200 minutes.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-params-parameter-map)# sleeping-client timeout 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits parameter-map webauth configuration mode and returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Note If you do not use the timeout keyword, the sleeping client is configured with the default timeout value of 720 minutes.
### Sleeping Clients with Multiple Authentications

#### Mobility Support for Sleeping Clients

From release 17.1.1 onwards, there is mobility support for guest and non-guest sleeping clients.

#### Supported Combinations of Multiple Authentications

Multiple authentication feature supports sleeping clients configured in the WLAN profile.

The following table outlines the supported combination of multiple authentications:

<table>
<thead>
<tr>
<th>Layer 2</th>
<th>Layer 3</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAB</td>
<td>LWA</td>
<td>Yes</td>
</tr>
<tr>
<td>MAB Failure</td>
<td>LWA</td>
<td>Yes</td>
</tr>
<tr>
<td>Dot1x</td>
<td>LWA</td>
<td>Yes</td>
</tr>
<tr>
<td>PSK</td>
<td>LWA</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Configuring Sleeping Clients with Multiple Authentications

#### Configuring WLAN for Dot1x and Local Web Authentication

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>wlan profile-name wlan-id SSID name</td>
<td>Enters WLAN configuration sub-mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wlan wlan-test 3 ssid-test</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>profile-name</strong> - Is the profile name of the configured WLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>wlan-id</strong> - Is the wireless LAN identifier. Range is from 1 to 512.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SSID_Name</strong> - Is the SSID which can contain 32 alphanumeric characters.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>security dot1x authentication-list auth-list-name</td>
<td>Enables security authentication list for dot1x security. The configuration is similar for all dot1x security WLANs.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# security dot1x authentication-list default</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>security web-auth authentication-list authenticate-list-name</td>
<td>Enables authentication list for dot1x security.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# security web-auth authentication-list default</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>security web-auth parameter-map parameter-map-name</td>
<td>Maps the parameter map.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# security web-auth parameter-map global</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>no shutdown</td>
<td>Enables WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring WLAN for MAC Authentication Bypass and Local Web Authentication

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>wlan profile-name wlan-id SSID_name</code></td>
<td>Enters WLAN configuration sub-mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# <code>wlan wlan-test 3 ssid-test</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>mac-filtering list-name</code></td>
<td>Sets the MAC filtering parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# <code>mac-filtering cat-radius</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>no security wpa akm dot1x</code></td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# <code>no security wpa akm dot1x</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>no security wpa wpa2 ciphers aes</code></td>
<td>Disables the WPA2 cipher.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# <code>no security wpa wpa2 ciphers aes</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>security web-auth parameter-map parameter-map-name</code></td>
<td>Maps the parameter map.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# <code>security web-auth parameter-map global</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>no shutdown</code></td>
<td>Enables WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# <code>no shutdown</code></td>
<td></td>
</tr>
</tbody>
</table>
## Configuring WLAN for Local Web Authentication and MAC Filtering

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code>&lt;br&gt;<code>Example:</code>&lt;br&gt;Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>wlan profile-name wlan-id SSID_name</code>&lt;br&gt;<code>Example:</code>&lt;br&gt;Device(config)# wlan wlan-test 3 ssid-test</td>
<td>Enters WLAN configuration sub-mode.&lt;br&gt;- <code>profile-name</code> - Is the profile name of the configured WLAN.&lt;br&gt;- <code>wlan-id</code> - Is the wireless LAN identifier. Range is from 1 to 512.&lt;br&gt;- <code>SSID_Name</code> - Is the SSID which can contain 32 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>mac-filtering list-name</code>&lt;br&gt;<code>Example:</code>&lt;br&gt;Device(config-wlan)# mac-filtering cat-radius</td>
<td>Sets the MAC filtering parameters.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>no security wpa akm dot1x</code>&lt;br&gt;<code>Example:</code>&lt;br&gt;Device(config-wlan)# no security wpa akm dot1x</td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>no security wpa wpa2 ciphers aes</code>&lt;br&gt;<code>Example:</code>&lt;br&gt;Device(config-wlan)# no security wpa wpa2 ciphers aes</td>
<td>Disables the WPA2 cipher.&lt;br&gt;<code>aes</code>—Encryption type that specifies WPA/AES support.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>security web-auth on-macfilter-failure</code>&lt;br&gt;<code>Example:</code>&lt;br&gt;Device(config-wlan)# security web-auth on-macfilter-failure wlan-id</td>
<td>Configures the fallback policy with MAC Filtering and Web Authentication.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>security web-auth parameter-map parameter-map-name</code>&lt;br&gt;<code>Example:</code>&lt;br&gt;Device(config-wlan)# security web-auth parameter-map global</td>
<td>Maps the parameter map.&lt;br&gt;Note: If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.</td>
</tr>
</tbody>
</table>
### Configuring a PSK + LWA in a WLAN

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>wlan profile-name wlan-id SSID_name</td>
<td>Enters WLAN configuration sub-mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wlan wlan-test 3 ssid-test</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>no security wpa akm dot1x</td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# no security wpa akm dot1x</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>security web-auth</td>
<td>Enables web authentication for a WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# security web-auth</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>no security wpa wpa2 ciphers aes</td>
<td>Disables the WPA2 cipher.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# no security wpa wpa2 ciphers aes</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>security wpa psk set-key ascii</td>
<td>Configures the pre-shared key on a WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# security wpa psk set-key ascii 0 1234567</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Sleeping Clients

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> parameter-map type webauth {parameter-map-name</td>
<td>Creates a parameter map and enters parameter-map webauth configuration mode.</td>
</tr>
<tr>
<td>global}</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# parameter-map type</td>
<td></td>
</tr>
<tr>
<td>webauth MAP-2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> sleeping client [timeout time]</td>
<td>Configures the sleeping client timeout in minutes. Available range for the time argument is from 10 to 43200.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-params-parameter-map)#</td>
<td></td>
</tr>
<tr>
<td>sleeping-client timeout 60</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** If you do not use the timeout keyword, the sleeping client is configured with the default timeout value of 720 minutes.
Verifying Sleeping Clients Configuration

To verify the sleeping clients configuration, use the following command:

Device#show wireless client sleeping-client
Total number of sleeping-client entries: 1

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Remaining time (mm:ss)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2477.031b.aa18</td>
<td>59:56</td>
</tr>
</tbody>
</table>
ISE Simplification and Enhancements

• Utilities for Configuring Security, on page 633
• Configuring Captive Portal Bypassing for Local and Central Web Authentication, on page 635
• Sending DHCP Options 55 and 77 to ISE, on page 637
• Captive Portal, on page 640

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 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 udp any eq bootps any
deny udp 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 1.1.1.1
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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless-default radius server ip key secret</td>
<td>Configures a radius server.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# wireless-default radius server 9.2.58.90 key cisco123</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note You can configure up to ten RADIUS servers.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

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 eq bootpc any
    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 1.1.1.1
    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 aborted, 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Security &gt; Web Auth.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Webauth Parameter Map tab, click the parameter map name. The Edit WebAuth Parameter window is displayed.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Captive Bypass Portal check box.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Update &amp; Apply to Device.</td>
<td></td>
</tr>
</tbody>
</table>

## Configuring Captive Bypassing for WLAN in LWA and CWA (CLI)

**Procedure**

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

**Example:**

```
Device# configure terminal
```

| Step 2 | parameter-map type webauth parameter-map-name | Creates the parameter map. |

---
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Device(config)# parameter-map type webauth WLAN1_MAP</td>
<td>The <code>parameter-map-name</code> must not exceed 99 characters.</td>
</tr>
<tr>
<td><strong>Step 3</strong> captive-bypass-portal</td>
<td>Configures captive bypassing.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# captive-bypass-portal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> wlan profile-name wlan-id ssid-name</td>
<td>Specifies the WLAN name and ID.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wlan WLAN1_NAME 4 WLAN1_NAME</td>
<td>• <code>profile-name</code> is the WLAN name which can contain 32 alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>• <code>wlan-id</code> is the wireless LAN identifier. The valid range is from 1 to 512.</td>
</tr>
<tr>
<td></td>
<td>• <code>ssid-name</code> is the SSID which can contain 32 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>Step 5</strong> security web-auth</td>
<td>Enables the web authentication for the WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wlan)# security web-auth</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> security web-auth parameter-map parameter-map-name</td>
<td>Maps the parameter map.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wlan)# security web-auth parameter-map WLAN1_MAP</td>
<td><strong>Note</strong> If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.</td>
</tr>
<tr>
<td><strong>Step 7</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wlan)# end</td>
<td></td>
</tr>
</tbody>
</table>

**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

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
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1  configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td>Step 2  wireless profile policy profile-policy</td>
<td>Configures WLAN policy profile and enters the wireless policy configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless profile policy rr-xyz-policy-1</td>
</tr>
<tr>
<td>Step 3  dhcp-tlv-caching</td>
<td>Configures DHCP TLV caching on a WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-policy)# dhcp-tlv-caching</td>
</tr>
<tr>
<td>Step 4  radius-profiling</td>
<td>Configures client radius profiling on a WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-policy)# radius-profiling</td>
</tr>
<tr>
<td>Step 5  end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-policy)# end</td>
</tr>
</tbody>
</table>
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** From the Dynamic WEP Key Index drop-down list, select the key index used for dynamic wired equivalent privacy (WEP).

**Step 5** 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 6** 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 7** 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 8** 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 9** 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 10** In the EAP-Broadcast Key Interval field, specify the time interval between rotations of the broadcast encryption key used for clients and click Apply.

---

### Configuring EAP Request Timeout

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless wps client-exclusion dot1x-timeout</td>
<td>Enables exclusion on timeout and no response.</td>
</tr>
<tr>
<td>Example: Device(config)# wireless wps client-exclusion dot1x-timeout</td>
<td>By default, this feature is enabled. To disable, append a no at the beginning of the command.</td>
</tr>
</tbody>
</table>
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

Procedure

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>

Example:

Device(config)# end

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

Example:

Device# configure terminal

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>wlan {profile-name</td>
<td>shutdow} network-name</td>
</tr>
</tbody>
</table>

Example:

Device(config)# wlan edc6 6 edc

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip {access-group</td>
<td>verify} web IPv4-ACL-Name</td>
</tr>
</tbody>
</table>

Note WLAN needs to be disabled before performing this operation.
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-wlan)# ip access-group web CPWebauth</td>
</tr>
<tr>
<td>Step 4</td>
</tr>
<tr>
<td>Example:</td>
</tr>
<tr>
<td>Step 5</td>
</tr>
<tr>
<td>Example:</td>
</tr>
<tr>
<td>Step 6</td>
</tr>
<tr>
<td>Example:</td>
</tr>
<tr>
<td>Step 7</td>
</tr>
<tr>
<td>Example:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Step 8</td>
</tr>
<tr>
<td>Example:</td>
</tr>
</tbody>
</table>

### 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.

### Purpose

- **Disables WPA security.**
- **Disables security AKM for dot1x.**
- **Disables WPA2 ciphers for AES.**
- **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.
  - **parameter-map**
    - `parameter-map-name`: Configures the parameter map.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>exit</td>
<td>Exits from the WLAN configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# exit</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>parameter-map type webauth parameter-map-name</td>
<td>Creates a parameter map and enters parameter-map webauth configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# parameter-map type webauth parMap6</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>parameter-map type webauth parameter-map-name</td>
<td>Creates a parameter map and enters parameter-map webauth configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# parameter-map type webauth parMap6</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>type webauth</td>
<td>Configures the webauth type parameter.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-params-parameter-map)# type webauth</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>timeout init-state sec &lt;timeout-seconds&gt;</td>
<td>Configures the WEBAUTH timeout in seconds. Valid range for the time in sec parameter is 60 seconds to 3932100 seconds.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-params-parameter-map)# timeout init-state sec 3600</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>redirect for-login &lt;URL-String&gt;</td>
<td>Configures the URL string for redirect during login.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-params-parameter-map)# redirect for-login <a href="https://172.16.100.157/portal/login.html">https://172.16.100.157/portal/login.html</a></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>exit</td>
<td>Exits the parameters configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-params-parameter-map)# exit</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>wireless tag policy policy-tag-name</td>
<td>Configures policy tag and enters policy tag configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless tag policy policy_tag_edc6</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>wlan wlan-profile-name policy policy-profile-name</td>
<td>Attaches a policy profile to a WLAN profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-policy-tag)# wlan edc6 policy policy_profile_flex</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

Command or Action | Purpose
--- | ---
**Step 18** 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:

```plaintext
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=cfdbece00-2ce2-11e8-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:

```plaintext
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
```

All WLANs have identical SSIDs.

**Note**

Associating WLANs to different policy tags:

```plaintext
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
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 DNAC, 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.
Configuring 802.1X Security for WLAN with Split Authentication and Authorization Servers

Configuring Explicit Authentication and Authorization Server List (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose <strong>Configuration</strong> &gt; <strong>Security</strong> &gt; <strong>AAA</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>On the <strong>Authentication Authorization and Accounting</strong> page, click the <strong>Servers/Groups</strong> tab.</td>
</tr>
</tbody>
</table>
| **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 (CLI)

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>radius server server-name</code></td>
<td>Specifies the RADIUS server name.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# radius server free-radius-authc-server</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>address ipv4 address auth-port auth_port_number acct-port acct_port_number</code></td>
<td>Specifies the RADIUS server parameters.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-radius-server)# address ipv4 9.2.62.56 auth-port 1812 acct-port 1813</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>[pac] key key</code></td>
<td>Specify the authentication and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-radius-server)# key cisco</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>exit</code></td>
<td>Returns to the configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-radius-server)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>
| 7    | `aaa group server radius server-group` | Creates a radius server-group identification.  
Note: `server-group` refers to the server group name. The valid range is from 1 to 32 alphanumeric characters. |
|      | **Example:**      |         |
|      | `Device(config)# aaa group server radius authc-server-group` |         |
| 8    | `server name server-name` | Configures the server name. |
|      | **Example:**      |         |
|      | `Device(config)# server name free-radius-authc-server` |         |
| 9    | `end` | Returns to privileged EXEC mode. Alternatively, you can also press `Ctrl-Z` to exit global configuration mode. |
|      | **Example:**      |         |
|      | `Device(config)# end` |         |
Configuring Explicit Authorization Server List (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td>Purpose</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td>Purpose</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>radius server server-name</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# radius server cisco-dnac-authz-server</td>
</tr>
<tr>
<td>Purpose</td>
<td>Specifies the RADIUS server name.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>address ipv4 address auth-port auth_port_number acct-port acct_port_number</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-radius-server)# address ipv4 9.4.62.32 auth-port 1812 acct-port 1813</td>
</tr>
<tr>
<td>Purpose</td>
<td>Specifies the RADIUS server parameters.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>[pac] key key</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-radius-server)# pac key cisco</td>
</tr>
<tr>
<td>Purpose</td>
<td>Specify the authorization and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-radius-server)# exit</td>
</tr>
<tr>
<td>Purpose</td>
<td>Returns to the configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>aaa group server radius server-group</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# aaa group server radius authr-server-group</td>
</tr>
<tr>
<td>Purpose</td>
<td>Creates a radius server-group identification. <strong>Note</strong> server-group refers to the server group name. The valid range is from 1 to 32 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>server name server-name</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

For more information, see [Configuring AAA for External Authentication](#).
### Configuring Authentication and Authorization List for 802.1X Security

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device&gt; enable</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device# configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>wlan wlan-name wlan-id SSID-name</strong></td>
<td>Enters WLAN configuration sub-mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config)#wlan wlan-name foo-ssid</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you have already configured this command, enter <strong>wlan wlan-name</strong> command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>security dot1x authentication-list authenticate-list-name</strong></td>
<td>Enables authentication list for dot1x security.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config-wlan)# security dot1x authentication-list authc-server-group</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>security dot1x authorization-list authorize-list-name</strong></td>
<td>Specifies authorization list for dot1x security. For more information on the Cisco Digital Network Architecture Center (DNAC), see the DNAC documentation.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config-wlan)# security dot1x authorization-list authz-server-group</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Web Authentication for WLAN with Split Authentication and Authorization Servers

#### Configuring Authentication and Authorization List for Web Authentication

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>enable</strong>&lt;br&gt;&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device&gt; enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>configure terminal</strong>&lt;br&gt;&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 3 | **wlan wlan-name wlan-id SSID-name**<br><br>**Example:**<br>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**<br><br>**Example:**<br>Device(config-wlan)# no security wpa | Disables WPA security. |
| Step 5 | **no security wpa akm dot1x**<br><br>**Example:**<br>Device(config-wlan)# no security wpa akm dot1x | Disables security AKM for dot1x. |
### Command or Action

**Step 6**
```
no security wpa wpa2
```
**Example:**
```
Device(config-wlan)# no security wpa wpa2
```
**Purpose:** Disables WPA2 security.

**Step 7**
```
security web-auth {authentication-list authenticate-list-name | authorization-list authorize-list-name}
```
**Example:**
```
Device(config-wlan)# security web-auth authentication-list authc-server-group
```
**Purpose:** Enables authentication or authorization list for dot1x security.

**Step 8**
```
end
```
**Example:**
```
Device(config-wlan)# end
```
**Purpose:** 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-dnac-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 DNAC: Example

This example shows how to configure Cisco Catalyst 9800 Series Wireless Controller for authorization with Cisco ISE or DNAC:

Device(config)# radius server cisco-dnac-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-dnac-authz-server
Device(config)# end
CHAPTER 76

Secure LDAP (SLDAP)

• Information About SLDAP, on page 653
• Prerequisite for Configuring SLDAP, on page 655
• Restrictions for Configuring SLDAP, on page 655
• Configuring SLDAP, on page 655
• Configuring an AAA Server Group (GUI), on page 656
• Configuring a AAA Server Group, on page 657
• Configuring Search and Bind Operations for an Authentication Request, on page 658
• Configuring a Dynamic Attribute Map on an SLDAP Server, on page 659
• Verifying the SLDAP Configuration, on page 659

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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. |
<p>| <strong>Step 6</strong> | <code>bind authenticate root-dn password [0 string | 7 string] string</code> | Specifies a shared secret text string used between the Cisco Catalyst 9800 Series... |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Wireless Controller embedded wireless controller and an LDAP server.</td>
</tr>
<tr>
<td>Device(config-ldap-server)# bind authenticate root-dn CN=ldapipv6user,CN=Users,DC=ca,DC=ssh2,DC=com password Cisco12345</td>
<td>Use the 0 line option to configure an unencrypted shared secret.</td>
</tr>
<tr>
<td></td>
<td>Use the 7 line option to configure an encrypted shared secret.</td>
</tr>
</tbody>
</table>

**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.

**Step 2**

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.
### Configuring a AAA Server Group

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>aaa new-model</code></td>
<td>Enables AAA.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>aaa group server ldap group-name</code></td>
<td>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+.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa group server ldap name1</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>server name</code></td>
<td>Associates a particular LDAP server with the defined server group. Each security server is identified by its IP address and UDP port number.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-ldap-sg)# server server1</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Search and Bind Operations for an Authentication Request

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device# enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>Example: Device(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ldap server name</td>
<td>Defines a Lightweight Directory Access Protocol (LDAP) server and enters LDAP server configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# ldap server server1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> authentication bind-first</td>
<td>Configures the sequence of search and bind operations for an authentication request.</td>
</tr>
<tr>
<td>Example: Device(config-ldap-server)# authentication bind-first</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> authentication compare</td>
<td>Replaces the bind request with the compare request for authentication.</td>
</tr>
<tr>
<td>Example: Device(config-ldap-server)# authentication compare</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Exits LDAP server group configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-ldap-server)# exit</td>
<td></td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures a dynamic LDAP attribute map and enters attribute-map configuration mode.</td>
</tr>
<tr>
<td><code>ldap attribute-map map-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ldap attribute-map map1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Defines an attribute map.</td>
</tr>
<tr>
<td><code>map type ldap-attr-type aaa-attr-type</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-attr-map)# map type department supplicant-group</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Exits attribute-map configuration mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-attr-map)# exit</td>
</tr>
</tbody>
</table>

**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
Verifying the SLDAP Configuration
CHAPTER 77

RADIUS DTLS

- Information About RADIUS DTLS, on page 661
- Prerequisites, on page 663
- Configuring RADIUS DTLS Server, on page 663
- Configuring DTLS Dynamic Author, on page 668
- Enabling DTLS for Client, on page 668
- Verifying the RADIUS DTLS Server Configuration, on page 671
- Clearing RADIUS DTLS Specific Statistics, on page 671

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 Number section.

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.
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.

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

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>radius server server-name</td>
<td>Specifies the RADIUS server name.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# radius server R1</td>
<td></td>
</tr>
</tbody>
</table>
Configuring RADIUS DTLS Connection Timeout

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>radius server server-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# radius server R1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>dtls connectiontimeout timeout</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-radius-server)# dtls connectiontimeout 1</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-radius-server)# end</td>
</tr>
</tbody>
</table>

*Configuring RADIUS DTLS Connection Timeout*  
Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>dtls</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-radius-server)# dtls</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-radius-server)# end</td>
</tr>
</tbody>
</table>

*Configuring RADIUS DTLS Connection Timeout*  
Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>radius server server-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# radius server R1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>dtls connectiontimeout timeout</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-radius-server)# dtls connectiontimeout 1</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-radius-server)# end</td>
</tr>
</tbody>
</table>

*Configuring RADIUS DTLS Connection Timeout*  
Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# enable</td>
</tr>
</tbody>
</table>
Configuring Source Interface for RADIUS DTLS Server

### Command or Action | Purpose
--- | ---
**Device# enable** |  

**Step 2**

**configure terminal**

*Example:*

**Device# configure terminal**

**Step 3**

**radius server server-name**

*Example:*

**Device(config)# radius server R1**

**Step 4**

**dtls idletimeout idle_timeout**

*Example:*

**Device(config-radius-server)# dtls idletimeout 2**

**Step 5**

**end**

*Example:*

**Device(config-radius-server)# end**

---

**Configuring Source Interface for RADIUS DTLS Server**

**Procedure**

### Command or Action | Purpose
--- | ---
**Step 1**

**enable**

*Example:*

**Device# enable**

**Step 2**

**configure terminal**

*Example:*

**Device# configure terminal**

**Step 3**

**radius server server-name**

*Example:*

**Device(config)# radius server R1**

**Step 4**

**dtls ip {radius source-interface Ethernet-Internal interface_number**

*Example:*

**Device(config-radius-server)# dtls ip radius source-interface Ethernet-Internal 0**

---

- **interface_number** refers to the Ethernet-Internal interface number. The default value is 0.
### Configuring RADIUS DTLS Port Number

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>radius server server-name</td>
<td>Specifies the RADIUS server name.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# radius server R1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>dtls port port_number</td>
<td>Configures RADIUS DTLS port number.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-radius-server)# dtls port 2</td>
<td>Here, <code>port_number</code> refers to the DTLS port number.</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-radius-server)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring RADIUS DTLS Connection Retries

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring RADIUS DTLS Trustpoint

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# configure terminal</td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>radius server</strong> <code>server-name</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config)# radius server R1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>dtls retries</strong> <code>retry_number</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-radius-server)# dtls retries 3</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>end</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-radius-server)# end</td>
</tr>
</tbody>
</table>

### Configuring RADIUS DTLS Trustpoint

#### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device# enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>radius server</strong> <code>server-name</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config)# radius server R1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>dtls trustpoint</strong> `{client LINE dtls</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>end</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-radius-server)# end</td>
</tr>
</tbody>
</table>
## Configuring DTLS Dynamic Author

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>aaa server radius dynamic-author</code></td>
<td>Configures local server profile for RFC 3576 support.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# aaa server radius dynamic-author</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>dtls</code></td>
<td>Configures DTLS source parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-locsvr-da-radius)# dtls</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-locsvr-da-radius)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

## Enabling DTLS for Client

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>aaa server radius dynamic-author</code></td>
<td>Configures local server profile for RFC 3576 support.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-locsvr-da-radius)# aaa server radius dynamic-author</code></td>
<td></td>
</tr>
</tbody>
</table>
## Configuring Client Trustpoint for DTLS

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <strong>Device#</strong> enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: <strong>Device#</strong> configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa server radius dynamic-author</td>
<td>Configures local server profile for RFC 3576 support.</td>
</tr>
<tr>
<td>Example: <strong>Device(config)#</strong> aaa server radius dynamic-author</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> client IP_addr dtls {client-tp client-tp-name</td>
<td>server-tp server-tp-name}</td>
</tr>
<tr>
<td>Example: <strong>Device(config-locsvr-da-radius)#</strong> client 10.104.49.14 dtls client-tp client_tp_name</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
<tr>
<td>Example: <strong>Device(config-locsvr-da-radius)#</strong> end</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring DTLS Idle Timeout

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# <code>enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>aaa server radius dynamic-author</code></td>
<td>Configures local server profile for RFC 3576 support.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# <code>aaa server radius dynamic-author</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>`client IP_addr dtls idletimeout timeout-interval {client-tp client_tp_name</td>
<td>server-tp server_tp_name}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-locsvr-da-radius)# <code>client 10.104.49.14 dtls idletimeout 62 client-tp dtls_ise</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-locsvr-da-radius)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Server Trustpoint for DTLS

#### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# <code>enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# <code>configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th>aaa server radius dynamic-author</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config)# aaa server radius dynamic-author</td>
</tr>
<tr>
<td>Purpose</td>
<td>Configures local server profile for RFC 3576 support.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>client IP_addr dtls server-tp server_tp_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config-locsvr-da-radius)# client 10.104.49.14 dtls server-tp dtls_client</td>
</tr>
<tr>
<td>Purpose</td>
<td>Configures server trust point.</td>
</tr>
</tbody>
</table>

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

---

### 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.*
Clearing RADIUS DTLS Specific Statistics
MAC Authentication Bypass

You can configure the controller to authorize clients based on the client MAC address by using the MAC authentication bypass (MAB) feature.

When MAB 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. After detecting a client, the controller waits for a packet from the client. The controller sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address. If authorization succeeds, the controller grants the client access to the network. If authorization fails, the controller assigns the port to the guest WLAN, if one is configured.

Clients that were authorized with MAC authentication bypass can be re-authenticated. The re-authentication process is the same as that for clients that were authenticated. During re-authentication, the port remains in the previously assigned WLAN. If re-authentication is successful, the controller keeps the port in the same WLAN. If re-authentication fails, the controller assigns the port to the guest WLAN, if one is configured.

MAB Configuration Guidelines

- MAB configuration guidelines are the same as the 802.1x authentication guidelines.
- When MAB is disabled from a port after the port has been authorized with its MAC address, the port state is not affected.
- If the port is in the unauthorized state and the client MAC address is not the authentication-server database, the port remains in the unauthorized state. However, if the client MAC address is added to the database, the switch can use MAC authentication bypass to re-authorize the port.
• If the port is in the authorized state, the port remains in this state until re-authorization occurs.

• You can configure a timeout period for hosts that are connected by MAB but are inactive. The valid range is from 1 to 65535, in seconds.

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. A sample configuration is given below:

```plaintext
aaa attribute list FILTER_2
    attribute type ssid "WLC3-MACFILTER2"

aaa attribute list FILTER_1
    attribute type ssid "WLC3-MACFILTER1"

aaa authorization network MACFILTER1 local

wlan EWLC3-MACFILTER1 5 WLC3-MACFILTER1
    mac-filtering MACFILTER1
    no security wpa
    no security wpa wpa2 ciphers aes
    no security wpa akm dot1x
    security web-auth
    security web-auth authentication-list WEBAUTH

wlan WLC3-MACFILTER2 6 WLC3-MACFILTER2
    mac-filtering MACFILTER1
    no security wpa
    no security wpa wpa2 ciphers aes
    no security wpa akm dot1x

wireless profile policy MAC_FILTER_POLICY
    aaa-override
    autoqos mode voice
    no central switching
    service-policy input platinum-up
    service-policy output platinum
    session-timeout 180
    vlan 504
    no shutdown

username xxxxx mac aaa attribute list FILTER_1
```

## Configuring 802.11 Security for WLAN (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 **Security** tab, you can configure the following:

- Layer2
- Layer3
**AAA**

**Step 4**
In the **Layer2** tab, you can configure the following:

a) Choose the **Layer2 Security Mode** from the following options:
   - None—No Layer 2 security.
   - WPA + WPA2—Wi-Fi Protected Access.
   - Static WEP—Static WEP encryption parameters.

b) Enable **MAC Filtering** if required. MAC Filtering is also known as MAC Authentication Bypass (MAB).

c) In the **Protected Management Frame** section, choose the **PMF** as **Disabled, Optional**, or **Required**. By default, the PMF is disabled.

d) In the **WPA Parameters** section, choose the following options, if required:
   - WPA Policy
   - WPA2 Policy
   - WPA2 Encryption

e) Choose an option for **Auth Key Mgmt**.

f) Choose the appropriate status for **Fast Transition** between APs.

h) Enter the **Reassociation Timeout** value, in seconds. This is the time after which a fast transition reassociation times out.

i) Click **Save & Apply to Device**.

**Step 5**
In the **Layer3** tab, you can configure the following:

a) Check the **Web Policy** check box to use the web policy.

b) Choose the required **Webauth Parameter Map** value from the drop-down list.

c) Choose the required **Authentication List** value from the drop down list.

d) In the **Show Advanced Settings** section, check the **On Mac Filter Failure** check box.

f) Choose the appropriate IPv4 and IPv6 ACLs from the drop-down lists.

g) Click **Save & Apply to Device**.

**Step 6**
In the **AAA** tab, you can configure the following:

a) Choose an authentication list from the drop-down.

b) Check the **Local EAP Authentication** check box to enable local EAP authentication on the WLAN. Also, choose the required **EAP Profile Name** from the drop-down list.

c) Click **Save & Apply to Device**.

---

**Configuring 802.11 Security for WLAN (CLI)**

Follow the procedure below to configure 802.11 security for WLAN:
## Configuring AAA for External Authentication

Follow the procedure given below to configure AAA for external authentication.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>radius server</strong> server-name</td>
<td>Sets the radius server.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# radius server ISE</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>address {ipv4</td>
<td>ipv6}radius-server-ip-address auth-port auth-port-no acct-port acct-port-no</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-radius-server)# address ipv4 9.2.58.90 auth-port 1812 acct-port 1813</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>key</strong> key</td>
<td>Sets the per-server encryption key.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-radius-server)# key any123</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>exit</strong></td>
<td>Returns to the configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-locsvr-da-radius)# exit</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>aaa local authentication default authorization default</code></td>
<td>Selects the default local authentication and authorization.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# aaa local authentication default authorization default</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>aaa new-model</code></td>
<td>Creates a AAA authentication model. Enable new access control commands and functions.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# aaa new-model</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>aaa session-id common</code></td>
<td>Creates common session ID.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# aaa session-id common</code></td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>aaa authentication dot1x default group radius</code></td>
<td>Configures authentication for the default dot1x method.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# aaa authentication dot1x default group radius</code></td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td><code>aaa authorization network default group radius</code></td>
<td>Configures authentication for network services.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# aaa authorization network default group radius</code></td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td><code>dot1x system-auth-control</code></td>
<td>Enables SysAuthControl.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# dot1x system-auth-control</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring AAA for Local Authentication (GUI)

**Procedure**

- **Step 1**: Choose **Configuration > Tags & Profiles > WLANs**.
- **Step 2**: On the **Wireless Networks** page, click **Add**.
- **Step 3**: In the **Add WLAN** window that is displayed, select **Security > AAA**.
- **Step 4**: Select a value from the **Authentication List** drop-down.
- **Step 5**: Check the **Local EAP Authentication** check box to enable local EAP authentication on the WLAN.
- **Step 6**: Select a value from the **EAP Profile Name** drop-down.
Step 7  
Click Save & Apply to Device.

## Configuring AAA for Local Authentication (CLI)

Follow the procedure given below to configure AAA for local authentication.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>aaa authentication dot1x default local</td>
<td>Configures to use the default local RADIUS server.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# aaa authentication dot1x default local</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>aaa authorization network default local</td>
<td>Sets the authorization method to local.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# aaa authorization network default local</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>aaa authorization credential-download default local</td>
<td>Configures default database to download credentials from local server.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# aaa authorization credential-download default local</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>username mac-address mac</td>
<td>For MAC filtering using username.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# username 6038e0dc2d3f mac</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>aaa local authentication default authorization default</td>
<td>Configures the local authentication method list.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# aaa local authentication default authorization default</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>aaa new-model</td>
<td>Creates a AAA authentication model. Enable new access control commands and functions.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>aaa session-id common</td>
<td>Creates common session ID.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# aaa session-id common</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring MAB for Local Authentication

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.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>wlan profile-name wlan-id</code></td>
<td>Specifies the WLAN name and ID.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>wlan CRISSID_mab-local-default 1 CR1SSID_mab-local-default</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>mac-filtering default</code></td>
<td>Sets MAC filtering support for the WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Device(config-wlan)# mac-filtering default</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>no security wpa</code></td>
<td>Disables WPA security.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Device(config-wlan)# no security wpa</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>no security wpa akm dot1x</code></td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Device(config-wlan)# no security wpa akm dot1x</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>no security wpa wpa2</code></td>
<td>Disables WPA2 security.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Device(config-wlan)# no security wpa wpa2</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>no security wpa wpa2 ciphers aes</code></td>
<td>Disables WPA2 ciphers for AES.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Device(config-wlan)# no security wpa wpa2 ciphers aes</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>no shutdown</code></td>
<td>Enables the WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Device(config-wlan)# no shutdown</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring MAB for External Authentication (GUI)

Before you begin
Configure AAA external authentication.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Wireless &gt; WLANs.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Wireless Networks page, click the name of the WLAN.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Edit WLAN window, click the Security tab.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Layer2 tab, check the MAC Filtering check box to enable the feature.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>With MAC Filtering enabled, choose the Authorization List from the drop-down list.</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>Save the configuration.</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>wlan wlan-name wlan-id ssid-name</td>
<td>Specifies the WLAN name and ID.</td>
</tr>
<tr>
<td>Example:</td>
<td>wlan CR1_SSID_mab-ext-radius 3 CR1_SSID_mab-ext-radius</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>mac-filtering list-name</td>
<td>Sets the MAC filtering parameters.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# mac-filtering ewlc-radius</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>no security wpa</td>
<td>Disables WPA security.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# no security wpa</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>no security wpa akm dot1x</td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Security

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-wlan)# no security wpa akm dot1x</td>
<td>Disables WPA2 security.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>no security wpa wpa2</td>
<td>Disables WPA2 security.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# no security wpa wpa2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>no security wpa wpa2 ciphers aes</td>
<td>Disables WPA2 ciphers for AES.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# no security wpa wpa2 ciphers aes</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>no shutdown</td>
<td>Enables the WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>

---

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x
Configuring MAB for External Authentication (CLI)
IP Source Guard

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

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vlan profile-name wlan-id ssid</td>
<td>Specifies the WLAN name and ID to use.</td>
</tr>
</tbody>
</table>

Example:

Device(config)# wlan mywlan 34 mywlan-ssid

Note: If a WLAN is not already configured, this step creates the WLAN.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td><code>shutdown</code></td>
<td>Disables the WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# shutdown</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip verify source mac-check</code></td>
<td>Enables the IP Source Guard feature.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# ip verify source mac-check</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>no shutdown</code></td>
<td>Enables the WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>
Managing Rogue Devices

• Rogue Devices, on page 685
• How to Configure Rogue Location Discovery Protocol (RLDP), on page 688
• How to Configure Rogue Detection, on page 692
• Verifying Rogue Detection, on page 694
• Examples: Rogue Detection Configuration, on page 695

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 implementations might mitigate the effectiveness of ad hoc containment.
It is possible to classify and report rogue access points by using rogue states and user-defined classification rules that enable rogues to automatically move between states.

Each controller limits the number of rogue containments to three and six per radio for access points in the monitor mode.

Rogue Location Discovery Protocol (RLDP) detects rogue access points that are configured for open authentication.

RLDP detects rogue access points that use a broadcast Basic Service Set Identifier (BSSID), that is, the access point broadcasts its Service Set Identifier in beacons.

RLDP detects only those rogue access points that are on the same network. If an access list in the network prevents the sending of RLDP traffic from the rogue access point to the controller, RLDP does not work.

RLDP does not work on 5-GHz Dynamic Frequency Selection (DFS) channels.

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.

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.

If the rogue is contained by any other means, such as auto, and rule, the rogue entry is deleted when it expires.

The controller requests to the AAA server for rogue client validation only once. As a result, if rogue client validation fails on the first attempt then the rogue client will not be detected as a threat any more. To avoid this, add the valid client entries in the authentication server before enabling Validate Rogue Clients Against AAA.

Restrictions on Rogue Detection

• Rogue containment is not supported on DFS channels.

Rogue Location Discovery Protocol

Rogue Location Discovery Protocol (RLDP) is an active approach, which is used when rogue AP has no authentication (Open Authentication) configured. This mode, which is disabled by default, instructs an active AP to move to the rogue channel and connect to the rogue as a client. During this time, the active AP sends de-authentication messages to all connected clients and then shuts down the radio interface. Then, it associates to the rogue AP as a client. The AP then tries to obtain an IP address from the rogue AP and forwards a User Datagram Protocol (UDP) packet (port 6352) that contains the local AP and rogue connection information to the controller through the rogue AP. If the controller receives this packet, the alarm is set to notify the network administrator that a rogue AP was discovered on the wired network with the RLDP feature.

The following steps describe the functioning of RLDP:

1. Identify the closest Unified AP to the rogue using signal strength values.

2. The AP then connects to the rogue as a WLAN client, attempting three associations before timing out.
3. If association is successful, the AP then uses DHCP to obtain an IP address.

4. If an IP address was obtained, the AP (acting as a WLAN client) sends a UDP packet to each of the controller’s IP addresses.

5. If the controller receives even one of the RLDP packets from the client, that rogue is marked as on-wire.

Note

The RLDP packets are unable to reach the controller if filtering rules are placed between the controller’s network and the network where the rogue device is located.

Restrictions for RLDP:

• RLDP only works with open rogue APs broadcasting their SSID with authentication and encryption disabled.

• RLDP requires that the Managed AP acting as a client is able to obtain an IP address via DHCP on the rogue network.

• Manual RLDP can be used to attempt an RLDP trace on a rogue multiple number of times.

• During RLDP process, the AP is unable to serve clients. This negatively impacts performance and connectivity for local mode APs. To avoid this case, RLDP can be selectively enabled for Monitor Mode AP only.

• RLDP does not attempt to connect to a rogue AP operating in a 5GHz DFS channel.

Detecting Rogue Devices

The controller continuously monitors all the nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) 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.

A rogue access point is moved to a contained state either automatically or manually. The controller selects the best available access point for containment and pushes the information to the access point. The access point stores the list of containments per radio. For auto containment, you can configure the controller to use only the monitor mode access point. The containment operation occurs in the following two ways:
   • The container access point goes through the list of containments periodically and sends unicast containment frames. For rogue access point containment, the frames are sent only if a rogue client is associated.
   • Whenever a contained rogue activity is detected, containment frames are transmitted.

Individual Rogue containment involves sending a sequence of unicast disassociation and deauthentication frames.

Cisco Prime Infrastructure Interaction and Rogue Detection

Cisco Prime Infrastructure supports rule-based classification and uses the classification rules configured on the controller. The controller sends traps to Cisco Prime Infrastructure after the following events:
   • If an unknown access point moves to the Friendly state for the first time, the controller sends a trap to Cisco Prime Infrastructure only if the rogue state is Alert. It does not send a trap if the rogue state is Internal or External.
   • If a rogue entry is removed after the timeout expires, the controller sends a trap to Cisco Prime Infrastructure for rogue access points that are categorized as Malicious (Alert, Threat) or Unclassified (Alert). The controller does not remove rogue entries with the following rogue states: Contained, Contained Pending, Internal, and External.

This section contains the following subsections:

How to Configure Rogue Location Discovery Protocol (RLDP)

Configuring an RLDP for Generating Alarms (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Security &gt; Wireless Protection Policies.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Rogue Policies tab, use the Rogue Detection Security Level drop-down to select the security level.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Expiration timeout for Rogue APs (seconds) field, enter the timeout value.</td>
</tr>
</tbody>
</table>
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 for rogues.

Step 7  Select the **Detect and Report Adhoc Networks** check box to validate rogue clients against AAA server.

Step 8  In the **Rogue Detection Client Number Threshold** field, enter the threshold for rogue client detection.

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 a particular SSID.

Step 14 Select the **Adhoc Rogue AP** check box to limit the auto-containment only to adhoc rogue APs.

Step 15 Click **Apply**.

### Configuring an RLDP for Generating Alarms (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enables RLDP to generate alarms. In this method, the RLDP is always enabled.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>The <code>monitor-ap-only</code> keyword is optional.</td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td>The command with just the <code>alarm-only</code> keyword enables RLDP without any restriction on the AP mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables RLDP to generate alarms. In this method, the RLDP is always enabled.</td>
</tr>
<tr>
<td><code>wireless wps rogue ap rldp alarm-only &lt;monitor-ap-only&gt;</code></td>
<td>The command with just the <code>alarm-only</code> keyword enables RLDP without any restriction on the AP mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>The command with <code>alarm-only &lt;monitor-ap-only&gt;</code> keyword enables RLDP in monitor mode access points only.</td>
</tr>
<tr>
<td><code>Device(config)# wireless wps rogue ap rldp alarm-only</code></td>
<td>The <code>monitor-ap-only</code> keyword is optional.</td>
</tr>
<tr>
<td><code>Device(config)# wireless wps rogue ap rldp alarm-only monitor-ap-only</code></td>
<td>The command with <code>alarm-only &lt;monitor-ap-only&gt;</code> keyword enables RLDP in monitor mode access points only.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <code>Ctrl-Z</code> to exit global configuration mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <code>Ctrl-Z</code> to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <code>Ctrl-Z</code> to exit global configuration mode.</td>
</tr>
<tr>
<td><code>Device(config)# end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <code>Ctrl-Z</code> to exit global configuration mode.</td>
</tr>
</tbody>
</table>
Configuring an RLDP for Auto-Contain (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Configuration &gt; Security &gt; Wireless Protection Policies</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the <strong>RLDP</strong> tab, use the <strong>Rogue Location Discovery Protocol</strong> drop-down to select All APs.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Retry Count</strong> field, enter the number of retries.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select the <strong>Schedule RLDP</strong> check box to set a schedule and enter the day and start time and end time.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

Configuring an RLDP for Auto-Contain (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td>Enables RLDP to perform auto-contain. In this method, the RLDP is always enabled.</td>
</tr>
<tr>
<td>Step 2 wireless wps rogue ap rldp auto-contain [monitor-ap-only]</td>
<td>Enables RLDP to perform auto-contain. In this method, the RLDP is always enabled.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wireless wps rogue ap rldp auto-contain</td>
<td>The <strong>monitor-ap-only</strong> keyword is optional.</td>
</tr>
<tr>
<td></td>
<td>The command with just the <strong>auto-contain</strong> keyword enables RLDP without any restriction on the AP mode.</td>
</tr>
<tr>
<td></td>
<td>The command with <strong>auto-contain &lt;monitor-ap-only&gt;</strong> keyword enables RLDP in monitor mode access points only.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Configuring a Schedule for RLDP (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Configuration &gt; Security &gt; Wireless Protection Policies</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the <strong>RLDP</strong> tab, choose one of the following options from the <strong>Rogue Location Discovery Protocol</strong> drop-down list:</td>
</tr>
</tbody>
</table>
• **Disable (default)**—Disables RLDP on all the access points.
• **All APs**—Enables RLDP on all APs.
• **Monitor Mode APs**—Enables RLDP only on APs in the monitor mode.

**Step 3** Enter the number of retries that should be attempted.

**Step 4** If you want to schedule the rogue location discovery process, 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wireless wps rogue ap rldp schedule day day start start-time end end-time</td>
<td>Enables RLDP based on a scheduled day, start time, and end time.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# wireless wps rogue ap rldp schedule day Monday start 10:10:01 end 12:00:00</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>wireless wps rogue ap rldp schedule</td>
<td>Enables the schedule.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# wireless wps rogue ap rldp schedule</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring RLDP Retry Times on Rogue Access Points (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Configuration &gt; Security &gt; Wireless Protection Policies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>On the Wireless Protection Policies page, click the RLDP tab.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the RLDP retry attempt value for rogue access points in the Retry Count field. The valid range is between 1 and 5.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Save the configuration.</td>
</tr>
</tbody>
</table>

Configuring RLDP Retry Times on Rogue Access Points (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless wps rogue ap rldp retries num-entries</td>
<td>Enables RLDP retry times on rogue access points.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wireless wps rogue ap rldp retries 2</td>
<td>Here, num-entries is the number of RLDP retry times for each of the rogue access points. The valid range is 1 to 5.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

How to Configure Rogue Detection

Configuring Rogue Detection (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Configuring Rogue Detection (CLI)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# configure terminal</td>
<td>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. <strong>Note</strong> 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.</td>
</tr>
<tr>
<td><strong>Step 2</strong> ap profile <em>profile-name</em> rogue detection min-rssi <em>rssi in dBm</em></td>
<td><strong>Example:</strong> Device(config)# ap profile profile1 Device(config)# rogue detection min-rssi -100</td>
</tr>
</tbody>
</table>
| **Step 3** ap profile *profile-name* rogue detection min-transient-time *time in seconds* | **Example:** Device(config)# ap profile profile1 Device(config)# rogue detection min-transient-time 120 Valid range for the time in sec parameter is 120 seconds to 1800 seconds, and the default value is 0. **Note** This feature is applicable to APs that are in monitor mode only. Using the transient interval values, you can control the time interval at which APs should scan for rogues. APs can also filter the rogues based on their transient interval values. This feature has the following advantages:

- Rogue reports from APs to the controller are shorter
- Transient rogue entries are avoided in the controller
- Unnecessary memory allocation for transient rogues are avoided |
| **Step 4** wireless wps rogue ap notify-rssi-deviation | **Example:** Device(config)# wireless wps rogue ap notify-rssi-deviation |
### Verify 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 21: Verifying Adhoc Rogues Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless wps rogue adhoc detailed mac_address</code></td>
<td>Displays the detailed information for an Adhoc rogue.</td>
</tr>
<tr>
<td><code>show wireless wps rogue adhoc summary</code></td>
<td>Displays a list of all Adhoc rogues.</td>
</tr>
</tbody>
</table>

#### Table 22: Verifying Rogue AP Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless wps rogue ap clients mac_address</code></td>
<td>Displays the list of all rogue clients associated with a rogue.</td>
</tr>
<tr>
<td><code>show wireless wps rogue ap custom summary</code></td>
<td>Displays the custom rogue AP information.</td>
</tr>
<tr>
<td><code>show wireless wps rogue ap detailed mac_address</code></td>
<td>Displays the detailed information for a rogue AP.</td>
</tr>
<tr>
<td><code>show wireless wps rogue ap friendly summary</code></td>
<td>Displays the friendly rogue AP information.</td>
</tr>
<tr>
<td><code>show wireless wps rogue ap list mac_address</code></td>
<td>Displays the list of rogue APs detected by a given AP.</td>
</tr>
<tr>
<td><code>show wireless wps rogue ap malicious summary</code></td>
<td>Displays the malicious rogue AP information.</td>
</tr>
<tr>
<td><code>show wireless wps rogue ap rldp detailed mac_address</code></td>
<td>Displays the RLDP details for a rogue AP.</td>
</tr>
<tr>
<td><code>show wireless wps rogue ap rldp in progress</code></td>
<td>Displays the list of in-progress RLDP.</td>
</tr>
<tr>
<td><code>show wireless wps rogue ap rldp summary</code></td>
<td>Displays the summary of RLDP scheduling information.</td>
</tr>
<tr>
<td><code>show wireless wps rogue ap summary</code></td>
<td>Displays a list of all Rogue APs.</td>
</tr>
<tr>
<td><code>show wireless wps rogue ap unclassified summary</code></td>
<td>Displays the unclassified rogue AP information.</td>
</tr>
</tbody>
</table>
Table 23: Verifying Rogue Auto-Containment Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless wps rogue auto-contain</code></td>
<td>Displays the rogue auto-containment information.</td>
</tr>
</tbody>
</table>

Table 24: Verifying Classification Rule Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless wps rogue rule detailed rule_name</code></td>
<td>Displays the detailed information for a classification rule.</td>
</tr>
<tr>
<td><code>show wireless wps rogue rule summary</code></td>
<td>Displays the list of all rogue rules.</td>
</tr>
</tbody>
</table>

Table 25: Verifying Rogue Statistics

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless wps rogue stats</code></td>
<td>Displays the rogue statistics.</td>
</tr>
</tbody>
</table>

Table 26: Verifying Rogue Client Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless wps rogue client detailed mac_address</code></td>
<td>Displays detailed information for a Rogue client.</td>
</tr>
<tr>
<td><code>show wireless wps rogue client summary</code></td>
<td>Displays a list of all the Rogue clients.</td>
</tr>
</tbody>
</table>

Table 27: Verifying Rogue Ignore List

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless wps rogue ignore-list</code></td>
<td>Displays the rogue ignore list.</td>
</tr>
</tbody>
</table>

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 at the:

```
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
Classifying Rogue Access Points

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).

- 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 classified, 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 28: Classification Mapping

<table>
<thead>
<tr>
<th>Rule-Based Classification Type</th>
<th>Rogue State</th>
</tr>
</thead>
</table>
| 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 rouges 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.

How to Classify Rogue Access Points

Classifying Rogue Access Points and Clients Manually (GUI)

**Procedure**

2. In the Unclassified tab, select an AP to view the detail in the lower pane.
3. Use the Class Type drop-down to set the status.
4. Click Apply.

Classifying Rogue Access Points and Clients Manually (CLI)

**Procedure**

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

Example:

---

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x
### Command or Action

<table>
<thead>
<tr>
<th>Command/Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device# configure terminal</code></td>
<td>Detects and reports the ad hoc rogue. Enter one of these options after you enter the <code>adhoc</code> keyword:</td>
</tr>
<tr>
<td>`wireless wps rogue adhoc {alert mac-addr</td>
<td>auto-contain</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config)# wireless wps rogue adhoc alert 74a0.2f45.c520</code></td>
<td>• <strong>auto-contain</strong>— Sets the automatically containing ad hoc rogue to auto-contain mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config)# wireless wps rogue adhoc auto-contain</code></td>
<td>• <strong>contain</strong>— Sets the containing ad hoc rogue access point to contain mode. If you choose this option, enter the MAC address for the <code>mac-addr</code> parameter and containment level for the <code>containment-level</code> parameter. The valid range for <code>containment-level</code> is from 1 to 4.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config)# wireless wps rogue adhoc contain</code></td>
<td>• <strong>external</strong>— Sets the ad hoc rogue access point as <strong>external</strong>. If you choose this option, enter the MAC address for the <code>mac-addr</code> parameter.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config)# wireless wps rogue adhoc external</code></td>
<td>• <strong>internal</strong>— Sets the ad hoc rogue access point as <strong>internal</strong>. If you choose this option, enter the MAC address for the <code>mac-addr</code> parameter.</td>
</tr>
</tbody>
</table>

### Command or Action

<table>
<thead>
<tr>
<th>Command/Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device# configure terminal</code></td>
<td>Configures the rogue access points. Enter one of the following options after the <code>ap</code> keyword:</td>
</tr>
<tr>
<td>`wireless wps rogue ap {friendly mac-addr</td>
<td>state [external</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config)# wireless wps rogue ap malicious 74a0.2f45.c520 state contain 3</code></td>
<td>• <strong>malicious</strong>—Configures the malicious rogue access points. If you choose this option, enter the MAC address for the</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 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**


**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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal&lt;br&gt;Example:&lt;br&gt;Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless wps rogue rule rule-name priority priority&lt;br&gt;Example:&lt;br&gt;Device(config)# wireless wps rogue rule rule_3 priority 3</td>
<td>Creates or enables a rule. While creating a rule, you must enter the priority for the rule.</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>classify {friendly</td>
<td>malicious}&lt;br&gt;Example:&lt;br&gt;Device(config)# wireless wps rogue rule rule_3 priority 3&lt;br&gt;Device(config-rule)# classify friendly</td>
</tr>
<tr>
<td>Step 4</td>
<td>condition {client-count value</td>
<td>duration duration_value</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>match {all</td>
<td>any}</td>
<td>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.</td>
</tr>
<tr>
<td>default</td>
<td>Sets a command to its default.</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits the sub-mode.</td>
<td></td>
</tr>
<tr>
<td>shutdown</td>
<td>Disables a particular rogue rule. In this example, the rule rule_3 is disabled.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

Example:

```
Device(config)# wireless wps rogue rule
rule_3 priority 3
Device(config-rule)# match all
```

**Step 6**

Example:

```
Device(config)# wireless wps rogue rule
rule_3 priority 3
Device(config-rule)# default
```

**Step 7**

Example:

```
Device(config)# wireless wps rogue rule
rule_3 priority 3
Device(config-rule)# exit
Device(config)#
```

**Step 8**

Example:
### Monitoring Rogue Classification Rules

You can monitor the rogue classification rules using the following commands:

**Table 29: Commands for Monitoring Rogue Classification Rules**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless wps rogue rule detailed</code></td>
<td>Displays detailed information of a classification rule.</td>
</tr>
<tr>
<td><code>show wireless wps rogue rule summary</code></td>
<td>Displays a summary of the classification rules.</td>
</tr>
</tbody>
</table>

### Examples: Classifying Rogue Access Points

This example shows how to create a rule that can organize and display rogue access points as Friendly:

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# classify friendly state internal
Device(config-rule)# end
```

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)# end

This example shows how to enable a rule:

Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# no shutdown
Examples: Classifying Rogue Access Points
CHAPTER 82

Configuring Secure Shell

• Information About Configuring Secure Shell, on page 707
• Prerequisites for Configuring Secure Shell, on page 709
• Restrictions for Configuring Secure Shell, on page 710
• How to Configure SSH, on page 710
• Monitoring the SSH Configuration and Status, on page 714

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.
SSH Configuration Guidelines

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 an SSHv1 server can be used by an SSHv2 server, and the reverse.
- If the SSH server is running on a stack master and the stack master fails, the new stack master uses the RSA key pair generated by the previous stack master.
- 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.
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:

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 Adleman (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.

---

**Note**

While upgrading from 16.11 to a later version, if you encounter a host key change by SSH client, you need to know the following:

• Wave 2 AP now supports a third key type ED25519 along with the RSA and ECDSA keys.

• The RSA and ECDSA keys are used for normal operations.

• The ED25519 key is used for FIPS mode.

---

### Restrictions for Configuring Secure Shell

The following are restrictions for configuring the device for secure shell.

• 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. This step is required. For more information, see Related Topics below.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> hostname <em>hostname</em></td>
<td>Configures a hostname and IP domain name for your Device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# hostname your_hostname</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip domain-name <em>domain_name</em></td>
<td>Configures a host domain for your Device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip domain-name your_domain</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> crypto key generate rsa</td>
<td>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.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# crypto key generate rsa</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

Follow this procedure only if you are configuring the Device as an SSH server.

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.
### Configuring the SSH Server

Follow the procedure given below to configure the SSH server:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `enable` | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Step 2** | `configure terminal` | Enters global configuration mode. |
  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. |

---

**Note**

This procedure is only required if you are configuring the Device as an SSH server.
### Configuring the SSH Server

#### Step 4
**Purpose**
Specifies the SSH window size. The recommended window size is 32K or lesser that that. The default window size is 8912.

**Command or Action**
`ip ssh window-size`

**Example:**
```
Device(config)# ip ssh window-size
```

**Purpose**
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 5
**Purpose**
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**
`ip ssh {timeout seconds | authentication-retries number}`

**Example:**
```
Device(config)# ip ssh timeout 90
```

#### Step 6
**Purpose**
(Optional) Configures the virtual terminal line settings.

**Command or Action**
- `line vty line_number[ending_line_number]`
- `transport input ssh`

**Example:**
```
Device(config)# line vty 1 10
```

Use one or both of the following:
**Purpose**

**Command or Action**

- `Device(config-line)# transport input ssh`

**Purpose**

- Specifies that the Device prevent non-SSH Telnet connections. This limits the router to only SSH connections.

---

**Step 7**

- **end**

**Example:**

- `Device(config-line)# end`

**Purpose**

- Returns to privileged EXEC mode.

---

**Step 8**

- **show running-config**

**Example:**

- `Device# show running-config`

**Purpose**

- Verifies your entries.

---

**Step 9**

- **copy running-config startup-config**

**Example:**

- `Device# copy running-config startup-config`

**Purpose**

- (Optional) Saves your entries in the configuration file.

---

### Monitoring the SSH Configuration and Status

This table displays the SSH server configuration and status.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip ssh</code></td>
<td>Shows the version and configuration information for the SSH server.</td>
</tr>
<tr>
<td><code>show ssh</code></td>
<td>Shows the status of the SSH server.</td>
</tr>
</tbody>
</table>

---

**Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x**
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.

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 pass phrase 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 pass phrase can remain the same.

**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.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>wlan wlan-name wlan-id ssid</code></td>
<td>Configures the WLAN and SSID.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wlan test-profile 4 abc</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>no security wpa akm dot1x</code></td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wlan)# no security wpa akm dot1x</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>security wpa akm psk</code></td>
<td>Configures the security type PSK.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wlan)# security wpa akm psk</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>security wpa akm psk set-key ascii/hex key</code></td>
<td>Configures the PSK authenticated key management (AKM) shared key.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wlan)# security wpa akm psk set-key ascii 0</td>
<td>Note: You must set the <code>psk set-key</code> before configuring AKM PSK.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>security wpa akm psk</code></td>
<td>Configures PSK support.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><code>Device(config-wlan)# security wpa akm psk</code></td>
<td>Configures multi-preshared key (MPSK) support.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> security wpa wpa2 mpsk <strong>Example:</strong> Device(config-wlan)# security wpa wpa2 mpsk</td>
<td>Configures multi-preshared key (MPSK) support. <strong>Note</strong> AKM PSK should be enabled for MPSK to work.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> <code>mac-filtering auth-list-name</code> <strong>Example:</strong> Device(config-wlan)# mac-filtering test1</td>
<td>Specifies MAC filtering in a WLAN.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring a PSK in a WLAN (GUI)

**Procedure**

1. **Step 1** Choose **Configuration** > **Tags & Profiles** > **WLANs**.
2. **Step 2** On the **Wireless Networks** page, click **Security** tab.
3. **Step 3** In the **Layer 2** window that is displayed, go to the **WPA Parameters** section.
4. **Step 4** From the **Auth Key Mgmt** drop-down, select PSK.
5. **Step 5** Click **Save & Apply to Device**.

### Applying a Policy Profile to a WLAN (GUI)

**Procedure**

1. **Step 1** Choose **Configuration** > **Tags & Profiles** > **Tags**.
2. **Step 2** On the **Manage Tags** page, click **Policy** tab.
3. **Step 3** Click **Add** to view the **Add Policy Tag** window.
4. **Step 4** Enter a name and description for the policy tag.
5. **Step 5** Click **Add** to map WLAN and policy.
6. **Step 6** Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.
7. **Step 7** Click **Save & Apply to Device**.
Applying a Policy Profile to a WLAN (CLI)

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

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>wireless profile policy</strong> policy-profile-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless profile policy policy-iot</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>aaa-override</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# aaa-override</td>
</tr>
</tbody>
</table>

### Verifying a Private PSK

Use the following `show` commands to verify the configuration of a WLAN and a client:

Device# show wlan id 2

<table>
<thead>
<tr>
<th>WLAN Profile Name</th>
<th>: test_ppsk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>: 2</td>
</tr>
<tr>
<td>Network Name (SSID)</td>
<td>: test_ppsk</td>
</tr>
<tr>
<td>Status</td>
<td>: Enabled</td>
</tr>
<tr>
<td>Broadcast SSID</td>
<td>: Enabled</td>
</tr>
<tr>
<td>Universal AP Admin</td>
<td>: Disabled</td>
</tr>
<tr>
<td>Max Associated Clients per WLAN</td>
<td>: 0</td>
</tr>
<tr>
<td>Max Associated Clients per AP per WLAN</td>
<td>: 0</td>
</tr>
<tr>
<td>Max Associated Clients per AP Radio per WLAN</td>
<td>: 0</td>
</tr>
<tr>
<td>Number of Active Clients</td>
<td>: 0</td>
</tr>
<tr>
<td>Exclusionlist Timeout</td>
<td>: 60</td>
</tr>
<tr>
<td>CHD per WLAN</td>
<td>: Enabled</td>
</tr>
<tr>
<td>Interface</td>
<td>: default</td>
</tr>
<tr>
<td>Multicast Interface</td>
<td>: Unconfigured</td>
</tr>
<tr>
<td>WMM</td>
<td>: Allowed</td>
</tr>
<tr>
<td>WiFiDirect</td>
<td>: Invalid</td>
</tr>
<tr>
<td>Channel Scan Defer Priority:</td>
<td></td>
</tr>
<tr>
<td>Priority (default)</td>
<td>: 4</td>
</tr>
<tr>
<td>Priority (default)</td>
<td>: 5</td>
</tr>
<tr>
<td>Priority (default)</td>
<td>: 6</td>
</tr>
<tr>
<td>Scan Defer Time (msecs)</td>
<td>: 100</td>
</tr>
<tr>
<td>Media Stream Multicast-direct</td>
<td>: Disabled</td>
</tr>
<tr>
<td>CCX - AironetIe Support</td>
<td>: Enabled</td>
</tr>
</tbody>
</table>
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)
  WPA (SSN IE) : Disabled
  WPA2 (RSN IE) : Enabled
TKIP Cipher : Enabled
AES Cipher : Enabled
Auth Key Management
  802.1x : Disabled
PSK
  CCKM : Disabled
  FT dot1x : Disabled
  FT PSK : Disabled
  PMF dot1x : Disabled
  PMF PSK : Disabled
CCKM TSF Tolerance : 1000
FT Support
  FT Reassociation Timeout : 20
  FT Over-The-DS mode : Enabled
PMF Support
  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
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
  Optimised Roaming 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 : 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
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

Verifying a Private PSK
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
Verifying a Private PSK
Multi-Preshared Key

- Information About Multi-Preshared Key, on page 723
- Restrictions on Multi-PSK, on page 724
- Configuring Multi-Preshared Key (GUI), on page 724
- Configuring Multi-Preshared Key (CLI), on page 726
- Verifying Multi-PSK Configurations, on page 727

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 16: Traditional PSK*

![Traditional PSK Diagram](image)

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.
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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configuration &gt; Tags &amp; Profiles &gt; WLANs</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the <strong>Wireless Networks</strong> page, click the name of the WLAN.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Edit WLAN</strong> window, click the <strong>Security</strong> tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the <strong>Layer 2</strong> tab, choose the <strong>Layer 2 Security Mode</strong> from the following options:</td>
</tr>
<tr>
<td></td>
<td>• None: No Layer 2 security</td>
</tr>
<tr>
<td></td>
<td>• 802.1X: WEP 802.1X data encryption type</td>
</tr>
<tr>
<td></td>
<td>• WPA + WPA2: Wi-Fi Protected Access</td>
</tr>
<tr>
<td></td>
<td>• Static WEP: Static WEP encryption parameters</td>
</tr>
<tr>
<td></td>
<td>• Static WEP+802.1X: Both Static WEP and 802.1X parameters</td>
</tr>
<tr>
<td>Parameters</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>802.1X</strong></td>
<td></td>
</tr>
<tr>
<td>WEP Key Size</td>
<td>Choose the key size. The available values are <em>None</em>, 40 bits, and 104 bits.</td>
</tr>
<tr>
<td><strong>WPA + WPA2</strong></td>
<td></td>
</tr>
<tr>
<td>Protected Management Frame</td>
<td>Choose from the following options:</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
</tr>
<tr>
<td></td>
<td>• Optional</td>
</tr>
<tr>
<td></td>
<td>• Required</td>
</tr>
<tr>
<td>WPA Policy</td>
<td>Check the check box to enable WPA policy.</td>
</tr>
<tr>
<td>WPA Encryption</td>
<td>Choose the WPA encryption standard. A WPA encryption standard must be specified if you have enabled WPA policy.</td>
</tr>
<tr>
<td>WPA2 Policy</td>
<td>Check the check box to enable WPA2 policy.</td>
</tr>
<tr>
<td>WPA2 Encryption</td>
<td>Choose the WPA2 encryption standard. A WPA encryption standard must be specified if you have enabled WPA policy.</td>
</tr>
<tr>
<td>Auth Key Mgmt</td>
<td>Choose the rekeying mechanism from the following options:</td>
</tr>
<tr>
<td></td>
<td>• 802.1X</td>
</tr>
<tr>
<td></td>
<td>• FT + 802.1X</td>
</tr>
<tr>
<td></td>
<td>• PSK: You must specify the PSK format and a preshared key</td>
</tr>
<tr>
<td></td>
<td>• CCKM: You must specify a CCKM Timestamp Tolerance value</td>
</tr>
<tr>
<td></td>
<td>• 802.1X + CCKM: You must specify a CCKM Timestamp Tolerance value</td>
</tr>
<tr>
<td></td>
<td>• FT + 802.1X + CCKM: You must specify a CCKM Timestamp Tolerance value</td>
</tr>
<tr>
<td><strong>Static WEP</strong></td>
<td></td>
</tr>
<tr>
<td>Key Size</td>
<td>Choose the key size from the following options:</td>
</tr>
<tr>
<td></td>
<td>• 40 bits</td>
</tr>
<tr>
<td></td>
<td>• 104 bits</td>
</tr>
</tbody>
</table>
## Configuring Multi-Preshared Key (CLI)

### Procedure

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

### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Index</td>
<td>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.</td>
</tr>
<tr>
<td>Key Format</td>
<td>Choose the encryption key format as either ASCII or HEX.</td>
</tr>
<tr>
<td>Encryption Key</td>
<td>Enter an encryption key that is 13 characters long.</td>
</tr>
</tbody>
</table>

### Static WEP + 802.1X

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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. |
| **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
### Security

<table>
<thead>
<tr>
<th>Config</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Name (SSID)</td>
<td>ssid_8</td>
</tr>
<tr>
<td>Status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Broadcast SSID</td>
<td>Enabled</td>
</tr>
<tr>
<td>Universal AP Admin</td>
<td>Disabled</td>
</tr>
<tr>
<td>Max Associated Clients per WLAN</td>
<td>0</td>
</tr>
<tr>
<td>Max Associated Clients per AP per WLAN</td>
<td>0</td>
</tr>
<tr>
<td>Max Associated Clients per AP Radio per WLAN</td>
<td>200</td>
</tr>
<tr>
<td>Number of Active Clients</td>
<td>0</td>
</tr>
<tr>
<td>CHD per WLAN</td>
<td>Enabled</td>
</tr>
<tr>
<td>Multicast Interface</td>
<td>Unconfigured</td>
</tr>
<tr>
<td>WMM</td>
<td>Allowed</td>
</tr>
<tr>
<td>WifiDirect</td>
<td>Invalid</td>
</tr>
<tr>
<td>Channel Scan Defer Priority:</td>
<td></td>
</tr>
<tr>
<td>Priority (default)</td>
<td>5</td>
</tr>
<tr>
<td>Priority (default)</td>
<td>6</td>
</tr>
<tr>
<td>Scan Defer Time (msecs)</td>
<td>100</td>
</tr>
<tr>
<td>Media Stream Multicast-direct</td>
<td>Disabled</td>
</tr>
<tr>
<td>CCX - Aironet Support</td>
<td>Enabled</td>
</tr>
<tr>
<td>CCX - Diagnostics Channel Capability</td>
<td>Disabled</td>
</tr>
<tr>
<td>Peer-to-Peer Blocking Action</td>
<td>Disabled</td>
</tr>
<tr>
<td>Radio Policy</td>
<td>All</td>
</tr>
<tr>
<td>DTIM period for 802.11a radio</td>
<td>1</td>
</tr>
<tr>
<td>DTIM period for 802.11b radio</td>
<td>1</td>
</tr>
<tr>
<td>Local EAP Authentication</td>
<td>Disabled</td>
</tr>
<tr>
<td>Mac Filter Authorization list name</td>
<td>Disabled</td>
</tr>
<tr>
<td>Mac Filter Override Authorization list name</td>
<td>Disabled</td>
</tr>
<tr>
<td>Accounting list name</td>
<td></td>
</tr>
<tr>
<td>802.1x authentication list name</td>
<td>Disabled</td>
</tr>
<tr>
<td>802.1x authorization list name</td>
<td>Disabled</td>
</tr>
<tr>
<td>802.11 Authentication</td>
<td>Open System</td>
</tr>
<tr>
<td>Static WEP Keys</td>
<td>Disabled</td>
</tr>
<tr>
<td>802.1x</td>
<td>Disabled</td>
</tr>
<tr>
<td>Wi-Fi Protected Access (WPA/WPA2/WPA3)</td>
<td></td>
</tr>
<tr>
<td>WPA (SSN IE)</td>
<td>Disabled</td>
</tr>
<tr>
<td>WPA2 (RSN IE)</td>
<td>Enabled</td>
</tr>
<tr>
<td>MPSK</td>
<td>Enabled</td>
</tr>
<tr>
<td>AES Cipher</td>
<td>Enabled</td>
</tr>
<tr>
<td>CCMP256 Cipher</td>
<td>Disabled</td>
</tr>
<tr>
<td>GCMP128 Cipher</td>
<td>Disabled</td>
</tr>
<tr>
<td>GCMP256 Cipher</td>
<td>Disabled</td>
</tr>
<tr>
<td>WPA3 (WPA3 IE)</td>
<td>Disabled</td>
</tr>
<tr>
<td>Auth Key Management</td>
<td></td>
</tr>
<tr>
<td>802.1x</td>
<td>Disabled</td>
</tr>
<tr>
<td>PSK</td>
<td>Enabled</td>
</tr>
<tr>
<td>CCKM</td>
<td>Disabled</td>
</tr>
<tr>
<td>FT dot1x</td>
<td>Disabled</td>
</tr>
<tr>
<td>FT PSK</td>
<td>Disabled</td>
</tr>
<tr>
<td>FT SAE</td>
<td>Disabled</td>
</tr>
<tr>
<td>PMF dot1x</td>
<td>Disabled</td>
</tr>
<tr>
<td>PMF PSK</td>
<td>Disabled</td>
</tr>
<tr>
<td>SAE</td>
<td>Disabled</td>
</tr>
<tr>
<td>OWE</td>
<td>Disabled</td>
</tr>
<tr>
<td>SUITEB-1X</td>
<td>Disabled</td>
</tr>
<tr>
<td>SUITEB192-1X</td>
<td>Disabled</td>
</tr>
<tr>
<td>CCKM TSF Tolerance</td>
<td>1000</td>
</tr>
<tr>
<td>FT Support</td>
<td>Adaptive</td>
</tr>
<tr>
<td>FT Reassociation Timeout</td>
<td>20</td>
</tr>
<tr>
<td>FT Over-The-DS mode</td>
<td>Enabled</td>
</tr>
<tr>
<td>PMF Support</td>
<td>Disabled</td>
</tr>
<tr>
<td>PMF Association Comeback Timeout</td>
<td>1</td>
</tr>
<tr>
<td>PMF SA Query Time</td>
<td>200</td>
</tr>
<tr>
<td>Web Based Authentication</td>
<td>Disabled</td>
</tr>
<tr>
<td>Conditional Web Redirect</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
To view the WLAN details, use the following command:

```
Device# show run wlan
wlan wlan_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 023456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123
Multiple Authentications for a Client

- Information About Multiple Authentications for a Client, on page 731
- Information About Supported Combination of Authentications for a Given Client, on page 731
- Configuring Multiple Authentication for a Client, on page 732
- Verifying Multiple Authentication Configurations, on page 736

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. For information on guest clients, see Configure Guest Access Using Different Security Methods.

Information About Supported Combination of Authentications for a Given Client

Multiple authentication feature supports multiple combination of authentications for a given client configured in the WLAN profile.

The following table outlines the supported combination of authentications:

<table>
<thead>
<tr>
<th>Layer 2</th>
<th>Layer 3</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAB</td>
<td>CWA</td>
<td>Yes</td>
</tr>
<tr>
<td>MAB</td>
<td>LWA</td>
<td>Yes</td>
</tr>
<tr>
<td>MAB + PSK</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>Configuration</td>
<td>Method</td>
<td>Result</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>MAB + 802.1X</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>MAB Failure</td>
<td>LWA</td>
<td>Yes</td>
</tr>
<tr>
<td>802.1X</td>
<td>CWA</td>
<td>Yes</td>
</tr>
<tr>
<td>802.1X</td>
<td>LWA</td>
<td>Yes</td>
</tr>
<tr>
<td>PSK</td>
<td>LWA</td>
<td>Yes</td>
</tr>
<tr>
<td>PSK</td>
<td>CWA</td>
<td>Yes</td>
</tr>
<tr>
<td>iPSK + MAB</td>
<td>CWA</td>
<td>Yes</td>
</tr>
</tbody>
</table>

From 16.10.1 onwards, 802.1X configurations on WLAN supports Web Authentication configurations with WPA or WPA2 configuration.

This feature also supports the following AP modes:

- Local
- FlexConnect
- Fabric

## Configuring Multiple Authentication for a Client

### Configuring WLAN for 802.1X and Local Web Authentication

#### Procedure

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

**Example:**

```
Device# configure terminal
```

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>wlan profile-name wlan-id SSID_Name</td>
<td>Enters WLAN configuration sub-mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Device(config)# wlan wlan-test 3
SSID_Name
```

- **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.

**Note**

If you have already configured this command, enter `wlan profile-name` command.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables security authentication list for dot1x security. The configuration is similar for all dot1x security WLANs.</td>
</tr>
<tr>
<td>security dot1x authentication-list auth-list-name</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# security dot1x authentication-list default</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables authentication list for dot1x security.</td>
</tr>
<tr>
<td>security web-auth authentication-list authenticate-list-name</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# security web-auth authentication-list default</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Maps the parameter map.</td>
</tr>
<tr>
<td>security web-auth parameter-map parameter-map-name</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# security web-auth parameter-map WLAN1_MAP</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Enables the WLAN.</td>
</tr>
<tr>
<td>no shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# no shutdown</td>
</tr>
</tbody>
</table>

### Configuring WLAN for Preshared Key (PSK) and Local Web Authentication

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters WLAN configuration sub-mode.</td>
</tr>
<tr>
<td>wlan profile-name wlan-id SSID_Name</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wlan wlan-test 3 ssid-test</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you have already configured this command, enter wlan profile-name command.</td>
</tr>
</tbody>
</table>
### Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication

#### Configuring WLAN

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wlan profile-name wlan-id SSID_Name</td>
<td>Enters WLAN configuration sub-mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wlan wlan-test 3 ssid-test</td>
<td></td>
</tr>
</tbody>
</table>

- **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.

---

### Configuring WLAN

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>no security wpa akm dot1x</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# no security wpa akm dot1x</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>security wpa akm psk set-key ascii/hex key</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# security wpa akm psk set-key ascii</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>security web-auth authentication-list authenticate-list-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# security web-auth authentication-list default</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>security web-auth parameter-map parameter-map-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# security web-auth parameter-map WLAN1_MAP</td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 3** | **no security wpa akm dot1x**
*Example:*  
Device(config-wlan)# no security wpa akm dot1x

- **Purpose:** Enables security AKM for dot1x.

| **Note** | If you have already configured this command, enter `wlan profile-name` command.

| **Step 4** | **security wpa akm psk set-key ascii/hex key**
*Example:*  
Device(config-wlan)# security wpa akm psk set-key ascii 0

- **Purpose:** Configures the PSK AKM shared key.

| **Step 5** | **mac-filtering list-name**
*Example:*  
Device(config-wlan)# mac-filtering ewlc-radius

- **Purpose:** Sets the MAC filtering parameters.

### Applying Policy Profile to a WLAN

#### Procedure

| Command or Action | Purpose |
--- | ---|
**Step 1** | **configure terminal**
*Example:*  
Device# configure terminal

- **Purpose:** Enters global configuration mode.

**Step 2** | **wireless profile policy policy-profile-name**
*Example:*  
Device(config)# wireless profile policy policy-iot

- **Purpose:** Configures the default policy profile.

**Step 3** | **aaa-override**
*Example:*  
Device(config-wireless-policy)# aaa override

- **Purpose:** Configures AAA override to apply policies coming from the AAA or ISE servers.

**Step 4** | **nac**
*Example:*  
Device(config-wireless-policy)# nac

- **Purpose:** Configures NAC in the policy profile.

**Step 5** | **no shutdown**
*Example:*  
Device(config-wireless-policy)# no shutdown

- **Purpose:** Shuts down the WLAN.
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
-------------------------------------------------------------------------------
0xa00000003 58ef.68b6.aa60 3 L3 Authentication

Device# show platform software wireless-client chassis active F0
ID MAC Address WLAN Client State AOM ID Status
-------------------------------------------------------------------------------
0xa00000003 58ef.68b6.aa60 3 L3 Authentication. 730.

Done
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
-----------------------------------------------
0xa000001 58ef.68b6.aa60  3   Run

Device# show platform software wireless-client chassis active f0
ID   MAC Address   WLAN   Client State   AOM ID. Status
-----------------------------------------------
0xa000001 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 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   DP IDX   MAC Address   VLAN   CT   MCVL AS E   WLAN   POA
---------------------------------------------------------------------------------
0x49 0x0a000003 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_hdl   mac   Input Uidb   Output Uidb
-----------------------------------------------
50 0xa0000003 58ef.68b6.aa60  95929  95927
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.

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.

MTU Guidelines

CTS tagged packets greater than 1518 bytes may get dropped on the Cisco wireless controller. This is due to a restriction on the size of incoming packets on the UCS server, which is hosting Cisco wireless controller instances. The UCS server have a default MTU of 1500 thereby allowing packets of 1518 bytes only. Here, the additional 18 bytes includes 4 bytes of 802.1Q and 14 bytes of Ethernet header.
An Ethernet link configured for CTS tagging imposes an 8-byte encapsulation called Cisco metadata. As a result, the total size of the Ethernet packet is increased by 8 bytes to 1526 bytes (1518 + 8 = 1526). Hence, the MTU of the receiving interface has to be increased by 8-bytes to accommodate the additional 8 bytes in the Ethernet.

While CTS interfaces on the routers and switches (for example, Cisco ASR 1000 Series Routers, Cisco 4000 Series Integrated Services Routers, Cisco Catalyst 3000 Series Switches, Cisco Catalyst 9000 Series Switches) auto-adjusts MTU to 1508 bytes to accommodate additional 8-byte. However, other devices like UCS servers require manual update to increase the MTU to 1508. For information on how to configure jumbo MTU on UCS, see the following link:


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.

<table>
<thead>
<tr>
<th>Cisco TrustSec Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1AE Tagging (MACsec)</td>
<td>Protocol for IEEE 802.1AE-based wire-rate hop-to-hop Layer 2 encryption.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This feature is only available between TrustSec hardware-capable devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This feature is not supported on Catalyst 3850 and Catalyst 3650 switches with</td>
</tr>
<tr>
<td>Endpoint Admission Control (EAC)</td>
<td>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).</td>
</tr>
</tbody>
</table>
Cisco TrustSec Features

<table>
<thead>
<tr>
<th><strong>Cisco TrustSec Feature</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Device Admission Control (NDAC)</td>
<td>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.</td>
</tr>
<tr>
<td>Security Group Access Control List (SGACL)</td>
<td>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.</td>
</tr>
<tr>
<td>Cisco TrustSec SGACL High Availability</td>
<td>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.</td>
</tr>
<tr>
<td>Security Association Protocol (SAP)</td>
<td>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. <strong>Note</strong> This feature is not supported on Catalyst 3850 and Catalyst 3650 switches with</td>
</tr>
<tr>
<td>Security Group Tag (SGT)</td>
<td>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.</td>
</tr>
<tr>
<td>SGT Exchange Protocol (SXP)</td>
<td>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.</td>
</tr>
</tbody>
</table>

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, it downloads all the SGACLs in the matrix cells.

When a wireless client connects to the network, the client pushes all the ACLs to the controller.

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.

---

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wireless profile flex flex-profile</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>Device(config)# wireless profile flex xyz-flex-profile</code></td>
<td>Enables role-based access control enforcement for the AP.</td>
</tr>
<tr>
<td><strong>Step 3</strong> cts role-based enforcement  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;<code>Device(config-wireless-flex-profile)# cts role-based enforcement</code></td>
<td>Enables role-based access control enforcement for the AP.</td>
</tr>
<tr>
<td><strong>Step 4</strong> cts inline-tagging  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;<code>Device(config-wireless-flex-profile)# cts inline-tagging</code></td>
<td>Enables inline tagging on the AP.</td>
</tr>
<tr>
<td><strong>Step 5</strong> cts profile <em>profile-name</em>  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;<code>Device(config-wireless-flex-profile)# cts profile xyz-profile</code></td>
<td>Enables the CTS profile name.</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;<code>Device(config-wireless-flex-profile)# exit</code></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> wireless tag site <em>site-name</em>  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;<code>Device(config)# wireless tag site xyz-site</code></td>
<td>Configures a site tag and enters site tag configuration mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong> flex-profile <em>flex-profile-name</em>  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;<code>Device(config-site-tag)# flex-profile xyz-flex-profile</code></td>
<td>Configures a flex profile.</td>
</tr>
<tr>
<td><strong>Step 9</strong> exit  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;<code>Device(config-site-tag)# exit</code></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 10</strong> ap <em>mac-address</em>  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;<code>Device(config)# ap F866.F267.7DFB</code></td>
<td>Configures an AP and enters AP profile configuration mode.</td>
</tr>
<tr>
<td><strong>Step 11</strong> site-tag <em>site-tag-name</em>  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;<code>Device(config-ap-tag)# site-tag xyz-site</code></td>
<td>Maps a site tag to an AP.</td>
</tr>
</tbody>
</table>
What to do next

Use the `show cts ap sgt-info ap-name` command to verify the SGACL configuration on the AP.

### Configuring SGACL, Inline Tagging, and SGT in Local Mode

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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
  
  `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. |
| **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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
configure terminal

  **Example:**
  
  Device# configure terminal |
  
  Enters global configuration mode. |
<table>
<thead>
<tr>
<th>Step 2</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>radius server <em>server-name</em></td>
<td>Specifies the RADIUS server name.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# radius server Test-SERVER1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>address ipv4 <em>ip address</em></td>
<td>Specifies the primary RADIUS server parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-radius-server)# address ipv4 124.3.50.62</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>pac key <em>key</em></td>
<td>Specify the authentication and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-radius-server)# pac key cisco</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exit</td>
<td>Returns to the configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-radius-server)# exit</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa group server radius <em>server-group</em></td>
<td>Creates a radius server-group identification.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa group server radius authc-server-group</td>
<td>Note <em>server-group</em> refers to the server group name. The valid range is from 1 to 32 alphanumeric characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>cts authorization list <em>mlist-name</em></td>
<td>Creates a CTS authorization list.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# cts authorization list authc-list</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa authorization network <em>mlist-name</em> <em>group-name</em></td>
<td>Creates an authorization method list for web-based authorization.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa authorization network default group group1</td>
<td>Note Ensure that the ISE IP address configured on your controller is the same as the IP address configured on ISE (Work Center &gt; TrustSec &gt; Components &gt; Trustsec AAA Servers).</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Policy Profile Name</th>
<th>SGACL Enforcement</th>
<th>Inline-Tagging</th>
<th>Default-Sgt</th>
</tr>
</thead>
<tbody>
<tr>
<td>xyz-policy</td>
<td>DISABLED</td>
<td>ENABLED</td>
<td>0</td>
</tr>
<tr>
<td>wireless-policy1</td>
<td>DISABLED</td>
<td>DISABLED</td>
<td>0</td>
</tr>
<tr>
<td>w-policy-profile1</td>
<td>DISABLED</td>
<td>DISABLED</td>
<td>0</td>
</tr>
<tr>
<td>default-policy-profile</td>
<td>DISABLED</td>
<td>DISABLED</td>
<td>0</td>
</tr>
</tbody>
</table>

Flex Mode CTS Configuration

<table>
<thead>
<tr>
<th>Flex Profile Name</th>
<th>SGACL Enforcement</th>
<th>Inline-Tagging</th>
</tr>
</thead>
<tbody>
<tr>
<td>xyz-flex</td>
<td>DISABLED</td>
<td>ENABLED</td>
</tr>
<tr>
<td>demo-flex</td>
<td>DISABLED</td>
<td>DISABLED</td>
</tr>
<tr>
<td>flex-demo</td>
<td>DISABLED</td>
<td>DISABLED</td>
</tr>
<tr>
<td>xyz-flex-profile</td>
<td>DISABLED</td>
<td>DISABLED</td>
</tr>
<tr>
<td>default-flex-profile</td>
<td>DISABLED</td>
<td>DISABLED</td>
</tr>
</tbody>
</table>

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
Verifying Cisco TrustSec Configuration
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.


Creating an SXP Profile

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


**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>wireless profile flex flex-profile</td>
<td>Configures a wireless flex profile and enters the wireless flex profile configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless profile flex rr-xyz-flex-profile</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>cts inline-tagging</td>
<td>Enables inline-tagging on the AP.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-flex-profile)# cts inline-tagging</td>
<td></td>
</tr>
</tbody>
</table>

**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

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

Example:
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

<table>
<thead>
<tr>
<th>IP Address</th>
<th>SGT</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>100</td>
<td>CLI</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>IP Address</th>
<th>SGT</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>100</td>
<td>CLI</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>AP Inline Tagging Mode</th>
<th>Enabled</th>
</tr>
</thead>
</table>

! The status can be Enabled or Disabled and is based on the tag that is pushed to the AP.

AP Sgac Enforcement : Disabled
AP Override Status : Disabled

AP# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

<table>
<thead>
<tr>
<th>IP</th>
<th>SGT</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.3.74.101</td>
<td>17</td>
<td>LOCAL</td>
</tr>
</tbody>
</table>
Verifying SGT Push to Access Points

IP-SGT Active Bindings Summary

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of LOCAL bindings</td>
<td>1</td>
</tr>
<tr>
<td>Total number of active bindings</td>
<td>1</td>
</tr>
</tbody>
</table>

Active IPv6-SGT Bindings Information

<table>
<thead>
<tr>
<th>IP SGT SOURCE</th>
<th>LOCAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::c1d5:3da2:8c96:757d</td>
<td>17 LOCAL</td>
</tr>
</tbody>
</table>
Locally Significant Certificates

- Information About Locally Significant Certificates (LSC), on page 757
- Provisioning Locally Significant Certificates, on page 759
- Verifying LSC Configuration, on page 768
- Configuring Management TrustPoint to LSC (GUI), on page 768
- Configuring Management TrustPoint to LSC (CLI), on page 769

Information About Locally Significant Certificates (LSC)

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 APs and controllers. You can then use the certificates to mutually authenticate the controller and AP.

In Cisco controllers, you can configure the controller to use an LSC. You can use 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 Certificate Authority (CA) Server.

The LAP communicates with the controller using the CAPWAP protocol. Any requests 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 reachable.

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 Certificate Authority servers use to support certificate enrollment and revocation. It is widely used in Cisco and supported by many CA-Servers. In the SCEP protocol, 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 RA Public Key Distribution
- Certificate Enrollment
Certificate Provisioning on Controllers

The new LSC certificates, both CA and Device certificates must be installed on the controller.

With the SCEP protocol, the CA certificates are received from the CA server. During this point, there are no certificates in the controller, this is a clear Get Operation. These are installed on the controller. The same CA certificates are also pushed to the APs when the APs are provisioned with LSCs.

Preventing the Expiry of Manufacturing Installed Certificate

To prevent Manufacturing Installed Certificate (MIC) certificate-expiry failures, ensure that you configure a policy as shown below:

- Create a certificate map and add the rules.

```
configure terminal
crypto pki certificate map map1
issuer-name co Cisco Manufacturing CA
```

**Note** You can add more rules and filters under the same map. The rule mentioned in the above configuration specifies that any certificate whose issuer-name contains *Cisco Manufacturing CA* (case insensitive) is selected under this map.

- Use the certificate map under the trustpool policy.

```
configure terminal
crypto pki trustpool policy
match certificate map1 allow expired-certificate
```

Device Certificate Enrollment Operation

For both LAP and controller that requests 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 digitally signed by the PrivateKey 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 identity and verify if the request is unaltered. Many a times PKCS#10 is combined with other approaches, such as PKCS#7 to send and receive the certificate request or response.

Here, the PKCS#10 is wrapped in a PKCS#7 SignedData 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 CA and Device certificates are now 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 self-reboots. The next time it comes up, since 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.

**Note**

The LSC is supported on the controller and all Cisco Aironet Access Points.

Also, the LSC is enabled on the controller (GUI and CLI).

**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.

## Provisioning Locally Significant Certificates

### Configuring RSA Key for PKI Trustpoint

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>crypto key generate rsa exportable general-keys modulus (key_size) label RSA_key</td>
<td>Configures RSA key for PKI trustpoint.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# crypto key generate rsa exportable general-keys modulus 2048</td>
<td></td>
</tr>
<tr>
<td></td>
<td>label ewlc-tpl</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For the (key_size), enter the size of the key modulus. The valid range is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>from 360 to 4096.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For the RSA_key, enter the RSA key pair label.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
# Configuring PKI TrustPoint Parameters

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>crypto pki trustpoint trustpoint_name</code></td>
<td>Creates a new trust point for an external CA server. Here, <code>trustpoint_name</code> refers to the trustpoint name.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# crypto pki trustpoint</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>microsoft-ca</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>enrollment url HTTP_URL</code></td>
<td>Enrolls trustpoint using the trustpoint enrollment parameters.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(ca-trustpoint)# enrollment url</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>http://CA_server/certsrv/mscep/mscep.dll</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>subject-name subject_name</code></td>
<td>Creates subject name parameters for the trustpoint.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(ca-trustpoint)# subject-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>IN, ST=KA, L=Bengaluru, O=Cisco, CN=eagle-eye/emailAddress=support@abc.com</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>rsakeypair RSA_key key_size</code></td>
<td>Maps RSA key with that of the trustpoint.</td>
</tr>
<tr>
<td></td>
<td>• <code>RSA_key</code>—Refers to the RSA key pair label.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>key_size</code>—Refers to the signature key length. Range is from 360 to 4096.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(ca-trustpoint)# rsakeypair</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>ewlc-tp1</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>`revocation {crl</td>
<td>none</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(ca-trustpoint)# revocation</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>none</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(ca-trustpoint)# end</td>
<td></td>
</tr>
</tbody>
</table>
Authenticating and Enrolling the PKI TrustPoint with CA Server (GUI)

Procedure

Step 1  Choose Configuration > Security > PKI Management.
Step 2  In the Trustpoint section, click Add.
Step 3  Enter a trustpoint label and enrollment URL.
Step 4  Check the Authenticate check box to authenticate the trustpoint label.
Step 5  In the Subject Name section, enter the country code, state, location, organisation, domain name, and email address.
Step 6  Check the Key Generated check box to view the available RSA keypairs. You can choose from the Available RSA Keypairs drop-down list.
Step 7  Check the Enroll Trustpoint check box, and enter the password and confirm the same as well.
Step 8  Click Save & Apply to Device.

Authenticating and Enrolling the PKI TrustPoint with CA Server (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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:  
  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 | Enroll for client certificate. |
### Configuring AP Join Attempts with LSC Certificate (GUI)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**  
**password**  
**Example:**  
Device(config)# abcd123

**Step 6**  
**password**  
**Example:**  
Device(config)# abcd123

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

---

**Configuring AP Join Attempts with LSC Certificate (GUI)**

**Procedure**

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

**Step 2**  
On the **All Access Points** page, click the LSC Provision name.

**Step 3**  
Use the **Status** drop-down to enable LSC.
Configuring AP Join Attempts with LSC Certificate (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap lsc-provision join-attempt number_of_attempts</td>
<td>Specifies the number of AP join attempts with the newly provisioned LSC certificate.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# ap lsc-provision join-attempt 10</td>
<td>When the number of AP joins exceed the specified limit, AP joins back with the MIC certificate.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# end</td>
<td>Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>

Configuring Subject-Name Parameters in LSC Certificate

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> 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</td>
<td>Specifies the attributes to be included in the subject-name of the certificate request generated by an AP.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# ap lsc-provision subject-name-parameter country India state Karnataka city Bangalore domain domain1 org Right email-address <a href="mailto:adc@gfe.com">adc@gfe.com</a></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Key Size for LSC Certificate

**Procedure**

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

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>ap lsc-provision key-size {1024</td>
<td>2048}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap lsc-provision key-size 1024</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring TrustPoint for LSC Provisioning on Access Point

**Procedure**

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

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>ap lsc-provision trustpoint tp-name</td>
<td>Specifies the trustpoint with which the LCS is provisioned to AP. Here, tp-name refers to the trustpoint name.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap lsc-provision trustpoint microsoft-ca</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring AP LSC Provision List (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configuration &gt; Wireless &gt; Access Points</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the <strong>All Access Points</strong> page, click the LSC Provision name.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Use the <strong>Status</strong> drop-down to enable LSC.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Use the <strong>Trustpoint Name</strong> drop-down to search or select the trustpoint.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the <strong>Number of Join Attempts</strong> field, enter the retry attempts.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Use the <strong>Key Size</strong> drop-down to select the key.</td>
</tr>
<tr>
<td>Step 8</td>
<td>In the <strong>Edit AP Join Profile</strong> window, click the <strong>CAPWAP</strong> tab.</td>
</tr>
<tr>
<td>Step 9</td>
<td>In the <strong>Add APs to LSC Provision List</strong> section, use the <strong>Select File</strong> option to upload a CSV file that contains AP details. After selecting the file, click <strong>Upload File</strong>.</td>
</tr>
<tr>
<td>Step 10</td>
<td>You can also use the <strong>AP MAC Address</strong> field to search for APs using the MAC address and add them. The APs added to the provision list are displayed in the <strong>APs in provision List</strong> list-box.</td>
</tr>
</tbody>
</table>
| Step 11 | In the **Subject Name Parameters** section, enter the following details:  
  - Country  
  - State  
  - City  
  - Organisation  
  - Department  
  - Email Address  |
| Step 12 | Click **Apply**. |

Configuring AP LSC Provision List (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**        | **configure terminal**  
  **Example:**  
  Device# configure terminal |
| **Step 2**        | **[no] ap lsc-provision mac-address mac-addr**  
  **Example:** |

Enters global configuration mode.  
Adds the access point to the LSC provision list.
### Configuring LSC Provisioning for all Access Points (GUI)

#### Procedure

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

**Step 2**  On the **Access Points** page, expand the **LSC Provision** section.

**Step 3**  Set the **Status** to **Enabled** state.

If you set the **Status** to **Provision List**, the LSC provisioning will be configured only for APs that are part of the provision list.

**Step 4**  From the **Trustpoint Name** drop-down list, select 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, select the appropriate key size of the certificate from the following options:

- 2048
- 3072
- 4096

**Step 7**  In the **Add APs to LSC Provision List** section, click **Select File** option to upload a CSV file that contains the AP details. After selecting the file, click **Upload File**.

**Step 8**  In the **AP MAC Address** field, enter the AP MAC address to search for APs and add them. The APs added to the provision list are displayed in the **APs in Provision List** section.

**Step 9**  In the **Subject Name Parameters** section, enter the following details:

- **a.** Country
- **b.** State
- **c.** City
- **d.** Organization
- **e.** Department
Configuring LSC Provisioning for all Access Points (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>no ap lsc-provision</td>
<td>Enables LSC provisioning for all access points.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# no ap lsc-provision</td>
<td>By default, the LSC provisioning is disabled for all APs.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# end</td>
<td>Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>

Configuring LSC Provisioning for Access Points in Provision List

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ap lsc-provision provision-list</td>
<td>Enables LSC provisioning for a set of access points configured in the provision list.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ap lsc-provision provision-list</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# end</td>
<td>Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>
Verifying LSC Configuration

To view 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 the Enable Trust Point field to Enabled state.
Step 3 From the Trust Points drop-down list, choose the appropriate trust point.
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, removing the AP LSC provisioning, the APs will reboot and join at non-LSC mode.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless management trustpoint</td>
<td>Configures the management trustpoint to LSC.</td>
</tr>
<tr>
<td></td>
<td>trustpoint_name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>trustpoint microsoft-ca</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Management TrustPoint to LSC (CLI)
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 whitelist and blacklist entries.
- Supports custom parameter-type Umbrella profiles. One Global profile and 15 custom profiles are supported.
• Although IPv6 is supported, device registration will always be over IPv4. There is no support of device registration over IPv6.
• The communication from device to the Umbrella Cloud can be done over IPv6 also.
• In the Flexconnect mode, DNS handling takes place in the AP instead of the controller. Multiple profiles are supported in the Flex mode.

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. 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Perform either of the following tasks:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• crypto pki trustpool import url</td>
<td>Imports the root certificate directly from</td>
</tr>
</tbody>
</table>
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.

  ```
  -----BEGIN CERTIFICATE-----
  MIIEldCCA3ygAwIBAgIQAf2j627KdciIQ4ty58+8kt
  .
  .
  .
  j6tJLp07kzQoH3j0l0rHvdPjBzeXDLz
  -----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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>parameter-map type regex</code></td>
<td>Creates a regex parameter map.</td>
</tr>
<tr>
<td><code>parameter-map-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# parameter-map type regex</td>
<td></td>
</tr>
<tr>
<td>dns_wl</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

Step 3

**pattern regex-pattern**

**Example:**

Device(config-profile)# pattern www.google.com

Configures the regex pattern to match.

**Note**

The following patterns are supported:

- Begins with . *. For example: . *facebook.com
- Begins with . * and ends with *. For example: . *google*
- 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. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

---

### Configuring Umbrella Parameter Map (GUI)

#### Procedure

**Step 1**

Choose **Configuration > Security > Threat Defense**.

**Step 2**

Click **Cisco Umbrella Integration**.

**Step 3**

Enter a name for the parameter map in the **Umbrella Parameter Map**.

**Step 4**

Click the **Apply** button.

To delete all umbrella configurations, click the **Unconfigure Umbrella** button.
## Configuring the Umbrella Parameter Map

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | configure terminal | Enters global configuration mode.  
**Example:**  
Device# configure terminal |
| Step 2 | parameter-map type umbrella global | Creates an umbrella global parameter map.  
**Example:**  
Device(config)# parameter-map type umbrella global |
| Step 3 | token token-value | Configures an umbrella token.  
**Example:**  
Device(config-profile)# token 5XXXXXXXXCXXXXXXXAXXXXXXXFXXXXCXXXXXXXX |
| Step 4 | local-domain regex-parameter-map-name | Configures local domain RegEx parameter map.  
**Example:**  
Device(config-profile)# local-domain dns_wl |
| Step 5 | resolver {IPv4 X.X.X.X | IPv6 X::X::X::X} | Configures the Anycast address. The default address is applied when there is no specific address configured.  
**Example:**  
Device(config-profile)# resolver IPv6 10::1:1:1 |
| Step 6 | end | Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.  
**Example:**  
Device(config-profile)# end |

### Enabling or Disabling DNScrypt

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | configure terminal | Enters global configuration mode.  
**Example:**  
Device# configure terminal |
| Step 2 | parameter-map type umbrella global | Creates an umbrella global parameter map.  
**Example:**  
Device(config)# parameter-map type umbrella global |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# <code>parameter-map type umbrella global</code></td>
<td>Enables or disables DNScrypt. By default, the DNScrypt option is enabled.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td><code>[no] dnscrypt</code></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Device(config-profile)# <code>no dnscrypt</code></td>
<td>Device(config-profile)# <code>end</code></td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>

### Configuring Timeout for UDP Sessions

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# <code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>parameter-map type umbrella global</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>parameter-map type umbrella global</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>udp-timeout timeout_value</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-profile)# <code>udp-timeout 2</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-profile)# <code>end</code></td>
</tr>
<tr>
<td></td>
<td>Configures timeout value for UDP sessions. The <code>timeout_value</code> ranges from 1 to 30 seconds. <strong>Note</strong> The public-key and resolver parameter-map options are automatically populated with the default values. So, you need not change them.</td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>
# Configuring Parameter Map Name in WLAN

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless profile policy profile-name</td>
<td>Creates policy profile for the WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# wireless profile policy</td>
<td>The profile-name is the profile name of the</td>
</tr>
<tr>
<td></td>
<td>default-policy-profile</td>
<td>policy profile.</td>
</tr>
<tr>
<td>Step 3</td>
<td>umbrella-param-map umbrella-name</td>
<td>Configures the Umbrella OpenDNS feature for</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)#</td>
<td>the WLAN.</td>
</tr>
<tr>
<td></td>
<td>umbrella-param-map global</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)# end</td>
<td></td>
</tr>
</tbody>
</table>

## Configuring the Umbrella Flex Profile

## Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless profile flex flex-profile-name</td>
<td>Creates a new flex policy. Enters the flex profile configuration mode. The flex-profile-name is the flex profile name.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# wireless profile flex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>default-flex-profile</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>umbrella-profile umbrella-profile-name</td>
<td>Configures the Umbrella flex feature. Use the no form of this command to negate the command or to set the command to its default.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-flex-profile)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>umbrella-profile global</td>
<td></td>
</tr>
</tbody>
</table>
Configuring the Umbrella Flex Profile (GUI)

Procedure

Step 1  Choose Configuration > Tags & Profiles > Flex.
Step 2  Click a Flex Profile Name. The Edit Flex Profile dialog box appears.
Step 3  Under the Umbrella tab, click the Add button.
Step 4  Select a name for the parameter map from the Parameter Map Name drop-down list and click Save.
Step 5  Click the Update & Apply to Device button. The configuration changes are successfully applied.

Configuring Umbrella Flex Parameters

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>wireless profile policy profile-policy-name</td>
<td>Configures the WLAN policy profile. Enters the wireless policy profile configuration mode. The policy-profile-name is the WLAN policy profile name.</td>
</tr>
<tr>
<td>flex umbrella dhcp-dns-option</td>
<td>Configures the Umbrella DHCP option for DNS. By default the option is enabled.</td>
</tr>
<tr>
<td>flex umbrella mode {force</td>
<td>ignore}</td>
</tr>
</tbody>
</table>
### Configuring the Umbrella Flex Policy Profile (GUI)

**Procedure**

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

**Step 2** Click the Add button. The Add Policy Profile dialog box appears.

**Step 3** In the Advanced tab, and under the Umbrella section, complete the following:

a) Select the parameter map from the Umbrella Parameter Map drop-down list. Click the Clear hyperlink to clear the selection.

b) Click the field adjacent to Flex DHCP Option for DNS to Disable the option. By default it is Enabled.

c) Click the field adjacent to DNS Traffic Redirect to set the option to Force. By default it is set to Ignore.

**Step 4** Click the Apply to Device button.

### Verifying the Cisco Umbrella Configuration

To view the Umbrella configuration details, use the following command:

```
Device# show umbrella config
Umbrella Configuration
------------------------
Token: 5XXXXXXABXXXXXFXXXXXXXXXXXXABXX
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 device registration details, use the following command:

```
Device# show umbrella deviceid
Device registration details
Param-Map Name  Status  Device-id
global         200 SUCCESS 010aa4eXXXXXXX8d
vj-1           200 SUCCESS 01XXXXXXXf4541e1
GUEST          200 SUCCESS 01a4f6XXXXXXXX42
EMP            200 SUCCESS 0XXXXXXXd106ecd
```
To view the detailed description for the Umbrella device ID, use the following command:

```
Device# show umbrella deviceid detailed
```

Device registration details

```
1.global
Tag : global
Device-id : 010aa4eXXXXXXX8d
Description : Device Id received successfully
WAN interface : None
2.vj-1
Tag : vj-1
Device-id : 01XXXXXXXf4541e1
Description : Device Id received successfully
WAN interface : None
```

To view the Umbrella DNSCrypt details, use the following command:

```
Device# show umbrella dnscrypt
DNSCrypt: Enabled
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 wireless policy profile Umbrella configuration, use the following command:

```
Device#show wireless profile policy detailed vj-pol-profile | s Umbrella
Umbrella information
Cisco Umbrella Parameter Map : vj-2
DHCP DNS Option : ENABLED
Mode : force
```

To view the wireless flex profile Umbrella configuration, use the following command:

```
Device#show wireless flex detailed vj-flex-profile | s Umbrella
Umbrella Profiles :
vj-1
vj-2
global
```

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
...
Verifying the Cisco Umbrella Configuration

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#
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.

For more information about FIPS, see


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.

**Limitations for FIPS**

- The console of APs get disabled when the controller is operating in FIPS mode.

**Note**

We recommend a minimum RSA key size of 2048 bits under RADSEC when operating in FIPS mode. Otherwise, the RADSEC fails.
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).

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> fips authorization-key key</td>
<td>The key length should be of 32 hexadecimal</td>
</tr>
<tr>
<td>Example:</td>
<td>characters.</td>
</tr>
<tr>
<td>Device(config)# fips authorization-key</td>
<td></td>
</tr>
<tr>
<td>12345678901234567890123456789012</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### What to do next

You must now reboot the controller to enable FIPS mode.

### Verifying FIPS Configuration

You can verify FIPS configuration using the following commands:

Use the following `show` command to display the installed authorization key:

```
Device# show fips authorization-key
FIPS: Stored key (16) : 12345678901234567890123456789012
```

Use the following `show` command to display the status of FIPS on the device:

```
Device# show fips status
Chassis is running in fips mode
```
Device Ecosystem

- Device Analytics, on page 787
- Adaptive 802.11r, on page 790

Device Analytics

Information About Device Analytics

The device analytics feature enhances the enterprise Wi-Fi experience for client devices to ensure seamless connectivity. This feature provides a set of data analytics tools for analysing wireless client device behaviour. With device profiling enabled on the controller, information is exchanged between the client device and the controller and AP. This data is encrypted using AES-256-CBC to ensure device security. This is applicable for Cisco device ecosystem partners only.

Note

From 17.1.1 release onwards, the device analytics feature is applicable to Samsung partner.

Restrictions for Device Analytics

- Device analytics is only supported by the 802.11ax and Wave 2 APs.
- Device analytics is only supported using central authentication in either local mode or flex mode.

Configuring Device Analytics (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 Advanced tab.
Step 4 In the Device Analytics section, select the Advertise Support check box.
### Configuring Device Analytics (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>wlan wlan-name wlan-id SSID-name</code></td>
<td>Enters the WLAN configuration sub-mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>wlan samsung_analytics 1 samsung_analytics</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>wlan-name</code>—Enter the profile name. The range is from 1 to 32 alphanumeric characters.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>wlan-id</code>—Enter the WLAN ID. The range is from 1 to 512.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>SSID-name</code>—Enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you have already configured WLAN, enter <code>wlan wlan-name</code> command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>[no] device-analytics</code></td>
<td>This is enabled by default. Enables or disables device analytics. WLANs advertise analytics capability in beacons &amp; probe responses.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>[no] device-analytics</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>[no] device-analytics [export]</code></td>
<td>When <code>export</code> option is set, the information from Cisco devices are shared with compatible clients (such as, Samsung devices). Here, information from Cisco devices refer to the Cisco controller details, AP version, and model number.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>[no] device-analytics export</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <code>Ctrl-Z</code> to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>
Verifying Multiple Device Analytics Configurations

To view the status of device analytics export, use the following command:

```
Device# show wlan 1 test-wlan
```

WLAN Profile Name : test-wlan

```
Identifier : 1
Description :
Network Name (SSID) : test-open-ssid
Status : Enabled
Broadcast SSID : Enabled
Advertise-Apname : Disabled
Universal AP Admin : Disabled
Device Analytics
Advertise Support : Enabled
Share Data with Client : Disabled
```

To view client device information, use the following command:

```
Device# show device classifier mac-address 0040.96ae.53b4 detail
```

Client Mac: 0040.96ae.53b4
Device Type: Samsung Galaxy S10e(Phone)
Confidence Level: 40
Device Name: android-dhcp-9
Software Version(Carrier Code): SD7(TMB)
Device OS: Android 9
Device Vendor: android-dhcp-9
Country: US

```
Device# show device classifier mac-address 0040.96ae.53b4 detail
```

Client MAC Address : 1098.c37b.af4e
Client IPv4 Address : 12.1.0.7
Client IPv6 Addresses : fe80::6200:353d:8832:fa41
Client Username: N/A
AP MAC Address : 7872.5dee.b5e0
AP Name: AP4C77.6D9E.61B2
AP slot : 0
Client State : Associated

To view the last disconnect reason, use the following command:

```
Device# show device classifier mac-address 0040.96ae.53b4 detail
```

Client MAC Address : 009d.6bf2.d616
Client IPv4 Address : 12.1.0.52
Client IPv6 Addresses : fe80::631b:5b4f:f9b6:53cc
Client Username: N/A
AP MAC Address : 7069.5a51.53c0
AP Name: AP4C77.6D9E.61B2
AP slot : 1
Client State : Associated

Assisted Roaming Neighbor List
Nearby AP Statistics:
EoGRE : No/Simple client
Last Disconnect Reason : User initiated disconnection - Device was powered off or Wi-Fi
Adaptive 802.11r

Information About Adaptive 802.11r

The Cisco device ecosystem partner now supports 11r functionality on an adaptive 802.11r SSID. Samsung is one of the partners.

Note

The Adaptive 802.11r is enabled by default. This means that when you create a WLAN, the adaptive 802.11r is configured by default.

Client device information such as its model number, supported operating system is shared with the controller and AP while the device receives information such as controller and AP type, software release, etc. Also, this enables 802.11r-compatible devices to benefit from adaptive 802.11r on Cisco networks. This ecosystem comes handy especially for troubleshooting device disconnection from the AP as the controller receives information such as the disconnect reason code from the client device.

Note

Devices without 11r support cannot join an SSID where 11r is enabled.

To use the 11r functionality on devices, you need to create a separate SSID with 11r enabled and another with 11r disabled to support the non-11r devices in the network.

Configuring Adaptive 802.11r (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Tags &amp; Profiles &gt; WLANs.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the WLANs page, click the name of the WLAN.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Edit WLAN window, click the Security &gt; Layer2 tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the WPA Parameters section and Fast Transition drop-down list, choose Adaptive Enabled.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Update &amp; Apply to Device.</td>
</tr>
</tbody>
</table>

Verifying Adaptive 802.11r

To view the details, use the following command:

Device# show running-config all
wlan test-psk 2 test-psk
security ft adaptive
"adaptive" is optional

The following command is used to enable or disable adaptive 11r:

```
[no] security ft adaptive
```

The following command is used to enable or disable 802.11r:

```
[no] security ft
```
Verifying Adaptive 802.11r
Adaptive WIPS

- Information About Adaptive WIPS, on page 793
- aWIPS in a Cisco Catalyst Wireless Controller environment, on page 793
- Supported Modes and Platforms, on page 794
- Prerequisites for Adaptive WIPS, on page 794
- Configuring Adaptive WIPS (GUI), on page 795
- Viewing Adaptive WIPS Alarms (GUI), on page 795
- Enabling Adaptive WIPS, on page 795
- Verifying Adaptive WIPS, on page 796

Information About Adaptive WIPS

The Cisco Adaptive Wireless Intrusion Prevention System (aWIPS) is a wireless intrusion threat detection and mitigation mechanism. aWIPS uses an advanced approach to wireless threat detection and performance management. The AP detects the threats and generates alarms. It combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention.

With a fully infrastructure-integrated solution, you can continually monitor wireless traffic on both the wired and wireless networks and use that network intelligence to analyze attacks from many sources to accurately pinpoint and proactively prevent attacks, rather than wait until damage or exposure has occurred.

aWIPS in a Cisco Catalyst Wireless Controller environment

The aWIPS solution comprises the following components:

- Cisco Catalyst 9800 Series Wireless Controller
- Cisco Catalyst and Aironet Wave 2 APs
- Cisco DNA Center

As the aWIPS functionality is integrated into the Cisco DNA Center, the aWIPS can configure and monitor WIPS policies and alarms and report threats.

aWIPS supports the following capabilities:

- Static signatures
• Standalone signature detection only
• Alarms only
• GUI support
• Controller commands to view alarms
• Static signature file packaged with controller and AP image
• Export alarms to Cisco DNA Center through WSA channel

aWIPS alarm details like the AP MAC address, alarm ID, client MAC address, alarm string, and signature ID are displayed on the Cisco Catalyst 9800 series wireless controller GUI.

**Supported Modes and Platforms**

The following Cisco Catalyst Wireless controllers support aWIPS:
• Cisco Catalyst 9800-CL cloud wireless controller
• Cisco Catalyst 9800 series wireless controller
• Cisco Catalyst 9300 series wireless controller
• Cisco Catalyst 9400 series wireless controller
• Cisco Catalyst 9500 and 9500H series wireless controller
• Cisco Catalyst 9600 series wireless controller
• Cisco Embedded Wireless Controller on Catalyst Access Points

The list of controller modes supported are listed below:
• Local
• Flex
• Fabric
• Cisco Embedded Wireless Controller on Catalyst Access Points

Both Cisco Catalyst Series APs (802.11ax) and Cisco Aironet Series APs support aWIPS. The AP modes that are supported include:
• Local
• Monitor
• Flex

**Prerequisites for Adaptive WIPS**

Set all entities (controller and APs) in an aWIPS deployment to the UTC time zone.
Configuring Adaptive WIPS (GUI)

aWIPS initialization is done by the controller. This could be triggered by Cisco DNA Center via the GUI, which then sends the configuration to the controller via Netconf or Yang. aWIPS initialization could also be triggered via the controller GUI or CLI. The controller then sends the aWIPS configuration to the APs using CAPWAP.

Procedure

Step 1 Choose Configuration > Tags & Profiles > AP Join.
Step 2 On the AP Join page, click the name of the desired AP join profile.
Step 3 In the Edit AP Join Profile window, click the Security tab.
Step 4 In the aWIPS section, select the aWIPS Enable check box.
Step 5 (Optional) In the aWIPS section, you can also select the Forensic Enable check box.
Step 6 Click Update & Apply to Device.

Viewing Adaptive WIPS Alarms (GUI)

The various aWIPS alarms and statistics for the last 5 minutes are displayed on the controller GUI.

Procedure

Step 1 Choose Configuration > Tags & Profiles > AP Join.
Step 2 On the AP Join page, click the default-ap-profile AP join profile.
Step 3 In the Edit AP Join Profile window, click the AP tab.
Step 4 Under Hyperlocation, select the Enable Hyperlocation check box.
Step 5 Click Update & Apply to Device.

Enabling Adaptive WIPS

Before you begin
### Verifying Adaptive WIPS

#### Example

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Example:</td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

- 

**Verifying Adaptive WIPS**
Simultaneous Authentication of Equals

WPA3 is the latest version of Wi-Fi Protected Access (WPA), which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks.

WPA3 leverages Simultaneous Authentication of Equals (SAE) to provide stronger protections for users against password guessing attempts by third parties. SAE employs a discrete logarithm cryptography to perform an efficient exchange in a way that performs mutual authentication using a password that is probably resistant to an offline dictionary attack. An offline dictionary attack is where an adversary attempts to determine a network password by trying possible passwords without further network interaction.

WPA3-Personal brings better protection to individual users by providing more robust password-based authentication making the brute-force dictionary attack much more difficult and time-consuming, while WPA3-Enterprise provides higher grade security protocols for sensitive data networks.

When the client connects to the access point, they perform an SAE exchange. If successful, they will each create a cryptographically strong key, from which the session key will be derived. Basically a client and access point goes into phases of commit and then confirm. Once there is a commitment, the client and access point can then go into the confirm states each time there is a session key to be generated. The method uses forward secrecy, where an intruder could crack a single key, but not all of the other keys.

Opportunistic Wireless Encryption

Opportunistic Wireless Encryption (OWE) is an extension to IEEE 802.11 that provides encryption of the wireless medium. The purpose of OWE based authentication is to avoid open unsecured wireless connectivity.
between the AP’s and clients. The OWE uses the Diffie-Hellman algorithms based Cryptography to setup the wireless encryption. With OWE, the client and AP perform a Diffie-Hellman key exchange during the access procedure and use the resulting pairwise secret with the 4-way handshake. The use of OWE enhances wireless network security for deployments where Open or shared PSK based networks are deployed.

### Configuring WPA3 SAE

Follow the procedure given below to configure WPA3 SAE.

**Before you begin**
Configure PMF internally. The associated ciphers configuration can use the WPA2 ciphers.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wlan wlan-name wlan-id SSID-name</td>
<td>Enters the WLAN configuration sub-mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wlan WPA3 1 WPA3</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>no security wpa akm dot1x</td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# no security wpa akm dot1x</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>no security ft over-the-ds</td>
<td>Disables fast transition over the data source on the WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# no security ft over-the-ds</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>no security ft</td>
<td>Disables 802.11r fast transition on the WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# no security ft</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>no security wpa wpa2</td>
<td>Disables WPA2 security. PMF is disabled now.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# no security wpa wpa2</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>security wpa wpa2 ciphers aes</td>
<td>Configures WPA2 cipher.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring SAE (WPA3+WPA2 Mixed Mode)

Follow the procedure given below to configure WPA3+WPA2 mixed mode for SAE.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-wlan)# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

---

### Configuring WPA3

1. **Purpose**: Enables WPA3 support.
2. **Example**: Device(config-wlan)# security wpa wpa3
3. **Note**: If both WPA2 and WPA3 are supported (SAE and PSK together), it is optional to configure PMF. However, you cannot disable PMF. For WPA3, PMF is mandatory.

---

### Configuring PSK

1. **Purpose**: Specifies a preshared key.
2. **Example**: Device(config-wlan)# security wpa psk set-key ascii value preshared-key

---

### Configuring PMF

1. **Purpose**: Enables PMF.
2. **Example**: Device(config-wlan)# security wpa wpa3

---

### Configuring AKM SAE

1. **Purpose**: Enables AKM SAE support.
2. **Example**: Device(config-wlan)# security wpa akm sae

---

### Configuring WLAN

1. **Purpose**: Enables the WLAN.
2. **Example**: Device(config-wlan)# no shutdown

---

### Configuring EXEC mode

1. **Purpose**: Returns to the privileged EXEC mode.
2. **Example**: Device(config-wlan)# end
<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>wlan wlan-name wlan-id SSID-name</td>
<td>Enters the WLAN configuration sub-mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wlan WPA3 1 WPA3</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>no security wpa akm dot1x</td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# no security wpa akm dot1x</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>no security ft over-the-ds</td>
<td>Disables fast transition over the data source on the WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# no security ft over-the-ds</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>no security ft</td>
<td>Disables 802.11r fast transition on the WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# no security ft</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>security wpa wpa2 ciphers aes</td>
<td>Configures WPA2 cipher.</td>
</tr>
<tr>
<td>Note:</td>
<td>You can check whether cipher is configured using no security wpa wpa2 ciphers aes command. If cipher is not reset, configure the cipher.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# security wpa wpa2 ciphers aes</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>security wpa psk set-key ascii value preshared-key</td>
<td>Specifies a preshared key.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>security wpa wpa3</td>
<td>Enables WPA3 support.</td>
</tr>
<tr>
<td>Note:</td>
<td>If both WPA2 and WPA3 are supported (SAE and PSK together), it is optional to configure PMF. However, you cannot disable PMF. For WPA3, PMF is mandatory.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# security wpa wpa3</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>security wpa akm sae</td>
<td>Enables AKM SAE support.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# security wpa akm sae</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>security wpa akm psk</td>
<td>Enables AKM PSK support.</td>
</tr>
</tbody>
</table>
Configuring WPA3 Enterprise

Follow the procedure given below to configure WPA3 enterprise.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device# configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>wlan wlan-name wlan-id SSID-name</td>
<td>Enters the WLAN configuration sub-mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config)# wlan wl-dot1x 4 wl-dot1x</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>no security wpa akm dot1x</td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config-wlan)# no security wpa akm dot1x</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>no security wpa wpa2</td>
<td>Disables WPA2 security.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config-wlan)# no security wpa wpa2</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>security wpa akm dot1x-sha256</td>
<td>Configures 802.1x support.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config-wlan)# security wpa akm dot1x-sha256</strong></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>security wpa wpa3</td>
<td>Enables WPA3 support.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config-wlan)# security wpa wpa3</strong></td>
</tr>
</tbody>
</table>
### Configuring the WPA3 OWE

Follow the procedure given below to configure WPA3 OWE.

**Before you begin**

Configure PMF internally. The associated ciphers configuration can use the WPA2 ciphers.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wlan wlan-name wlan-id SSID-name</td>
<td>Enters the WLAN configuration sub-mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wlan WPA3 1 WPA3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>no security ft over-the-ds</td>
<td>Disables fast transition over the data source on the WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# no security ft over-the-ds</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>no security ft</td>
<td>Disables 802.11r fast transition on the WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# no security ft</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>no security wpa akm dot1x</td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# no security wpa akm dot1x</td>
<td>Disables WPA2 security. PMF is disabled now.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>no security wpa wpa2</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# no security wpa wpa2</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>security wpa wpa2 ciphers aes</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# security wpa wpa2 ciphers aes</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>security wpa wpa3</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# security wpa wpa3</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>security wpa akm owe</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# security wpa akm owe</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>no shutdown</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# no shutdown</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring WPA3 OWE Transition Mode

Follow the procedure given below to configure the WPA3 OWE transition mode.

**Note**

Policy validation is not done between open WLAN and OWE WLAN. The operator is expected to configure them appropriately.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>2</td>
<td><code>wlan wlan-name wlan-id SSID-name</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# wlan WPA3 1 WPA3</td>
</tr>
<tr>
<td>3</td>
<td><code>no security wpa akm dot1x</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-wlan)# no security wpa akm dot1x</td>
</tr>
<tr>
<td>4</td>
<td><code>no security ft over-the-ds</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-wlan)# no security ft over-the-ds</td>
</tr>
<tr>
<td>5</td>
<td><code>no security ft</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-wlan)# no security ft</td>
</tr>
<tr>
<td>6</td>
<td><code>no security wpa wpa2</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-wlan)# no security wpa wpa2</td>
</tr>
<tr>
<td>7</td>
<td><code>security wpa wpa2 ciphers aes</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-wlan)# security wpa wpa2 ciphers aes</td>
</tr>
<tr>
<td>8</td>
<td><code>security wpa wpa3</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-wlan)# security wpa wpa3</td>
</tr>
<tr>
<td>9</td>
<td><code>security wpa akm owe</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-wlan)# security wpa akm owe</td>
</tr>
<tr>
<td>10</td>
<td><code>security wpa transition-mode-wlan-id wlan-id</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
</tbody>
</table>
**Purpose**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-wlan)# security wpa transition-mode-wlan-id 1</td>
<td>Validation is not performed on the transition mode WLAN. The operator is expected to configure it correctly with OWE WLAN having open WLAN identifier and the opposite way. You should configure OWE WLAN ID as transition mode WLAN in open WLAN. Similarly, open WLAN should be configured as transition mode WLAN in OWE WLAN configuration.</td>
</tr>
</tbody>
</table>

**Step 11**

**Command or Action:**

no shutdown

**Example:**

Device(config-wlan)# no shutdown

**Purpose:** Enables the WLAN.

**Step 12**

**Command or Action:**

end

**Example:**

Device(config-wlan)# end

**Purpose:** Returns to the privileged EXEC mode.

---

**Configuring Anti-Clogging and SAE Retransmission**

Follow the procedure given below to configure anti-clogging and SAE retransmission.

---

**Note**

If the simultaneous SAE ongoing sessions are more than the configured anti-clogging threshold, then anti-clogging mechanism is triggered.

---

**Before you begin**

Ensure that SAE WLAN configuration is in place, as the steps given below are incremental in nature, in addition to the SAE WLAN configuration.

---

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wlan wlan-name wlan-id SSID-name</td>
<td>Enters the WLAN configuration sub-mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>Device(config)# wlan WPA3 1 WPA3</code></td>
<td>Enables simultaneous authentication of equals as a security protocol.</td>
</tr>
<tr>
<td><strong>Step 3</strong> shutdown</td>
<td>Disables the WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config-wlan)# no shutdown</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> security wpa akm sae</td>
<td>Configures threshold on the number of open sessions to trigger the anti-clogging procedure for new sessions.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config-wlan)# security wpa akm sae</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> security wpa akm sae anti-clogging-threshold threshold</td>
<td>Configures the maximum number of retransmissions.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config-wlan)# security wpa akm sae anti-clogging-threshold 2000</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> security wpa akm sae max-retries retry-limit</td>
<td>Configures SAE message retransmission timeout value.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config-wlan)# security wpa akm sae max-retries 10</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> security wpa akm sae retransmit-timeout retransmit-timeout-limit</td>
<td>Enables the WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config-wlan)# security wpa akm sae retransmit-timeout 500</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> no shutdown</td>
<td>Returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config-wlan)# no shutdown</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config-wlan)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Verifying WPA3 SAE and OWE**

To view the system level statistics for the client that has undergone successful SAE authentication, SAE authentication failures, SAE ongoing sessions, SAE commit and confirm message exchanges, use the following show command:

```
Device# show wireless stats client detail
```

Total Number of Clients : 0

client global statistics:
Total association requests received : 0
Total association attempts : 0
Total FT/LocalAuth requests : 0
Total association failures : 0
Total association response accepts : 0
Total association response rejects : 0
Total association response errors : 0
Total association failures due to blacklist : 0
Total association drops due to multicast mac : 0
Total association drops due to throttling : 0
Total association drops due to unknown bssid : 0
Total association drops due to parse failure : 0
Total association drops due to other reasons : 0
Total association requests wired clients : 0
Total association drops wired clients : 0
Total association success wired clients : 0
Total peer association requests wired clients : 0
Total peer association drops wired clients : 0
Total peer association success wired clients : 0
Total 11r ft authentication requests received : 0
Total 11r ft authentication response success : 0
Total 11r ft authentication response failure : 0
Total 11r ft action requests received : 0
Total 11r ft action response success : 0
Total 11r ft action response failure : 0
Total AID allocation failures : 0
Total AID free failures : 0
Total roam attempts : 0
Total CCKM roam attempts : 0
Total 11r roam attempts : 0
Total 11i fast roam attempts : 0
Total 11i slow roam attempts : 0
Total other roam type attempts : 0
Total roam failures in dot11 : 0
Total WPA3 SAE attempts : 0
Total WPA3 SAE successful authentications : 0
Total WPA3 SAE authentication failures : 0
Total incomplete protocol failures : 0
Total WPA3 SAE commit messages received : 0
Total WPA3 SAE commit messages rejected : 0
Total unsupported group rejections : 0
Total WPA3 SAE commit messages sent : 0
Total WPA3 SAE confirm messages received : 0
Total WPA3 SAE confirm messages rejected : 0
Total WPA3 SAE confirm message field mismatch : 0
Total WPA3 SAE confirm message invalid length : 0
Total WPA3 SAE confirm messages sent : 0
Total WPA3 SAE Open Sessions : 0
Total SAE Message drops due to throttling : 0
Total Flexconnect local-auth roam attempts : 0
Total AP 11i fast roam attempts : 0
Total 11i slow roam attempts : 0
Total client state starts : 0
Total client state associated : 0
Total client state l2auth success : 0
Total client state l2auth failures : 0
Total blacklisted clients on dot1xauth failure : 0
Total client state mab attempts : 0
Total client state mab failed : 0
Total client state ip learn attempts : 0
To view the WLAN summary details, use the following command.

Device# show wlan summary

Number of WLANs: 3

<table>
<thead>
<tr>
<th>ID</th>
<th>Profile Name</th>
<th>SSID</th>
<th>Status</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>wlan-demo</td>
<td>ssid-demo</td>
<td>DOWN</td>
<td>[WPA3][SAE][AES]</td>
</tr>
<tr>
<td>3</td>
<td>CR1_SSID_mab-ext-radius</td>
<td>CR1_SSID_mab-ext-radius</td>
<td>DOWN</td>
<td>[WPA2][802.1x][AES]</td>
</tr>
<tr>
<td>109</td>
<td>guest-wlan1</td>
<td>docssid</td>
<td>DOWN</td>
<td>[WPA2][802.1x][AES],[Web Auth]</td>
</tr>
</tbody>
</table>

To view the WLAN properties (WPA2 and WPA3 mode) based on the WLAN ID, use the following command.

Device# show wlan id 1

WLAN Profile Name : wlan-demo

Identifier : 1

Security

802.11 Authentication : Open System
Static WEP Keys : Disabled
Wi-Fi Protected Access (WPA/WPA2/WPA3) : Enabled
WPA (SSN IE) : Disabled
WPA2 (RSN IE) : Disabled
WPA3 (WPA3 IE) : Enabled
AES Cipher : Enabled
CCMP256 Cipher : Disabled
GCMP128 Cipher : Disabled
GCMP256 Cipher : Disabled
Auth Key Management

802.1x : Disabled
PSK : Disabled
CCKM : Disabled
FT dot1x : Disabled
FT PSK : Disabled
Dot1x-SHA256 : Disabled
PSK-SHA256 : Disabled
SAE : Enabled
OWE : Disabled
SUITEB-1X : Disabled
SUITEB192-1X : Disabled
CCKM TSF Tolerance : 1000
OSEN : Disabled
To view the correct AKM for the client that has undergone SAE authentication, use the following command.

Device# show wireless client mac-address <e0ca.94c9.6be0> detail

Client MAC Address : e0ca.94c9.6be0
!
!
Wireless LAN Name: WPA3
!
!
Policy Type : WPA3
Encryption Cipher : CCMP (AES)
Authentication Key Management : SAE
!
!

To view the correct AKM for the client that has undergone OWE authentication, use the following command.

Device# show wireless client mac-address <e0ca.94c9.6be0> detail

Client MAC Address : e0ca.94c9.6be0
!
!
Wireless LAN Name: WPA3
!
!
Policy Type : WPA3
Encryption Cipher : CCMP (AES)
Authentication Key Management : OWE
!
!

To view the list of PMK cache stored locally, use the following command.

Device# show wireless pmk-cache

Number of PMK caches in total : 0

<table>
<thead>
<tr>
<th>Type</th>
<th>Station</th>
<th>Entry Lifetime</th>
<th>VLAN Override</th>
<th>IP Override</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit-Session-Id</td>
<td>Username</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Verifying WPA3 SAE and OWE
PART VII

Mobility

- Mobility, on page 813
- NAT Support on Mobility Groups, on page 831
- Static IP Client Mobility, on page 835
Mobility

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.
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.
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.
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.

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 encrypted 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 21: 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. This could either be the access switch that is currently providing the service or the controller.

- **Point of Presence**—A station's point of presence is the place in the network where the station is being advertised. For instance, if an access switch is advertising reachability to the station via a routing protocol, the interface on which the route is being advertised is considered the station's point of presence.

- **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**
When an AP moves from one controller to another controller (when both controllers are mobility peers), a client associated with the first controller before the move might be anchored to the first controller even after the move. To prevent such a scenario, remove the mobility peer configuration of the controller.

*Figure 22: 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 9800-40 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, WLAN and policy profile configuration must be identical on both the controllers.

- 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.

- Data DTLS and SSC hash key must be same for mobility tunnels between members.

- 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.

- 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.
• RadioactivetracingisnotsupportedforIPv4addressinmobility.

• 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.

• Only IPv4 tunnel is supported between Cisco Catalyst 9800 Series Wireless Controller and Cisco AireOS controller.

• In an HA scenario, ensure that you explicitly configure wireless mobility using mac-address, else mobility tunnel will go down after SSO.

• Mobility tunnel will not work if ECDSA based certificate or trustpoint is used for wireless management.

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 IP address for the mobility peer.
c) Additionally, when NAT is used, enter the optional public IP address to enter the mobility peer's NATed address. When NAT is not used, the public IP address is not used and the device displays the mobility peer's direct IP address.
d) Enter the mobility group to which you want to add the mobility peer.
e) Select the required status for Data Link Encryption.
f) Specify the SSC Hash as required.
g) Click Save & Apply to Device.
h) In the Non-Local Mobility Group Multicast Configuration section, click Add.
i) Enter the mobility group name.
j) Enter the multicast IP address for the mobility group.
k) Click Save.

## Configuring Mobility (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>wireless mobility group name group-name</code></td>
<td>Creates a mobility group named <strong>Mygroup</strong>.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config)# wireless mobility group name Mygroup</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>wireless mobility mac-address mac-addr</code></td>
<td>Configures the MAC address to be used in mobility messages.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config)# wireless mobility mac-address 00:0d:ed:dd:25:82</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>wireless mobility dscp value-0-to-63</code></td>
<td>(Optional) Configures mobility intercontroller DSCP value.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config)# wireless mobility dscp 10</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>wireless mobility group keepalive interval time-in-seconds</code></td>
<td>(Optional) Configures the interval between two keepalives sent to a mobility member. Valid range is between 1 and 30 seconds.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config)# wireless mobility group keepalive interval 5</code></td>
<td><strong>Note</strong> For controllers connected through mobility tunnels, ensure that both controllers have the same keepalive interval value.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>wireless mobility group keepalive count count</code></td>
<td>(Optional) Configures the keepalive retries before a member status is termed DOWN.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config)# wireless mobility group keepalive count 3</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Use the options given below to configure IPv4 or IPv6.</td>
<td>Adds a peer IPv4 or IPv6 address to a specific group.</td>
</tr>
<tr>
<td></td>
<td>• <code>wireless mobility mac-address mac-address ip peer-ip-address group group-name data-link-encryption</code></td>
<td>To remove the peer from the local group, use the no form of this command.</td>
</tr>
<tr>
<td></td>
<td>• <code>wireless mobility mac-address mac-address ip peer-ip-address public-ip public-ip-address group group-name</code></td>
<td></td>
</tr>
</tbody>
</table>
## 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.

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:

- Cisco Catalyst 9800 Series Wireless Controller platforms running Cisco IOS XE Software version 16.10.1 or later.

- Supported Cisco AireOS Wireless Controllers running Cisco AireOS 8.5.14x.x IRCM image based on the 8.5 Maintenance Release software. The following controllers are supported:
- Cisco 3504 Wireless Controllers
- Cisco 5508 Wireless Controllers
- Cisco 5520 Wireless Controllers
- Cisco 8510 Wireless Controllers
- Cisco 8540 Wireless Controllers

Note
Contact the Cisco Technical Assistance Center (TAC) or send an email to wnbu-escalation@cisco.com to receive the Cisco AireOS 8.5 IRCM special image based on the 8.5 Maintenance Release software.

- 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

- 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, the WLAN profile name and the policy profile name are the same.

- 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, DNAC, 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).

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

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

**Example:**
Device# configure terminal

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Use the options given below to configure IPv4 or IPv6.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>wireless mobility group member mac-address mac-address ip peer-ip group group-name</td>
</tr>
<tr>
<td></td>
<td>wireless mobility group member mac-address mac-address ip peer-ip-address public-ip public-ip-address group group-name</td>
</tr>
</tbody>
</table>

**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 public-ip fd09:9:2:49::55 group scalemobility

<table>
<thead>
<tr>
<th>Step 3</th>
<th>wireless mobility group name group-name</th>
</tr>
</thead>
</table>

**Example:**
Device(config)# wireless mobility group name test-group

Adds a name for the local group. The default local group name is "default."
### 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:**

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Built</th>
<th>Tx</th>
<th>Rx</th>
<th>Processed</th>
<th>Tx Error</th>
<th>Rx Error</th>
<th>Forwarded</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Allocs</td>
<td>Frees</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Announce</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>25350</td>
</tr>
<tr>
<td>5624</td>
<td>0</td>
<td>2826</td>
<td>2826</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Mobile Announce Nak</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Static IP Mobile Annce</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Static IP Mobile Annce Rsp</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Handoff</td>
<td>0</td>
<td>42</td>
<td>42</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Handoff End</td>
<td>0</td>
<td>0</td>
<td>2783</td>
<td>2783</td>
<td>0</td>
<td>0</td>
<td>2783</td>
</tr>
<tr>
<td>Handoff End Ack</td>
<td>0</td>
<td>0</td>
<td>2783</td>
<td>2783</td>
<td>2783</td>
<td>0</td>
<td>2783</td>
</tr>
<tr>
<td>Anchor Req</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anchor Grant</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anchor Xfer</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anchor Xfer Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Export Anchor Req</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2812</td>
</tr>
<tr>
<td>Export Anchor Rsp</td>
<td>0</td>
<td>0</td>
<td>2812</td>
<td>2812</td>
<td>2812</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AAA Handoff</td>
<td>0</td>
<td>8436</td>
<td>8436</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AAA Handoff Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 Addr Update</td>
<td>0</td>
<td>0</td>
<td>2792</td>
<td>2792</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 Addr Update Ack</td>
<td>0</td>
<td>0</td>
<td>2792</td>
<td>2792</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
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 output.

**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
```
Verifying Mobility
NAT Support on Mobility Groups

- Information About NAT Support on Mobility Groups, on page 831
- Restrictions for NAT Support on Mobility Groups, on page 832
- Functionalities Supported on Mobility NAT, on page 832
- Configuring a Mobility Peer, on page 833
- Verifying NAT Support on Mobility Groups, on page 833

Information About NAT Support on Mobility Groups

The Network Address Translation (NAT) on Mobility Groups feature supports the establishment of mobility tunnels between peer controllers when one or both peers are behind a NAT. This is achieved by translating the public and private IP addresses of the peers (see figure below). Depending on the placement and number of NATs, translation might be required at one or both ends of the tunnel.

*Figure 23: Mobility NAT*

When configuring a NATed mobility peer, both the private IP address (address in the network before the NAT device) and the public IP address (address in the public network) have to be configured. Also, if you are using a firewall, ensure that the ports listed below can be accessed through the firewall:

- Port 16666 for mobility control messages
Restrictions for NAT Support on Mobility Groups

- Only 1:1 (static) NAT entries can exist for the controller peers that form the mobility tunnels.
- Configuring multiple peers with the same public IP address is not supported.
- Private IP addresses of the configured peers must be unique.
- Port Address Translation (PAT) is not supported.
- If peer controllers of different types, for example, Cisco AireOS and Cisco Catalyst 9800 Series) are placed behind NAT, Inter-Release Controller Mobility (IRCM) is not supported for client roaming.
- IPv6 address translation is not supported.

Functionalities Supported on Mobility NAT

The following table lists the functionalities supported on mobility NAT:

<table>
<thead>
<tr>
<th>Table 31: Functionalities Supported on Mobility NAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two controllers, with the foreign controller behind a NAT device (1to1 NAT only)</td>
</tr>
<tr>
<td>Two controllers, with the anchor controller behind a NAT device (1to1 NAT only)</td>
</tr>
<tr>
<td>Two controllers, with the anchor and foreign controller behind a NAT device (1to1 NAT only)</td>
</tr>
<tr>
<td>Multiple foreign and anchor controllers behind NATs (1to1 NAT only)</td>
</tr>
</tbody>
</table>
| Supported Cisco Catalyst 9800 Series Wireless Controllers | • Cisco Catalyst 9800-40 Wireless Controller  
• Cisco Catalyst 9800-80 Wireless Controller  
• Catalyst 9800 Wireless Controller for Cloud  
• Cisco Catalyst 9800-L Wireless Controller |
| Number of peers supported | 72 |
| Manageability using SNMP, Yang, and web UI | Yes |
| IRCM support for mobility | Yes |
SSO | Yes
---|---
Client roaming (Layer 2 and Layer 3) between Cisco Catalyst 9800 Series Wireless Controllers | Yes
Client roaming (Layer 2 and Layer 3) between Cisco Catalyst 9800 Series Wireless Controller and AireOS controller | No

Supported applications on the mobility tunnel:
- Native profiling
- AP list
- PMK cache
- Mesh AP

Configuring a Mobility Peer

Before you begin
Ensure that the private and public IP addresses of a mobility peer are of the same type, either IPv4 or IPv6.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  configure terminal
  **Example:**
  Device# configure terminal | Enters global configuration mode. |
| **Step 2**
  wireless mobility group member mac-address peer_mac ip peer_private_ip [public-ip peer_public_ip] group group_name
  **Example:**
  Device(config)# wireless mobility group member mac-address 001e.494b.04ff ip 11.0.0.2 public-ip 4.0.0.112 group dom1 | Adds a mobility peer to the list with an optional public IP address. |
  **Note** You cannot configure multiple peers with the same private or public IP address. |
| **Step 3**
  exit
  **Example:**
  Device(config)# exit | Returns to privileged EXEC mode. |

Verifying NAT Support on Mobility Groups

To display the mobility information of a client, use the following command:

Device# show wireless client mac-address 000a.bd15.0010 detail
To display mobility peer information using a private peer IP address, use the following command:

Device# show wireless mobility peer ip 21.0.0.2

Mobility Peer Info
-------------------
Ip Address : 21.0.0.2
Public Ip Address : 3.0.0.22
MAC Address : cc70.ed02.c3b0
Group Name : dom1
.
Static IP Client Mobility

- Information About Static IP Client Mobility, on page 835
- Restrictions, on page 835
- Configuring Static IP Client Mobility (GUI), on page 836
- Configuring Static IP Client Mobility (CLI), on page 836
- Verifying Static IP Client Mobility, on page 837

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Tags &amp; Profiles &gt; Policy.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Policy page, click the policy profile name or click Add to create a new one.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Mobility tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Set the Static IP Mobility field to Enabled state.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Update &amp; Apply to Device.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless profile policy</td>
<td>Configures a WLAN policy profile and enters wireless policy configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless profile policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> static-ip-mobility</td>
<td>Enables static IP mobility.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)#</td>
<td></td>
</tr>
<tr>
<td>static-ip-mobility</td>
<td></td>
</tr>
</tbody>
</table>
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
Static IP 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
  Cisco Umbrella Parameter Map : Not Configured
Autoqos Mode : None
Call Snooping : Disabled
Fabric Profile
```
Profile Name : Not Configured
Accounting list : Not Configured
Accounting List : Not Configured
DHCP
  required : DISABLED
  server address : 0.0.0.0
Opt82
  DhcpOpt82Enable : DISABLED
  DhcpOpt82Ascii : DISABLED
  DhcpOpt82Rid : DISABLED
SSID : DISABLED
APMAC : 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 841
- Redundancy Management Interface (RMI), on page 855
High Availability

- Information About High Availability, on page 841
- Prerequisites for High Availability, on page 843
- Restrictions on High Availability, on page 844
- Configuring Boot Variables Manually on the Controller, on page 845
- Configuring High Availability (GUI), on page 845
- Configuring High Availability, on page 846
- Verifying High Availability Configurations, on page 847
- Verifying AP or Client SSO Statistics, on page 848
- Verifying High Availability, on page 850
- Deleting High Availability, on page 850
- Configuring SNMP in High Availability, on page 851

Information About High Availability

High Availability (HA) allow you to reduce the downtime of wireless networks that occurs because of the failover of controllers.

Two controllers form a 1:1 (Active:Standby) redundancy pair deployed in two separate Cisco Unified Computing System (UCS) boxes for failure protection. If the Active UCS box fails, a switchover occurs and the Standby becomes Active.

The two controllers form a virtual chassis managed as a single node with a single management IP address. The Active box owns the IP address, which means that the connection to the management IP will always reach the Active box. All the interfaces in a controller are virtual Network Interface Controllers (vNICs).

Note

iOS does not sync up with the DHCP addresses and even if it supports, the standby SVI interface has a different mac address and DHCP server does not provide the same IP assigned to be active.

The Standby box covers configurations that are identical to those the Active box covers, which includes all the interfaces. The same set of interfaces are retained after a switchover. This means that the interface state on the Standby box reflects the same state on the Active box. For example, if an interface is UP on the Active box, the interfaces will be up in the new active after a switchover.

Note
The Active box and Standby box must be paired with the same interface name.

Note
Static IP addressing can synch to standby, but the IP address cannot be used from the standby controller.

Both the Active and Standby boxes use a dedicated HA port to send HA traffic between the two controllers. Configure the dedicated HA port by running the `chassis ha-interface <x>` command, as described in High Availability section. The HA port provides the following functionalities:

- Enables communication between the two UCS boxes before the IOSd boots up.
- Transports HA control messages, such as role selection, keepalive, and so on.
- Provides transport for IPC between the two UCS boxes.

You can map a dedicated HA port to a 1 GB interface only. This way, the controller 1:1 HA model runs on two UCS boxes.

You can select either SFP or RJ-45 connection for HA port.

The following Cisco SFPs are supported:

- GLC-SX-MMD
- GLC-LH-SMD

When either SFP or RJ-45 connection is present, HA works between the two UCS boxes. 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 reverts to SFP HA connectivity. If the link between the SFPs are not connected, the HA pair reverts to a single box operation.

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.

IPv4 and IPv6 Multicast

Both IPv4 and IPv6 multicast are HA-aware. For IGMP snooping, the multicast groups and membership are created and managed on the Active box. The multicast packets are then snooped and handled. The same multicast group and membership are synchronized with the Standby box, which will re-create and plumb them to the data plane. For MoU, you should plumb the replication list (CAPWAP interfaces) for each multicast group. After a switchover, the multicast packets continue to reach all the clients of the group.
**AP SSO**

AP SSO provides the following functionalities (as appropriate):

- Synchronizes the live AP states from the Active box to the Standby box in persistent memory.
- Plumbs the AP states to data plane on the Standby box.

After an SSO, you will notice the following:

- There is no AP downtime.
- The AP is not aware of the SSO.

This way, the APs still continue to work in the same manner. Only the APs that have reached the RUN state are preserved in an SSO.

---

**Note**

All AP sessions and transient states are synched to Standby.

---

**Client SSO**

Client SSO is supported for clients that have reached the RUN state. This is typically at the point when a client is authenticated and the IP address is acquired.

The corresponding receiver handler is invoked when:

- A client SSO record is synchronized to the Standby box.
- Dependency is resolved on the Standby box.

At this time, the client state is plumbed to the data plane once all relevant client records are synched to standby.

---

**Note**

After a switchover, the TCP connection to the client will not be retained.

---

**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, 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

This is a dedicated interface reserved for HA transport. This interface comes first (before the IOSd comes up), so that the IPC connection and HA role negotiation can both proceed as send packets over this interface.

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.

Note

You need to manually configure boot variables on the controller. For more details, refer to the Configuring Boot Variables Manually on the Controller section.

Restrictions on High Availability

- 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 because the first packet of the flow is missed.
- The HA connection supports only IPv4.
- Two HA interfaces must be configured on the same subnet, and the subnet cannot be shared with any other interfaces on the device. The HA interfaces must not use 10.10.10.x/24 network as the IP address.
- 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. Hence, the show wireless stats ap discovery chassis active r0 command does not display the AP entries after a switchover.
- Machine snapshot of a VM hosting controller HA interfaces is not supported. It may lead to a crash in the HA controller.
- The maximum length of the hostname 16 charaters. An error is displayed when the hostname exceeds the limit.
- Mobility-side restrictions:
  - Clients that have not reached the complete mobility state are removed after the SSO.
- The cache timer must be persistent and synchronized from Active to Standby. After the synchronization, the timer is resumed on standby with an addition of 30 seconds to the value in the Active box to facilitate deletion from the Active box. During SSO, the session timeout value is also persistent.
- Most of the application classification might 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.

---

### Configuring Boot Variables Manually on the Controller

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>boot system bootflash image_path</td>
<td>Configures the boot image in ROMMON.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# boot system bootflash:C9800-universalk9_wlc.bin</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>config-register 0x2102</td>
<td>Sets the config register to 0x2102.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# config-register 0x2102</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

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

---

### Configuring High Availability (GUI)

You can configure the high availability parameters for the selected access point by performing the following steps.

**Procedure**

- **Step 1** Choose *Configuration > Wireless > Access Points*.
- **Step 2** Click an AP Name. The *Edit AP* screen appears.
- **Step 3** Click the *High Availability* tab.
- **Step 4** Enter the name of the Primary Controller and Management IP Address (IPv4/IPv6). Similarly, enter names and management IP addresses for the Secondary and Tertiary Controllers.
Step 5  Choose any one of the available options from the AP Failover Priority drop-down list. The available options are:

- Low
- Medium
- High
- Critical

Step 6  Click the Update & Apply to Device button.

Configuring High Availability

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> chassis ha-interface GigabitEthernet num local-ip local-chassis-ip-addr network-mask remote-ip remote-chassis-ip-addr</td>
<td>Configures the chassis HA interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# chassis ha-interface GigabitEthernet 2 local-ip 1.1.1.2 255.255.255.0 remote-ip 1.1.1.3</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> This command is issued on both the devices of redundancy pair.</td>
<td></td>
</tr>
<tr>
<td>• num—GigabitEthernet interface number. The range is from 0 to 32.</td>
<td></td>
</tr>
<tr>
<td>• local-chassis-ip-addr—Enter the IP address of the local chassis HA interface.</td>
<td></td>
</tr>
<tr>
<td>• network-mask—Enter the network mask or prefix length in the /nn or A.B.C.D format.</td>
<td></td>
</tr>
<tr>
<td>• remote-chassis-ip-addr—Enter the remote chassis IP address.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Reload the devices for the changes to become effective.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> chassis chassis-num priority chassis-priority</td>
<td>Configures the priority of the specified device.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# chassis 1 priority 1</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Changing the device priority may result in a configuration change for that device. The new device priority will be effective after the next reboot.</td>
<td></td>
</tr>
<tr>
<td>• chassis-num—Enter the chassis number. The range is from 1 to 2.</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

* `chassis-priority`—Enter the chassis priority. The range is from 1 to 2. The default value is 1.

**Note**
When both the devices boot up at the same time, the higher priority 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 3

**chassis timer peer-timeout** `{timeout | default}`

**Example:**

```
Device# chassis timer peer-timeout 500
```

Configures the peer keepalive timeout value.

**Note**
You need not reload the devices after executing this command. Also, this command configures both the devices at the same time with the same timeout value.

`timeout`—Enter the peer timeout value. The range is from 500 milliseconds to 16 seconds. The default is 500 milliseconds.

### 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.vwl.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 =
```
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

<table>
<thead>
<tr>
<th>Inst</th>
<th>Timestamp</th>
<th>Dura (ms)</th>
<th>#APs</th>
<th>#Succ</th>
<th>#Fail</th>
<th>Avg (ms)</th>
<th>Min (ms)</th>
<th>Max (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>00:06:29.042</td>
<td>98</td>
<td>34</td>
<td>34</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>35</td>
</tr>
<tr>
<td>1</td>
<td>00:06:29.057</td>
<td>56</td>
<td>33</td>
<td>30</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>2</td>
<td>00:06:29.070</td>
<td>82</td>
<td>33</td>
<td>33</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>13</td>
</tr>
</tbody>
</table>

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

WNCD Instance : 1
No. of AP radio recovery failures : 0
No. of AP BSSID recovery failures : 0
No. of CAPWAP recovery failures : 3
No. of DTLS recovery failures : 0
No. of reconcile message send failed : 0
No. of reconcile message successfully sent : 30
No. of Mesh BSSID recovery failures : 0
No. of Partial delete cleanup done : 0

WNCD Instance : 2
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 : 33
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 statistics 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 reconciliation : 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 reconciliation : 0
BSSID mismatch with shadow rec reconciliation(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 reconciliation : 0
Zero aid during heap recreate : 0
AID mismatch with shadow rec during reconciliation : 0
AP slotid mismatch shadow rec during reconciliation : 0
Client shadow record not present : 0

To view the mobility details, use the following command:

```
Device# show wireless stat redundancy statistics 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 statistics 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
Verifying High Availability

Table 32: Commands for Monitoring Chassis and Redundancy

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show chassis</td>
<td>Displays the chassis information.</td>
</tr>
</tbody>
</table>
| **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.                         |

Table 33: Command for Monitoring Power Supply, Fan Status, and Serial Number of Active and Standby Chassis

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show inventory</td>
<td>Displays the power supplies, fan, and chassis details of standby and active chassis.</td>
</tr>
</tbody>
</table>

Deleting High Availability

To clear all the HA-related parameters, such as local IP, remote IP, HA interface, mask, timeout, and priority, run the following command:

clear chassis redundancy
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
- 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 23:42:26.359: %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

## Configuring SNMP in High Availability

**Prerequisites**

- The management port must be up and running.
- The management port must have a 10x network IP address to query SNMP commands because the IP Address from where you are issuing the SNMP getmany is in 10.x.x.x network.
## Configuring SNMP in High Availability

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>show interface ip brief</code></td>
<td>Verifies, if the management port IP address is up and running.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# <code>show interface ip brief</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>`show run</td>
<td>sec GigabitEthernet0`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# `show run</td>
<td>sec GigabitEthernet0`</td>
</tr>
<tr>
<td>3</td>
<td>`show run</td>
<td>sec SNMP`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# `show run</td>
<td>sec SNMP`</td>
</tr>
<tr>
<td>4</td>
<td><code>snmp-server community public RW</code></td>
<td>Configures the SNMP server.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# <code>snmp-server community public RW</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>

### ENTITY-MIB

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

<table>
<thead>
<tr>
<th>MIB Objects</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>entPhysicalSerialNum</td>
<td>Is the only MIB object that needs to be monitored.</td>
</tr>
<tr>
<td>entPhysicalIndex</td>
<td>Is the unique ID that is read only and set by entity MIB when an instance is created.</td>
</tr>
</tbody>
</table>
| entPhysicalName | Refers to `chassis chassis_num`.  
[chassis_num]—Refers to a standalone or dual chassis.  
The length of `entPhysicalName` must be less than 32 characters. |

### ENTITY-STATE-MIB

The ENTITY-STATE-MIB defines objects to extend the functionality provided by the ENTITY-MIB. This MIB supports entities with the following `entPhysicalClass` values:
• chassis
• powerSupply
• fan

Table 35: MIB Object and Notes

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>entStateOper</td>
<td>Is the only MIB object that needs to be monitored.</td>
</tr>
</tbody>
</table>
Redundancy Management Interface (RMI)

- Information About Redundancy Management Interface (RMI), on page 855
- Prerequisite for RMI, on page 857
- Configuring Redundancy Management Interface (GUI), on page 858
- Configuring a Redundancy Management Interface IP Address (CLI), on page 858
- Configuring Gateway Monitoring (CLI), on page 860
- Verifying the Gateway-Monitoring Configuration, on page 860
- Verifying the Redundancy Management Interface Configuration, on page 861

Information About Redundancy Management Interface (RMI)

The Redundancy Management Interface (RMI) is used as a secondary link between the active and standby Cisco Catalyst 9800 Series Wireless 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. The RMI is used for the following purposes:

- Dual Active Detection
- Exchange resource health between controllers, for instance, gateway reachability status from either controller.

Note

The RMI might trigger a switchover based on the resource status on the controllers.

Active Controller

The primary address on the active controller is the management IP. The secondary IPv4 address on the management VLAN is the RMI IP for the active controller. Do not configure the secondary IPv4 addresses explicitly because a single secondary IPv4 address is configured automatically by RMI under the RMI interface.

Note

RMI supports only IPv4 addresses.
Standby Controller

The management interface on the standby controller remains UP for normal operation. The standby controller does not have the wireless management IP configured; it has the RMI IP address configured as the primary IP address. When the standby controller becomes active, the management IP becomes the primary IP and the RMI IP becomes the secondary IP. If the interface on the active controller is administratively down, the same state is reflected on standby controller.

Note

If the uplink for the standby controller is down, the standby controller will keep rebooting.

Dual Stack Support with RMI IPv4

Dual stack refers to the fact that the wireless management interface can be configured with IPv4 and IPv6 addresses. If RMI IPv4 address is configured along with an IPv4 management IP, you can additionally configure an IPv6 management address on the wireless management interface. This IPv6 management IP will not be visible on the standby controller.

Note

The RMI feature supports only RMI IPv4 addresses.

RMI-Based High-Availability Pairing

You should consider the following requirements for High-Availability (HA) pairing:

• Use either privileged EXEC-mode RP-based CLIs or RMI IP-based HA pairing for a fresh installation.
• Perform seamless upgrade of an HA pair.
• Perform seamless downgrade of an HA pair.
• The RP IPs are derived from the RMI IPs after a HA pair is formed. Also, the privileged EXEC-mode RP-based CLI method of clearing and forming an HA pair is not allowed.

Note

Dynamic HA pairing requires both active controller and the standby controller to reload on Cisco Catalyst 9800 Series Wireless Controllers. However, dynamic HA pairing occurs on Cisco Catalyst 9800-40 Wireless Controller and Cisco Catalyst 9800-80 Wireless Controller when one of them reloads and becomes standby.

Already Paired Controllers

If the controllers are already in an HA pair, the existing exec-mode RP-based CLIs will continue to be used. You can enable RMI to migrate to the RMI based HA pairing.

If the controllers are already paired and RMI is configured, it will overwrite the RP IPs with the RMI derived IPs. The HA pair will not be disturbed immediately but the controllers will pick up the new IP when the next reload happens. RMI feature mandates a reload for the feature to be effective. When both controllers reload, they would come up as a pair with the new RMI derived RP IPs.
Upgrade Scenario

A system that is being upgraded can choose to:

- Migrate with the existing RP IP configuration intact—In this case, the existing RP IP configuration will continue to be used. The exec-mode RP-based CLIs are used for future modifications.

- Migrate after clearing the HA configuration—In this case, you can choose between the old (exec-mode RP-based CLIs) and new RMI based RP configuration methods.

Note

In case the older configuration is retained, the RMI configuration updates the RP IPs with the IPs derived from the RMI IPs.

Downgrade Scenario

The downgrade scenario will have only the exec-mode RP-based CLIs. The following are the two possibilities:

- If the upgraded system used the RMI based RP configuration.
- If the upgraded system continued to use the exec-mode RP-based CLIs.

Note

In the above cases, the downgraded system uses the exec-mode RP-based CLIs to modify the configuration. However, the downgraded system will continue to use the new derived RP IPs.

Prerequisite for RMI

It is mandatory to configure the Redundancy Management IP address and Peer Redundancy Management address before HA pairing. Both the interfaces must be in the same subnet as the Wireless Management Interface. If controller1 is configured with 9.10.90.147 as the Redundancy Management IP and controller2 with 9.10.90.149, you need to execute the following command in controller1 for redundancy mode:

```
redun-management interface Vlan vlan-interface-no chassis-number address ip-address chassis-number address ip-address
```

Note

The `redun-management` command needs to be configured on both the controllers prior to HA pairing. Here, the IP addresses 9.10.90.147 and 9.10.90.149 refer to the RMI IPs.

```
Device# conf t
Device(config)# redun-management interface Vlan Vlan90 chassis 1 address 9.10.90.147 chassis 2 9.10.90.149
```
Configuring Redundancy Management Interface (GUI)

**Procedure**

**Step 1**
In the Administration > Device > Redundancy window, perform the following:

a. Set the Redundancy Configuration toggle button to Enabled to activate redundancy configuration.

b. In the Redundancy Pairing Type field, select **RMI+RP** to perform RMI+RP redundancy pairing as follows:
   - In the **RMI IP for Chassis 1** field, enter RMI IP address for chassis 1.
   - In the **RMI IP for Chassis 2** field, enter RMI IP address for chassis 2.

c. In the Redundancy Pairing Type field, select **RP** to perform RP redundancy pairing as follows:
   - In the **Local IP** field, enter an IP address for Local IP.
   - In the **Netmask** field, enter the subnet mask assigned to all wireless clients.
   - From the **HA Interface** drop-down list, choose one of the HA interface.
   
   **Note** You can select the HA interface only for Cisco Catalyst 9800 Series Wireless Controllers.
   - In the **Remote IP** field, enter an IP address for Remote IP.

d. In the **Keep Alive Timer** field, enter an appropriate timer value. The valid range is between 1 and 10 (x100 milliseconds).

e. In the **Keep Alive Retries** field, enter an appropriate retry value. The valid range is between 3 and 10 seconds.

f. In the **Active Chassis Priority** field, enter a value.

**Step 2**
Click **Apply**.

---

Configuring a Redundancy Management Interface IP Address (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  * chassis redundancy ha-interface
  * GigabitEthernet *num*
| Creates an HA interface for your controller.  
  *num*: GigabitEthernet interface number. The range is from 1 to 32. |

*Example:*
### Purpose

The chosen interface will be used as the dedicated interface for HA communication between the 2 controllers.

### Command or Action

Device# chassis redundancy ha-interface GigabitEthernet 3

### Note

This command is applicable only for Cisco Catalyst 9800 Series Wireless Controllers.

### Step 2

**configure terminal**

**Example:**

Device# configure terminal

- **Purpose:**
  - Enters global configuration mode.

### Step 3

**redun-management interface vlan vlan-interface-no chassis chassis-number address ip-address chassis chassis-number address ip-address**

**Example:**

Device(config)# redun-management interface Vlan 200 chassis 1 address 9.10.90.147 chassis 2 address 9.10.90.149

- **Purpose:**
  - Configures Redundancy Management Interface.

### Note

- **Note:**
  - Here, the `vlan-interface-no` is the same VLAN as the Management VLAN. That is, both must be on the same subnet.

### Step 4

**end**

**Example:**

Device(config)# end

- **Purpose:**
  - Returns to privileged EXEC mode.

### Note

- **Note:**
  - You need to execute the following command for the RMI configuration to be effective:

```plaintext
write memory
```
Configuring Gateway Monitoring (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> [no] management gateway-failover enable</td>
<td>Enables gateway monitoring. (Use the no form of this command to disable gateway monitoring.)</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# management gateway-failover enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# end</td>
<td><strong>Note</strong> Use the following command to save the configuration: <code>write memory</code>.</td>
</tr>
</tbody>
</table>

Verifying the Gateway-Monitoring Configuration

To verify the status of the gateway-monitoring configuration on an active controller, use the following command:

Device# `show redundancy states`

```
my state = 13 -ACTIVE
peer state = 8 -STANDBY HOT
Mode = Duplex
Unit = Primary
Unit ID = 1
Redundancy Mode (Operational) = sso
Redundancy Mode (Configured) = sso
Redundancy State = sso
Maintenance Mode = Disabled
Manual Swact = enabled
Communications = Up
client count = 127
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x0
Gateway Monitoring = Enabled
```

**Note**

If gateway monitoring is enabled, you can configure the gateway IP using the following command:

`ip default-gateway gateway-ip`

Here, the `gateway-ip` should be in the same subnet as the wireless management subnet.
To verify the status of the gateway-monitoring configuration on a standby controller, use the following command:

```
Device-stby# show redundancy states
my state = 8 -STANDBY HOT
peer state = 13 -ACTIVE
Mode = Duplex
Unit = Primary
Unit ID = 2
Redundancy Mode (Operational) = sso
Redundancy Mode (Configured) = sso
Redundancy State = sso
Maintenance Mode = Disabled
Manual Swact = cannot be initiated from this the standby unit
Communications = Up
client count = 127
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x0
Gateway Monitoring = Enabled
```

## Verifying the Redundancy Management Interface Configuration

To verify the interface configuration for an active controller, use the following command:

```
Device# show running-config interface vlan
Building configuration...
Current configuration : 109 bytes
!
interface Vlan90
ip address 9.10.90.147 255.255.255.0 secondary
ip address 9.10.90.41 255.255.255.0
end
```

To verify the interface configuration for a standby controller, use the following command:

```
Device-stby# show running-config interface vlan 90
Building configuration...
Current configuration : 62 bytes
!
interface Vlan90
ip address 9.10.90.149 255.255.255.0
end
```

To verify the chassis redundancy management interface configuration for an active controller, use the following command:

```
Device# show chassis rmi
Chassis/Stack Mac Address : 000c.2964.1eb6 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Chassis# Role Mac Address Priority Version State IP RMI-IP
*1 Active 000c.2964.1eb6 1 V02 Ready 169.254.90.147 9.10.90.147
2 Standby 000c.2975.3aa6 1 V02 Ready 169.254.90.149 9.10.90.149
```
To verify the chassis redundancy management interface configuration for a standby controller, use the following command:

Device-stby# show chassis rmi

Chassis/Stack Mac Address : 000c.2964.1eb6 - Local Mac Address
Mac persistency wait time: Indefinite

<table>
<thead>
<tr>
<th>Chassis#</th>
<th>Role</th>
<th>Mac Address</th>
<th>Priority</th>
<th>Version</th>
<th>State</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active</td>
<td>000c.2964.1eb6</td>
<td>1</td>
<td>V02</td>
<td>Ready</td>
<td>169.254.90.147</td>
</tr>
<tr>
<td></td>
<td>Standby</td>
<td>000c.2975.3aa6</td>
<td>1</td>
<td>V02</td>
<td>Ready</td>
<td>169.254.90.149</td>
</tr>
</tbody>
</table>

To verify the ROMMON variables on an active controller, use the following command:

Device# show romvar | include RMI

RMI_INTERFACE_NAME = Vlan90
RMI_CHASSIS_LOCAL_IP = 9.10.90.147
RMI_CHASSIS_REMOTE_IP = 9.10.90.149

To verify the ROMMON variables on a standby controller, use the following command:

Device-stby# show romvar | include RMI

RMI_INTERFACE_NAME = Vlan90
RMI_CHASSIS_LOCAL_IP = 9.10.90.149
RMI_CHASSIS_REMOTE_IP = 9.10.90.147

To verify the switchover reason, use the following command:

Device# show redundancy switchover history

<table>
<thead>
<tr>
<th>Index</th>
<th>Previous active</th>
<th>Current active</th>
<th>Current reason</th>
<th>Switchover</th>
<th>Switchover time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
<td>Active lost GW</td>
<td>17:02:29</td>
<td>UTC Mon Feb 3 2020</td>
</tr>
</tbody>
</table>
PART IX

Quality of Service

• Quality of Service, on page 865
• Wireless Auto-QoS, on page 879
• Native Profiling, on page 883
• Air Time Fairness, on page 897
CHAPTER 99

Quality of Service

• Information about Wireless QoS, on page 865
• How to Configure Wireless QoS, on page 868
• SIP Call Admission Control (CAC), on page 873
• SIP Voice Call Snooping, on page 875

Information about Wireless QoS

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.

**Supported QoS Features on Wireless Targets**

This table describes the various features available on wireless targets.

*Table 36: QoS Features Available on Wireless Targets*

<table>
<thead>
<tr>
<th>Target</th>
<th>Features</th>
<th>Direction Where Policies Are Applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>• Set</td>
<td>Upstream and downstream</td>
</tr>
<tr>
<td></td>
<td>• Police</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Drop</td>
<td></td>
</tr>
<tr>
<td>Client</td>
<td>• Set</td>
<td>Upstream and downstream</td>
</tr>
<tr>
<td></td>
<td>• Police</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Drop</td>
<td></td>
</tr>
</tbody>
</table>

This table describes the various features available on wireless targets.

*Table 37: QoS Policy Actions*

<table>
<thead>
<tr>
<th>Policy Action Types</th>
<th>Local Mode</th>
<th>Flex Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Police</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Set</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

This table describes the various features available on wireless targets.

*Table 38: QoS Policy Set Actions*

<table>
<thead>
<tr>
<th>Set Action Types</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Mode</td>
<td>Flex Mode</td>
</tr>
<tr>
<td>set dscp</td>
<td>Supported</td>
</tr>
<tr>
<td>set qos-group</td>
<td>Supported</td>
</tr>
<tr>
<td>set wlan user-priority (downstream only)</td>
<td>Supported (BSSID only)</td>
</tr>
<tr>
<td></td>
<td>Supported (BSSID only)</td>
</tr>
</tbody>
</table>
**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.

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.

---

**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).
- 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.

- 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.

AP Side Restrictions

- For Cisco Embedded Wireless Controller, the QoS policies are enforced on the AP. Due to this AP-side restriction, police actions are only enforced at a per flow (5-tuple) level.

How to Configure Wireless QoS

Configuring a Policy Map with Class Map (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Services &gt; QoS.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Add to view the Add QoS window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the text box next to the Policy Name, enter the name of the new policy map that is being added.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Add Class-Maps.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure AVC based policies or User Defined policies. To enable AVC based policies, and configure the following:</td>
</tr>
<tr>
<td>a)</td>
<td>Choose either Match Any or Match All.</td>
</tr>
<tr>
<td>b)</td>
<td>Choose the required Mark Type and then specify the appropriate Mark Value.</td>
</tr>
<tr>
<td>c)</td>
<td>Choose the required Mark Type. If you choose DSCP, you must specify the appropriate Mark Value.</td>
</tr>
<tr>
<td>d)</td>
<td>Check the Drop check box to drop traffic from specific sources.</td>
</tr>
<tr>
<td>Note</td>
<td>When Drop is enabled, the Mark Type and Police(kbps) options are disabled.</td>
</tr>
</tbody>
</table>

- Based on the chosen match type, select the required protocols from the Available Protocol(s) list and move them to the Selected Protocols list. These selected protocols are the ones from which traffic is dropped.
- Click Save.
To add more Class Maps, repeat steps 4 and 5.

**Step 6**
To enable User-Defined QoS policy, and configure the following:

a) Choose either Match Any or Match All.

b) Choose the required Match Type 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> class-map class-map-name</td>
<td>Creates a class map.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# class-map test</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> match dscp dscp-value</td>
<td>Matches the DSCP value in the IPv4 and IPv6 packets.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-cmap)# match dscp 46</td>
<td></td>
</tr>
</tbody>
</table>
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.

• Platinum
• Gold
• Silver
• Bronze

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.

Configuring Policy Profile to Apply QoS Policy (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless profile policy policy-policy</td>
<td>Configures WLAN policy profile and enters the wireless policy configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless profile policy qostest</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> service-policy client {input</td>
<td>output} policy-name</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# service-policy client input policy-map-client</td>
<td>• input—Assigns the client policy for ingress direction on the policy profile.</td>
</tr>
<tr>
<td></td>
<td>• output—Assigns the client policy for egress direction on the policy profile.</td>
</tr>
</tbody>
</table>
### Applying Policy Profile to Policy Tag (GUI)

**Procedure**

1. Choose Configuration > Tags & Profiles > Tags.
2. On the Manage Tags page in the Policy tab, click Add.
3. In the Add Policy Tag window that is displayed, enter a name and description for the policy tag.
4. Map the required WLAN IDs and WLAN profiles with appropriate policy profiles.
5. Click Update & Apply to Device.

### Applying Policy Profile to Policy Tag (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless tag policy policy-tag-name</td>
<td>Configures policy tag and enters the policy tag configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-policy-tag)# wireless tag policy qostag</td>
<td></td>
</tr>
</tbody>
</table>
### Attaching Policy Tag to an AP

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ap mac-address</td>
<td>Configures Cisco APs and enters the ap profile configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap F866.F267.7DFB</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>policy-tag policy-tag-name</td>
<td>Maps a Policy tag to the AP.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-ap-tag)# policy-tag qostag</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
<td>Saves the configuration and exits the configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-ap-tag)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show ap tag summary</td>
<td>Displays the ap details and tags associated to it.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show ap tag summary</td>
<td></td>
</tr>
</tbody>
</table>

### Purpose Command or Action

**Purpose**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>wlan wlan-name policy profile-policy-name</td>
<td>Maps a policy profile to a WLAN profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-policy-tag)# wlan test policy qostest</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
<td>Saves the configuration and exits the configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-policy-tag)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show wireless tag policy summary</td>
<td>Displays the configured policy tags.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show wireless tag policy summary</td>
<td><strong>Note</strong> To view the detailed information of a policy tag, use the show wireless tag policy detailed policy-tag-name command.</td>
</tr>
</tbody>
</table>
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.

Using this feature, you can specify the bandwidth parameters manually for one SIP call and then use this configuration to reserve bandwidth whenever a new call is received.

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 on the controller.

Configuring SIP CAC

SIP CAC controls the total number of SIP calls that can be made.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures WLAN policy profile and enters the wireless policy configuration mode.</td>
</tr>
<tr>
<td>wireless profile policy &lt;policy-name&gt;</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# wireless profile policy policy1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Disables the wireless policy profile.</td>
</tr>
<tr>
<td>shutdown</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configure the policy profile with the Platinum metal QoS Policy. The upstream policy is specified with the keyword platinum-up as shown in the example.</td>
</tr>
<tr>
<td>service-policy input policy-name</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-wireless-policy)# service-policy input platinum</td>
<td></td>
</tr>
</tbody>
</table>

Note
Upstream policies differ from downstream policies. The upstream policies have a suffix of -up.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 5** | service-policy output *policy-name*  
**Example:**  
Device(config-wireless-policy)# service-policy output platinum-up |
| **Note** | SSID policies should be configured with Platinum when Call Snoop is enabled |
| **Step 6** | service-policy clientinput *client-policy-name*  
**Example:**  
Device(config-wireless-policy)# service-policy client input voice-client |
| **Step 7** | service-policy clientoutput *client-policy-name*  
**Example:**  
Device(config-wireless-policy)# service-policy client output voice-client |
| **Step 8** | call-snoop  
**Example:**  
Device(config-wireless-policy)# call-snoop |
| **Step 9** | [no] shutdown  
**Example:**  
Device(config-wireless-policy)# no shutdown |
| **Step 10** | ap dot11 {5ghz|24ghz} cac {voice | video} acm  
**Example:**  
Device(config-wireless-policy)#ap dot11 5ghz cac voice acm |
| **Step 11** | ap dot11 {5ghz|24ghz} cac voice sip  
**Example:**  
Device(config)#ap dot11 5ghz cac voice sip |
| **Step 12** | ap dot11 {5ghz|24ghz} cac voicesipbandwidth <bandwidth>  
sample-interval <interval-value> |
| **Step 5** | Enables call snooping for WLAN. |
| **Step 6** | Enables the wireless policy profile. |
| **Step 10** | Enables the ACM static on the radio. When enabling SIP snooping, use the static CAC, not the load-based CAC. |
| **Step 11** | Configures SIP-based CAC. |
| **Step 12** | (Optional) Configures the bandwidth and the interval value. |
Verifying SIP CAC

Use the following Show command to verify the SIP CAC feature:

```
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
0  802.11b/g  1  23437  765  3

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.
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

#### Before you begin

- To enable call-snoop, the BSSID platinum policy should be configured first.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>wireless profile policy &lt;policy-name&gt;</code></td>
<td>Configures WLAN policy profile and enters the wireless policy configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless profile policy policy-name</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>shutdown</code></td>
<td>Disables the wireless policy profile.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# Shutdown</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>`service-policy {input</td>
<td>output} policy-name`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# service-policy input platinum-up</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# service-policy output platinum</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>Upstream policies differ from downstream policies. The upstream policies have a suffix of <code>-up</code>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>SSID policies should be configured with Platinum when Call Snoop is enabled.</td>
</tr>
<tr>
<td>5</td>
<td>`service-policy client {input</td>
<td>output} client-policy-name`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# service-policy client input voice-client</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

#### Command or Action

```
Device(Config-wireless-policy)#
service-policy client output voice-client
```

#### Purpose

Enables call snooping for WLAN.

### Step 6

**call-snoop**

**Example:**

```
Device(config-wireless-policy)#
call-snoop
```

### Step 7

**[no] shutdown**

**Example:**

```
Device(config-wireless-policy)# no shutdown
```

### Step 8

**end**

**Example:**

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

### 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**

---

877
Verifying SIP Voice Call Snooping
Wireless Auto-QoS

- Information About Auto QoS, on page 879
- How to Configure Wireless AutoQoS, on page 880

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 39: AutoQoS Policy Configuration

<table>
<thead>
<tr>
<th>Mode</th>
<th>Client Ingress</th>
<th>Client Egress</th>
<th>BSSID Ingress</th>
<th>BSSID Egress</th>
<th>Port Ingress</th>
<th>Port Egress</th>
<th>Radio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>N/A</td>
<td>N/A</td>
<td>P3</td>
<td>P4</td>
<td>N/A</td>
<td>P7</td>
<td>ACM on</td>
</tr>
<tr>
<td>Guest</td>
<td>N/A</td>
<td>N/A</td>
<td>P5</td>
<td>P6</td>
<td>N/A</td>
<td>P7</td>
<td>edca-parameters</td>
</tr>
<tr>
<td>Fastlane</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>P7</td>
<td>edca-parameters</td>
</tr>
<tr>
<td>Enterprise-avc</td>
<td>N/A</td>
<td>N/A</td>
<td>P1</td>
<td>P2</td>
<td>N/A</td>
<td>P7</td>
<td></td>
</tr>
</tbody>
</table>

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
How to Configure Wireless AutoQoS

Configuring Wireless AutoQoS on Profile Policy

You can enable AutoQoS on a profile policy.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>wireless autoqos policy-profile policy-name mode { enterprise-avc</td>
<td>fastlane</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# wireless autoqos policy-profile test-profile mode voice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• enterprise-avc—Enables AutoQos Wireless Enterprise AVC Policy.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• fastlane—Enable AutoQos Wireless Fastlane Policy.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• guest—Enable AutoQos Wireless Guest Policy.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• voice—Enable AutoQos Wireless Voice Policy.</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>shutdown</td>
<td>Shuts down the policy profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device shutdown</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>wireless autoqos disable</td>
<td>Globally disables wireless AutoQoS.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# wireless autoqos disable</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>[no] shutdown</td>
<td>Enables the wireless policy profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>no shutdown</td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>clear platform software autoqos config template { enterprise_avc</td>
<td>guest}</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# clear platform software autoqos config template guest</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Clearing Wireless AutoQoS Policy Profile

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>shutdown</code></td>
<td>Shuts down the policy profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device shutdown</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>wireless autoqos policy-profile policy-name mode clear</code></td>
<td>Clears the configured AutoQoS wireless policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# wireless autoqos policy-profile test-profile mode clear</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>[no] shutdown</code></td>
<td>Enables the wireless policy profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>no shutdown</code></td>
<td></td>
</tr>
</tbody>
</table>

Viewing AutoQoS on policy profile

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>show wireless profile policy detailed policy-profile-name</code></td>
<td>Shows policy-profile detailed parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# show wireless profile policy detailed testqos</code></td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 101

Native Profiling

- Information About Native Profiling, on page 883
- Creating a Class Map (GUI), on page 884
- Creating a Class Map (CLI), on page 885
- Creating a Service Template (GUI), on page 887
- Creating a Service Template (CLI), on page 888
- Creating a Parameter Map, on page 889
- Creating a Policy Map (GUI), on page 889
- Creating a Policy Map (CLI), on page 890
- Configuring Native Profiling in Local Mode, on page 892
- Verifying Native Profile Configuration, on page 895

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)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>class-map type control subscriber match-any class-map-name</code></td>
<td>Specifies the class map type and name.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# class-map type control subscriber match-any cls_user</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>match username username</code></td>
<td>Specifies the class map attribute filter criteria.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-filter-control-classmap)# match username ciscoise</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>class-map type control subscriber match-any class-map-name</code></td>
<td>Specifies the class map type and name.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# class-map type control subscriber match-any cls_userrule</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>match user-role user-role</code></td>
<td>Specifies the class map attribute filter criteria.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-filter-control-classmap)# match user-role engineer</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>class-map type control subscriber match-any class-map-name</code></td>
<td>Specifies the class map type and name.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# class-map type control subscriber match-any cls_oui</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>match oui oui-address</code></td>
<td>Specifies the class map attribute filter criteria.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-filter-control-classmap)# match oui 48.f8.b3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>class-map type control subscriber match-any class-map-name</code></td>
<td>Specifies the class map type and name.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# class-map type control subscriber match-any cls_mac</code></td>
<td>Specifies the class map attribute filter criteria.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> match mac-address <em>mac-address</em></td>
<td>Specifies the class map type and name.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-filter-control-classmap)# match mac-address 0040.96b9.4a0d</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> class-map type control subscriber match-any <em>class-map-name</em></td>
<td>Specifies the class map attribute filter criteria.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# class-map type control subscriber match-any cls_devtype</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> match device-type <em>device-type</em></td>
<td>Specifies the class map attribute filter criteria.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-filter-control-classmap)# match device-type windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> class-map type control subscriber match-all <em>class-map-name</em></td>
<td>Specifies the class map type and name.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# class-map type control subscriber match-all match_tod</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> match join-time-of-day <em>start-time end-time</em></td>
<td>Specifies a match to the time of day.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-filter-control-classmap)# match join-time-of-day 10:30 12:30</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> You should also disable AAA override for this command to work.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong> match day <em>day-of-week</em></td>
<td>Matches day of the week.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-filter-control-classmap)# match day Monday</td>
<td>Use the <code>show class-map type control subscriber name name</code> command to verify the configuration.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| **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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose <strong>Configuration &gt; Security &gt; Local Policy</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>On the Local Policy page, <strong>Service Template</strong> tab, click ADD.</td>
</tr>
</tbody>
</table>
| **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. |
**Creating a Service Template (CLI)**

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 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:**  
Device(config-service-template)# service-policy qos output out_qos | Configures an output QoS policy for the client. |
Creating a Parameter Map

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>parameter-map type subscriber attribute-to-service parameter-map-name</td>
<td>Specifies the parameter map type and name.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# parameter-map type subscriber attribute-to-service param</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>map-index map device-type eq filter-name</td>
<td>Specifies the parameter map attribute filter criteria. Multiple filters are used in the example provided here.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-parameter-map-filter)# 1 map device-type eq &quot;windows&quot; mac-address eq 3c77.e602.2f91 username eq &quot;cisco&quot;</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>map-index service-template service-template-name precedence precedence-num</td>
<td>Specifies the service template and its precedence.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-parameter-map-filter-submode)# 1 service-template svc1 precedence 150</td>
<td></td>
</tr>
</tbody>
</table>

Creating a Policy Map (GUI)

**Procedure**

2. Enter a name for the Policy Map in the Policy Map Name text field.
3. Click Add
4. Choose the service template from the Service Template drop-down list.
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
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.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>policy-map type control subscriber</td>
<td>Specifies the policy map type.</td>
</tr>
<tr>
<td>policy-map-name</td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# policy-map type control subscriber</td>
<td></td>
</tr>
<tr>
<td></td>
<td>polmap5</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>event identity-update match-all</td>
<td>Specifies the match criteria to the policy map.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-event-control-policymap)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>event identity-update match-all</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>You can apply a service template using either a class map or a parameter map, as shown here.</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• class-num class class-map-name do-until-failure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• action-index activate service-template service-template-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• action-index map attribute-to-service table parameter-map-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>The following example shows how a class-map with a service-template has to be applied:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-class-control-policymap)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10 class cls_mac do-until-failure</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Device(config-action-control-policymap)# 10 activate service-template svc1</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-action-control-policymap)# end</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> wireless profile policy profile-policy</td>
<td>Configures a wireless policy profile. <strong>Caution</strong> Do not configure aaa-override for native profiling under a named wireless profile policy.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wireless profile policy default-wlan-policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> description profile-policy-description</td>
<td>Adds a description for the policy profile.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wireless-policy)# description &quot;default policy profile&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> dhcp-tlv-caching</td>
<td>Configures DHCP TLV caching on a WLAN.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wireless-policy)# dhcp-tlv-caching</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> http-tlv-caching</td>
<td>Configures client HTTP TLV caching on a WLAN.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wireless-policy)# http-tlv-caching</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> subscriber-policy-name policy-name</td>
<td>Configures the subscriber policy name.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wireless-policy)# subscriber-policy-name polmap5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> vlan vlan-id</td>
<td>Configures a VLAN name or VLAN ID.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Native Profiling in Local Mode

**Purpose**

**Command or Action**

**Step 13**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>no shutdown</td>
<td>Saves the configuration.</td>
</tr>
</tbody>
</table>

**Example:**

```
Device(config-wireless-policy)# no shutdown
```
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>no shutdown</td>
<td>Saves the configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# no shutdown</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>exit</td>
<td>Exits wireless policy configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# exit</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>wireless tag site <strong>site-name</strong></td>
<td>Configures site tag and enters site tag configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless tag site np_local_site</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>local-site</td>
<td>Configure this site as local site.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-site-tag)# local-site</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>exit</td>
<td>Exits site tag configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-site-tag)# exit</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>wireless tag policy <strong>policy-tag-name</strong></td>
<td>Configures a policy tag and enters policy tag configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless tag policy new1</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>wlan wlan-profile-name policy <strong>policy-name</strong></td>
<td>Maps a policy profile to a WLAN profile.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-policy-tag)# wlan godavari-cwa policy np_local_policy</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>exit</td>
<td>Exits policy tag configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-policy-tag)# exit</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>wlan wlan-profile-name wlan-id ssid</td>
<td>Configures the WLAN and SSID.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wlan godavari-cwa 199 gcae</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>no security wpa</td>
<td>Disables WPA security.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# no security wpa</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>18</td>
<td>no security wpa akm dot1x</td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wlan)# no security wpa akm dot1x</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>no security wpa wpa2</td>
<td>Disables WPA2 security.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wlan)# no security wpa wpa2</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>no security wpa wpa2 ciphers aes</td>
<td>Disables WPA2 ciphers for AES.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wlan)# no security wpa wpa2 ciphers aes</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>no shutdown</td>
<td>Saves the configuration.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wlan)# no shutdown</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>exit</td>
<td>Exits WLAN configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wlan)# exit</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>ap ap-mac-address</td>
<td>Enters AP configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# ap D46D.50A6.ED40</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>policy-tag policy-tag</td>
<td>Associates the policy tag to the AP.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-ap-tag)# policy-tag new1</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>site-tag site-tag</td>
<td>Associates the site tag to the AP.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-ap-tag)# site-tag np_local_site</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wlan)# end</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>show ap summary</td>
<td>(Optional) Displays whether the APs are in flex mode or local mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# show ap summary</td>
<td></td>
</tr>
</tbody>
</table>
Verifying Native Profile Configuration

Use the following `show` commands to verify the native profile configuration:

```
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: 78380209000000174BF2B5B9
  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

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
```

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
```
| 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
Air Time Fairness

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 the following usage groups at the policy level: low, medium, and high.
- Client-based ATF metrics accumulation is performed in the transmit complete routine. This allows the air time that is unused by clients in low-usage or medium-usage groups to be accumulated to a common share pool bucket where the high-usage clients can be replenished.

**Supported Access Point Platforms**

Cisco ATF is supported on the following Cisco IOS access points:

- Cisco Aironet 2600 Series Access Points
- Cisco Aironet 3500 Series Access Points
- Cisco Aironet 3600 Series Access Points
- Cisco Aironet 3700 Series Access Points

---

**Note**

Cisco ATF is supported on MESH, if APs support ATF.

**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 AP Group
* per AP
* per client

* 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
    * An AP group
    * An AP
    * A client

---

**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 service provider. Each group can be assigned a certain percentage of air time.

**Enterprise/Hospitality/Retail**

In this instance, the venue is sharing a WLAN between employees and guests. The guest network can be further partitioned by service provider. The guests could be sub-grouped by tier of service type with each subgroup being assigned a certain percentage of air time, for example a paid group is entitled 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.

The following are the high-level steps to configure Cisco ATF:

1. Enable Monitor mode to determine network usage (optional).
2. Create Cisco ATF policies.
3. Add WLAN ATF policies per network, AP group, or AP. The policies set in AP or AP group overrides per network polices.
4. Determine, if optimization must be enabled.
5. Periodically check the Cisco ATF statistics.

Configuring Cisco Air Time Fairness (ATF)

Creating Cisco ATF Policy

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wireless profile airtime-fairness atf-policy-name atf-profile-id</td>
<td>Creates a new Cisco ATF policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless profile airtime-fairness atf-policy-name 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>atf-policy-name</em>—Enters the ATF profile name.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>atf-profile-id</em>—Enters the ATF profile ID. Range is from 0 to 511.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>weight policy-weight</td>
<td>Adds a weight to the Cisco ATF policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-config-atf)# weight 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>policy-weight</em>—Enters the policy weight. Range is from 5 to 100.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>client-sharing</td>
<td>Enables or disables the client sharing for Cisco ATF policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-config-atf)# client-sharing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-config-atf)# end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Attaching Cisco ATF Policy to a Policy Profile in an AP (GUI)

**Procedure**

**Step 1** Choose the Configuration > Tags & Profiles > Air Time Fairness to configure the following.

**Step 2** 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.

**Step 3** Use the slider to enable or disable the Client Sharing feature.

**Step 4** Click Save & Apply to Device to save your ATF configuration.

**Step 5** To delete a policy, select the check box next to the appropriate policy and click Delete.

**Step 6** To edit an existing ATF policy, select the check box next to the policy you want to edit. Details of the policy are displayed in the Edit ATF Policy window. You can modify the weight for the policy and client sharing detail.

---

**Attaching Cisco ATF Policy to a Policy Profile in an AP**

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless profile policy profile-name</td>
<td>Creates policy profile for the WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless profile policy profile-name</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dot11 {24ghz</td>
<td>5ghz} airtime-fairness atf-policy-name</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# dot11 24ghz airtime-fairness atf-policy-name</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>You can assign the same ATF policy to both 2.4-GHz and 5-GHz radios (or) have two different ATF policies as well.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# end</td>
<td></td>
</tr>
</tbody>
</table>

---

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x
Enabling ATF in RF Profile Associated to an AP

Cisco ATF must be enabled on 2.4- or 5-GHz radios separately.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Example: <code>Device# configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures an RF profile for 2.4- or 5-GHz radio.</td>
</tr>
<tr>
<td>`ap dot11 {24ghz</td>
<td>5ghz} rf-profile rf-profile`</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures air time fairness in either of the modes:</td>
</tr>
<tr>
<td>`airtime-fairness mode {enforce-policy</td>
<td>monitor}`</td>
</tr>
<tr>
<td></td>
<td>• Monitor—This mode gathers information about air time and reports air time usage.</td>
</tr>
<tr>
<td>Example: <code>Device(config-rf-profile)# airtime-fairness mode enforce-policy</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables the air time fairness optimization.</td>
</tr>
<tr>
<td><code>airtime-fairness optimization</code></td>
<td>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.</td>
</tr>
<tr>
<td>Example: <code>Device(config-rf-profile)# airtime-fairness optimization</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Device(config-rf-profile)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Verifying Cisco ATF Configurations**

You can verify Cisco ATF configurations using the following commands:

**Table 40: Commands for Verifying Cisco ATF Configurations**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless profile airtime-fairness summary</code></td>
<td>Displays the summary of air time fairness profiles.</td>
</tr>
<tr>
<td><code>show wireless profile airtime-fairness mapping</code></td>
<td>Displays the ATF policy mapping with the wireless profiles.</td>
</tr>
<tr>
<td><code>show ap airtime-fairness summary</code></td>
<td>Displays the ATF configuration summary of all radios.</td>
</tr>
</tbody>
</table>
Verifying Cisco ATF Statistics

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ap dot11 24ghz airtime-fairness</td>
<td>Displays the ATF configuration for 2.4-GHz radio.</td>
</tr>
<tr>
<td>show ap dot11 5ghz airtime-fairness</td>
<td>Displays the ATF configuration for 5-GHz radio.</td>
</tr>
<tr>
<td>show ap name ap-name airtime-fairness</td>
<td>Displays the ATF configuration or statistics for an AP.</td>
</tr>
<tr>
<td>show ap name ap-name dot11 {24ghz</td>
<td>5ghz} airtime-fairness statistics summary</td>
</tr>
</tbody>
</table>

**Table 41: ATF Statistics per WLAN**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ap name ap-name dot11 {24ghz</td>
<td>5ghz} airtime-fairness wlan wlan_name statistics</td>
</tr>
</tbody>
</table>

**Table 42: ATF Statistics per ATF Policy**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ap name ap-name dot11 {24ghz</td>
<td>5ghz} airtime-fairness policy policy-name statistics</td>
</tr>
</tbody>
</table>

**Table 43: ATF Statistics per Client**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ap airtime-fairness statistics client mac_address</td>
<td>Displays the ATF statistics related to a client.</td>
</tr>
</tbody>
</table>
Verifying Cisco ATF Statistics
PART X

IPv6

• IPv6 Client IP Address Learning, on page 907
• Configuring IPv6 ACL, on page 923
• IPv6 Client Mobility, on page 935
• IPv6 Support on Flex and Mesh, on page 939
• IPv6 CAPWAP UDP Lite Support, on page 943
CHAPTER 103

IPv6 Client IP Address Learning

- Information About IPv6 Client Address Learning, on page 907
- Prerequisites for IPv6 Client Address Learning, on page 910
- Configuring RA Throttle Policy (CLI), on page 911
- Applying RA Throttle Policy on VLAN (GUI), on page 911
- Applying RA Throttle Policy on VLAN (CLI), on page 912
- Configuring IPv6 on Interface, on page 913
- Configuring DHCP Pool on Switch (GUI), on page 914
- Configuring DHCP Pool on Switch, on page 914
- Configuring Stateless Auto Address Configuration Without DHCP on Switch (CLI), on page 915
- Configuring Stateless Auto Address Configuration With DHCP on Switch, on page 916
- Native IPv6, on page 918

Information About IPv6 Client Address Learning

Client Address Learning is configured on device to learn the IPv4 and IPv6 address of the wireless client, and the client's transition state maintained by the device on association, re-association, de-authentication, and timeout.

There are three ways for an IPv6 client to acquire IPv6 addresses:

- Stateless Address Auto-Configuration (SLACC)
- Stateful DHCPv6
- Static Configuration

In all of the methods listed above, the IPv6 client always sends neighbor solicitation DAD (Duplicate Address Detection) request to ensure that there is no duplicate IP address on the network. The device snoops on the NDP and DHCPv6 packets of the client to learn about its client IP addresses.

Note

APs can join IPv6 controllers only with an IPv6 static address. APs with auto configurations and multiple IPv6 addresses cannot join the IPv6 controllers.
SLAAC Address Assignment

The most common method for IPv6 client address assignment is Stateless Address Auto-Configuration (SLAAC). SLAAC provides simple plug-and-play connectivity where clients self-assign an address based on the IPv6 prefix.

Stateless Address Auto-Configuration (SLAAC) is configured as follows:

- Host sends a Router Solicitation message.
- Host waits for a Router Advertisement message.
- Hosts 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.
- The choice of algorithm is up to the client and is often configurable.

The last 64 bits of the IPv6 address can be learned based on the following algorithms:

- EUI-64 which is based on the MAC address of the interface, or
- Private addresses that are randomly generated

Figure 24: SLAAC Address Assignment

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
```
The use of DHCPv6 is not required for IPv6 client connectivity if SLAAC is already deployed. There are two modes of operation for DHCPv6 called 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 as this is already provided by SLAAC. This information includes the DNS domain name, DNS server(s), and other DHCP vendor-specific options.

The following interface configuration is for a Cisco IOS IPv6 router implementing stateless DHCPv6 with SLAAC enabled:

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPPOOL
  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_DHCPPPOOL
ipv6 address 2001:DB8:0:20::1/64
end
```

**Static IP Address Assignment**

Statically configured address on a client.

**Router Solicitation**

A Router Solicitation message is issued by a host controller to facilitate local routers to transmit Router Advertisement from which it 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 hosts 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 ARP, 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 expired from the table according to Neighbor Binding timers.

Neighbor Discovery Suppression

The IPv6 addresses of wireless clients are cached by the device. When the device receives an 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. The result of this process generates the equivalent of the Address Resolution Protocol (ARP) table of IPv4 but is more efficient - uses generally fewer messages.

Note

The device acts like proxy and respond with NA, only when the `ipv6 nd suppress` command is configured.

If the device does not have the IPv6 address of a wireless client, the device will not respond with NA and forward the NS packet to the wireless side. To resolve this, an NS Multicast Forwarding knob is provided. If this knob is enabled, the device gets the NS packet for the IPv6 address that it does not have (cache miss) and forwards it to the wireless side. This packet reaches the intended wireless client and the client replies with NA.

This cache miss scenario occurs rarely, and only very few clients which do not implement complete IPv6 stack may not advertise their IPv6 address during NDP.

RA 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.

RA Throttling

RA throttling allows the controller to enforce limits to RA packets headed toward the wireless network. By enabling RA throttling, routers that send many RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity. If a client sends an RS packet, 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.

**Configuring RA Throttle Policy (CLI)**

Configure RA Throttle policy to allow the enforce the limits

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ipv6 nd ra-throttler policy ra-throttler1</td>
<td>Define the router advertisement (RA) throttl er policy name and enter IPv6 RA throttle policy configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# ipv6 nd ra-throttler policy ra-throttler1</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>throttle-period 500</td>
<td>Configures the throttle period in an IPv6 RA throttle policy.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-nd-ra-throttle)# throttle-period 500</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>max-through 10</td>
<td>Limits multicast RAs per VLAN per throttle period.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-nd-ra-throttle)# max-through 500</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>allow-atleast 5 at-most 10</td>
<td>Limits the number of multicast RAs per device per throttle period in an RA throttle policy.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-nd-ra-throttle)# allow-atleast 5 at-most 10</td>
<td></td>
</tr>
</tbody>
</table>

**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.
- Inherit
- 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 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>vlan configuration 1</td>
<td>Configures a VLAN or a collection of VLANs</td>
</tr>
<tr>
<td>Example:</td>
<td>and enters VLAN configuration mode.</td>
</tr>
<tr>
<td>Device(config)# vlan</td>
<td></td>
</tr>
<tr>
<td>configuration 1</td>
<td></td>
</tr>
</tbody>
</table>

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x
Configuring IPv6 on Interface

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td><code>ipv6 nd ra throttler attach-policy ra-throttler1</code></td>
<td>Attaches an IPv6 RA throttler policy to a VLAN or a collection of VLANs.</td>
</tr>
</tbody>
</table>

Example:
```
Device(config-vlan)# ipv6 nd ra throttler attach-policy ra-throttler1
```
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.

Configuring DHCP Pool on Switch

Follow the procedure given below to configure DHCP Pool on an interface:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 1</th>
<th>enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
</tbody>
</table>

### Purpose

Enables privileged EXEC mode. Enter your password if prompted.

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

Follow the procedure given below to configure stateless auto address configuration without DHCP:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>

### Step 1

enable

Example:

Device> enable

Enables privileged EXEC mode. Enter your password if prompted.
### Purpose

**Command or Action**

**Step 2**

configure terminal  
**Example:**

Device# configure terminal

**Step 3**

interface vlan 1  
**Example:**

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

**Step 5**

ipv6 enable  
**Example:**

Device(config)# ipv6 enable

(Optional) Enables IPv6 on the 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Device&gt; <strong>enable</strong></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# <strong>configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>interface vlan 1</strong></td>
<td>Creates an interface and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# <strong>interface vlan 1</strong></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>ip address fe80::1 link-local</strong></td>
<td>Configures IPv6 address on the interface using the link-local option.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# <strong>ip address</strong> 198.51.100.1 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# <strong>ipv6 address</strong> fe80::1 link-local</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# <strong>ipv6 address</strong> 2001:DB8:0:1:FFFF:1234::5/64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# <strong>ipv6 address</strong> 2001:DB8:0:0:E000::F/64</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>ipv6 enable</strong></td>
<td>(Optional) Enables IPv6 on the interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# <strong>ipv6 enable</strong></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>no ipv6 nd managed-config-flag</strong></td>
<td>Ensures the attached hosts do not use stateful autoconfiguration to obtain addresses.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# <strong>interface vlan 1</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# <strong>no ipv6 nd managed-config-flag</strong></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><strong>ipv6 nd other-config-flag</strong></td>
<td>Ensures the attached hosts do not use stateful autoconfiguration to obtain non-address options from DHCP (domain etc).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# <strong>no ipv6 nd other-config-flag</strong></td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><strong>end</strong></td>
<td>Exits from the interface mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# <strong>end</strong></td>
<td></td>
</tr>
</tbody>
</table>
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

- For IPv6 functionality to work, ensure that you disable IPv6 multicast routing.
- The Wireless Management interface should have only one static IPv6 address.
- IPv6 Neighbor Discovery—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.

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:

All the features and functions that work on IPv4 networks with IPv4 addresses will work on IPv6 networks with IPv6 addresses too.
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ipv6 unicast-routing</td>
<td>Configures IPv6 for unicasting.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# ipv6 unicast-routing</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface vlan 1</td>
<td>Creates an interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface vlan 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ipv6 address ipv6-address</td>
<td>Specifies a global IPv6 address.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ipv6 address FD09:9:2:49::53/64</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ipv6 enable</td>
<td>Enables IPv6 on the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ipv6 enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ipv6 nd ra suppress all</td>
<td>Suppresses IPv6 router advertisement transmissions on the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ipv6 nd ra suppress all</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> wireless management interface gigabitEthernet gigabitEthernet-interface-number &lt;0-1&gt;</td>
<td>Configures the ports that are connected to the supported APs with the wireless management interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless management interface gigabitEthernet 0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> ipv6 route ipv6-address</td>
<td>Specifies IPv6 static routes.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# ipv6 route ::/0 FD09:9:2:49::11</td>
<td></td>
</tr>
</tbody>
</table>
Creating an AP Join Profile (GUI)

Procedure

Step 1  Choose Configuration > Services > AP Join.
Step 2  On the AP Join Profile page, select the General tab and click Add.
Step 3  Enter a name for the AP Join Profile in the Name field.
Step 4  [Optional] Enter a description for the AP Join Profile.
Step 5  Click the CAPWAP > Advanced tab.
Step 6  From the Preferred Mode drop-down list, choose IPv6. Sets the preferred mode of APs as IPv6.
Step 7  Click Save & Apply to Device.

Creating an AP Join Profile (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>ap profile ap-profile</code></td>
<td>Configures an AP profile and enters AP profile configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# ap profile xyz-ap-profile</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>description ap-profile-name</code></td>
<td>Adds a description for the AP profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-ap-profile)# description &quot;xyz ap profile&quot;</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>preferred-mode ipv6</code></td>
<td>Sets the preferred mode of APs as IPv6.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-ap-profile)# preferred-mode ipv6</code></td>
<td></td>
</tr>
</tbody>
</table>

Configuring 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 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 Primary and Backup Controller (CLI)

Follow the procedure given below to configure primary and secondary controllers for a selected access point:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ap profile profile-name</td>
<td>Configures an AP profile and enters the ap profile configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ap profile yy-ap-profile</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>capwap backup primary primary-controller-name primary-controller-ip</td>
<td>Configures ap capwap parameters with the primary backup controller name.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# capwap backup primary WLAN-Controller-A 10.2.3.4</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>ap capwap backup secondary secondary-controller-name secondary-controller-ip</td>
<td>Configures ap capwap parameters with the secondary backup controller name.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# capwap backup secondary WLAN-Controller-B 10.2.3.5</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>syslog host ipaddress</td>
<td>Configure the system logging settings for Cisco AP.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# syslog host 10.5.6.7</td>
<td></td>
</tr>
</tbody>
</table>
Verifying an IPv6 Configuration

Use the following `show` command to verify the IPv6 configuration:

Device# show wireless interface summary

Wireless Interface Summary

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Interface Type</th>
<th>VLAN ID</th>
<th>IP Address</th>
<th>IP Netmask</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan49</td>
<td>Management</td>
<td>49</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>001e.f6c.1eff</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>fd09:9:2:49::54/64</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

### Command or Action | Purpose
---|-------------------
**Step 6** | tftp-downgrade *tftp-server-ip imagename*  
*Example:*  
Device(config)# tftp-downgrade 10.6.7.8  
testimage  
Initiate AP image downgrade from a TFTP server for all Cisco APs.
Configuring IPv6 ACL

- Information About IPv6 ACL, on page 923
- Prerequisites for Configuring IPv6 ACL, on page 924
- Restrictions for Configuring IPv6 ACL, on page 924
- Configuring IPv6 ACLs, on page 925
- How To Configure an IPv6 ACL, on page 926
- Verifying IPv6 ACL, on page 930
- Configuration Examples for IPv6 ACL, on page 930

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 devicend 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 Cisco Secure Access Control Server (Cisco Secure ACS).
The ACE is not configured on the Controller Embedded Wireless 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 device and only the filter-id is configured on the Cisco Secure ACS.

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.

**Downloadable IPv6 ACL**

For the downloadable ACL (dACL), all the full ACEs and the dacl name are configured only on the Cisco Secure ACS.

The Cisco Secure ACS sends the dacl name to the device in its ACCESS-Accept attribute, which takes the dacl name and sends the dACL name back to the Cisco Secure ACS for the ACEs, using the ACCESS-request attribute.

**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 an IPv6 router ACL is configured to deny a packet, the packet is not routed. A copy of the packet is sent to the Internet Control Message Protocol (ICMP) queue to generate an ICMP unreachable message for the frame.

• 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 dropped 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 dropped on the interface.
# How To Configure an IPv6 ACL

## Creating an IPv6 ACL

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td><strong>Device&gt; enable</strong></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><strong>Device# configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ipv6 access-list acl_name</td>
<td>Use a name to define an IPv6 access list and enter IPv6 access-list configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><strong>Device# ipv6 access-list access-list-name</strong></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>{deny</td>
<td>permit} protocol</td>
</tr>
</tbody>
</table>
| Example: | ```
{deny | permit} protocol
{source-ipv6-prefix/prefix-length | any | host source-ipv6-address}
[operator [port-number]]
{destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]]
[dscp value]
[fragments][log] [log-input]
[routing][sequence value]
[time-range name]
``` |

- For protocol, enter the name or number of an Internet protocol: ahp, esp, icmp, ipv6, pcp, step, tcp, or udp, or an integer 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
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>in hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td></td>
<td>• (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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• (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.</td>
</tr>
<tr>
<td></td>
<td>• (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.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Enter fragments to check noninitial fragments. This keyword is visible only if the protocol is ipv6.</td>
</tr>
<tr>
<td></td>
<td>• (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.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Enter routing to specify that IPv6 packets be routed.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Enter sequence value to specify the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Enter time-range name to specify the time range that applies to the deny or permit statement.</td>
</tr>
</tbody>
</table>
### Purpose

Command or Action | Purpose
--- | ---
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.

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\}\}
   \[psh\|\range\{port | protocol\}\]
   \[routing\|sequence value\]
   \[time-range name\]

(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\}
   \{destination-ipv6-prefix/prefix-length | any \| hostdestination-ipv6-address\}
   \[operator \[port-number\]\{icmp-type\]

(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:
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| [icmp-code] [icmp-message] [dscpvalue] [log] [log-input] [routing] [sequence value] [time-range name] | • 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**  
**Example:**  
Device(config)# end  
Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

**Step 9**  
**Example:**  
show ipv6 access-list  
Verify the access list configuration.

**Step 10**  
**Example:**  
copy running-config startup-config  
(Optional) Save your entries in the configuration file.

---

### Creating WLAN IPv6 ACL

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
**Example:**  
DeviceController # configure terminal | Configures the terminal. |
| **Step 2**  
**Example:**  
Device(config)# wireless profile policy profile-name | Creates policy profile for the WLAN. The profile-name is the profile name of the policy profile. |
| **Step 3**  
**Example:**  
Device(config-wireless-policy)# ipv6 acl acl_name | Creates a named WLAN ACL. |
Verifying IPv6 ACL

Displaying IPv6 ACLs

To display IPv6 ACLs, perform this procedure:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>show access-list</td>
<td>Displays all access lists configured on the device</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show access-lists</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show ipv6 access-list acl_name</td>
<td>Displays all configured IPv6 access list or the access list specified by name.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show ipv6 access-list {access-list-name}</td>
<td></td>
</tr>
</tbody>
</table>

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
```

---

**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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>ipv6 nd ra-throttler policy Mythrottle</strong></td>
<td>Creates a RA throttler policy called Mythrottle.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device (config)# ipv6 nd ra-throttler policy Mythrottle</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>throttle-period 20</strong></td>
<td>Determines the time interval segment during which throttling applies.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device (config-nd-ra-throttle)# throttle-period 20</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>max-through 5</strong></td>
<td>Determines how many initial RA’s are allowed.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device (config-nd-ra-throttle)# max-through 5</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>allow at-least 3 at-most 5</strong></td>
<td>Determines how many RA’s are allowed after the initial RA’s have been transmitted, until the end of the interval segment.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device (config-nd-ra-throttle)# allow at-least 3 at-most 5</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>switch (config)# vlan configuration 100</strong></td>
<td>Creates a per vlan configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device (config)# vlan configuration 100</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><strong>ipv6 nd ra-th attach-policy attach-policy_name</strong></td>
<td>Enables the router advertisement throttling.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device (config)# ipv6 nd ra-throttle attach-policy attach-policy_name</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 8**

end

**Example:**

Device(config)# end |

Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Example: Configuring RA Throttling
IPv6 Client Mobility

- Information About IPv6 Client Mobility, on page 935
- Prerequisites for IPv6 Client Mobility, on page 937
- Monitoring IPv6 Client Mobility, on page 938

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 Protocol (NDP) packet management.
- Client IPv6 addresses learning.
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 Advertisement**

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 a new IP address and breaks into L3 mobility’s point of presence.

*Figure 26: Roaming Client Receives Valid RA from Router 1*

**RA Throttling**

To safeguard the power-saving wireless clients form being disturbed by frequent unsolicited periodic RAs, the controller can throttle the unsolicited multicast RA.
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>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless client summary</td>
<td>Displays the wireless specific configuration of active clients.</td>
</tr>
<tr>
<td>show wireless client mac-address (mac-addr-detail)</td>
<td>Displays the wireless specific configuration of active clients based on their MAC address.</td>
</tr>
</tbody>
</table>
IPv6 Support on Flex and Mesh

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface vlan vlan-interface-number</td>
<td>Creates an interface and enters the interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)#interface vlan 89</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> shutdown</td>
<td>Disables the interface configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)#shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ipv6 enable</td>
<td>Enables IPv6 on the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)#ipv6 enable</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Preferred IP Address as IPv6

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Configure Terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> ap profile default-ap-profile</td>
<td>Enters AP profile configuration mode.</td>
</tr>
</tbody>
</table>

---

#### Configuring Preferred IP Address as IPv6

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> ipv6 address $X:Y:Z:W/&lt;0-128&gt;</td>
<td>Configures IPv6 address on the interface using the IPv6 prefix option.</td>
</tr>
<tr>
<td><strong>Step 6</strong> no shutdown</td>
<td>Enables the IPv6 address.</td>
</tr>
<tr>
<td><strong>Step 7</strong> ipv6 mld version version-number</td>
<td>Enables the IPv6 MLD version. The version are either 1 or 2.</td>
</tr>
<tr>
<td><strong>Step 8</strong> ip pim dense-mode</td>
<td>Configures the PIM dense-mode operation.</td>
</tr>
<tr>
<td><strong>Step 9</strong> no shutdown</td>
<td>Enables the PIM dense-mode operation.</td>
</tr>
<tr>
<td><strong>Step 10</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 11</strong> show ipv6 interface brief</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Step 12</strong> ping ipv6 destination-address or hostname</td>
<td>Checks the gateway connectivity.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device(config)# ap profile default-ap-profile</code></td>
<td>Uses IPv6 to join the controller.</td>
</tr>
</tbody>
</table>

**Step 3**

**preferred-mode ipv6**

**Example:**

```
Device(config-ap-profile)# preferred-mode ipv6
```

**Step 4**

**end**

**Example:**

```
Device(config-ap-profile)# end
```

---

### 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
```
Verifying IPv6 on Flex+Mesh
Information About UDP Lite

The UDP Lite Support feature, which is an enhancement to the existing IPv6 functionality, supports the UDP Lite protocol.

This feature is only applicable to the IPv6 addresses of the controller and APs. IPv6 mandates complete payload checksum for UDP. The UDP Lite Support feature minimises the performance impact on the controller and AP by restricting the checksum calculation coverage for the UDP Lite header to 8 bytes only.

The use of the UDP Lite Support feature impacts intermediate firewalls to allow UDP Lite protocol (protocol ID of 136) packets. Existing firewalls might not provide the option to open specific ports on UDP Lite protocol. In such cases, the administrator must open up all the ports on UDP Lite.

Restrictions for UDP Lite Support

- Mobility IPv6 tunnels do not support the UDP Lite Support feature.

Enabling UDP Lite Support

The following procedure describes the steps involved in enabling UDP Lite for an AP profile.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ap profile ap-profile</td>
<td>Configures an AP profile and enters AP profile configuration mode.</td>
</tr>
</tbody>
</table>
### Verifying UDP Lite Support Configuration

To verify the CAPWAP UDP Lite status, use the following command:

```
Device# show ap profile name default-ap-profile detailed
```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# ap profile default-ap-profile</td>
<td>Enables IPv6 CAPWAP UDP Lite on the AP.</td>
</tr>
<tr>
<td><strong>Step 3</strong> capwap udplite</td>
<td>Enables IPv6 CAPWAP UDP Lite on the AP.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-ap-profile)# capwap udplite</td>
<td>The following message is displayed after the configuration: This feature is supported only for IPv6 data packets, APs will be rebooted.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-ap-profile)# end</td>
<td>Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
</tbody>
</table>

---

**Verifying UDP Lite Support Configuration**

To verify the CAPWAP UDP Lite status, use the following command:

```
Device# show ap profile name default-ap-profile detailed
```

```
CAPWAP UDP-Lite: ENABLED
Lawful-Interception: ENABLED
LI timer: 60
AWIPS: DISABLED
AWIPS Forensic: Unknown
Client RSSI Statistics:
  Reporting: ENABLED
  Reporting Interval: 30 seconds
```
PART XI

CleanAir

- Cisco CleanAir, on page 947
- Bluetooth Low Energy, on page 963
- Persistent Device Avoidance, on page 967
- Spectrum Intelligence, on page 971
Cisco CleanAir

• Information About Cisco CleanAir, on page 947
• Prerequisites for CleanAir, on page 950
• Restrictions for CleanAir, on page 951
• How to Configure CleanAir, on page 951
• Verifying CleanAir Parameters, on page 958
• Configuration Examples for CleanAir, on page 961
• CleanAir FAQs, on page 961

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 802.11n 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 45: CleanAir-Related Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AQI</td>
<td>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 &gt; 85 is good.</td>
</tr>
<tr>
<td>AQR</td>
<td>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.</td>
</tr>
<tr>
<td>DC</td>
<td>Duty Cycle. Percentage of time that the channel is utilized by a device.</td>
</tr>
<tr>
<td>EDRRM</td>
<td>Event-Driven RRM. EDRRM allows an access point in distress to bypass normal RRM intervals and immediately change channels.</td>
</tr>
<tr>
<td>IDR</td>
<td>Interference Device Reports that an access point sends to the controller.</td>
</tr>
<tr>
<td>ISI</td>
<td>Interference Severity Index. The ISI is an indicator of the severity of the interference.</td>
</tr>
<tr>
<td>RSSI</td>
<td>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.</td>
</tr>
</tbody>
</table>

Cisco CleanAir Components

The basic Cisco CleanAir architecture consists of Cisco CleanAir-enabled APs and device.

**Figure 27: Cisco CleanAir Solution**

An access point equipped with Cisco CleanAir technology collects information about non-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 DCM. 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.

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.

Spectrum event-driven RRM can be triggered only by Cisco CleanAir-enabled access points in local mode.
All the APs using Qualcomm Atheros chipsets send air-quality as 100 percent even if the radios detect interference.

**Note**

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.

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.
- **FlexConnect**—When a FlexConnect access point is connected to the controller, its Cisco CleanAir functionality is identical to local mode.
- **Monitor**—When Cisco CleanAir is enabled in monitor mode, the access point provides air quality and interference detection reports for all monitored channels.

The following options are available:

- **All**—All channels
- **DCA**—Channel selection governed by the DCA list
- **Country**—All channels are legal within a regulatory domain
Note
Manually reboot the AP once a sensor crash occurs multiple times and AP radio does not come up. The controller does not display any error message.

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.

- Monitor Mode access point in slot 2 operates at 2.4 GHz only.

- We recommend a ratio of 1 monitor-mode access point for every 5 local-mode access points; this can vary based on the network design and expert guidance for best coverage.

- 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Configuration &gt; Radio Configurations &gt; CleanAir</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>On the CleanAir page, click the 2.4 GHz Band &gt; General tab.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Check the Enable CleanAir checkbox.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Apply.</td>
</tr>
</tbody>
</table>

Enabling CleanAir for the 2.4-GHz Band (CLI)

Procedure

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 2 | **ap dot11 24ghz cleanair**<br>**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**<br>**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
### Configuring Interference Reporting for a 2.4-GHz Device (CLI)

**Procedure**

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

**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
- 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 superag

**Purpose**

- 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
- **jammer**—Jammer
- **mw-oven**—Microwave oven
- **nonstd**—Device using nonstandard Wi-Fi channels
- **report**—No description
- **superag**—802.11 SuperAG device
Purpose

Command or Action

device jammer

device mw-oven

device nonstd

device report

device superag

device tdd-tx

device video

device wimax-fixed

device wimax-mobile

device xbox

device zigbee

• tdd-tx—TDD transmitter

• video—Video camera

• wimax-fixed—WiMax Fixed

• wimax-mobile—WiMax Mobile

• xbox—Xbox device

• zigbee—802.15.4 device

---

Step 3

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 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ap dot11 5ghz cleanair</code></td>
<td>Enables the CleanAir feature on a 802.11a network. Run the <code>no</code> form of this command to disable CleanAir on the 802.11a network.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)#ap dot11 5ghz cleanair</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)#no ap dot11 5ghz cleanair</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

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

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
| Step 2 | `ap dot11 5ghz cleanair device {canopy | cont-tx | dect-like | inv | jammer | nonstd | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile}` | 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  
  - `report`—Interference device reporting  
  - `superag`—802.11 SuperAG device  
  - `tdd-tx`—TDD transmitter  
  - `video`—Video camera  
  - `wimax-fixed`—WiMax fixed  
  - `wimax-mobile`—WiMax mobile |

- Video Camera

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

**Step 6** Save the configuration.

### Configuring EDRRM for a CleanAir Event (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables EDRRM CleanAir event. Run the no form of this command to disable EDRRM.</td>
</tr>
<tr>
<td>`ap dot11 {24ghz</td>
<td>5ghz} rrm channel cleanair-event`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# ap dot11 24ghz rrm channel</code></td>
<td></td>
</tr>
</tbody>
</table>
Verifying CleanAir Parameters

You can verify CleanAir parameters using the following commands:

Table 46: Commands for verifying CleanAir

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ap dot11 24ghz cleanair air-quality summary</td>
<td>Displays CleanAir AQ data for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair air-quality worst</td>
<td>Displays CleanAir AQ worst data for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair config</td>
<td>Displays CleanAir configuration for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type all</td>
<td>Displays all the CleanAir interferers for the 2.4-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 24ghz cleanair device type</td>
<td>Displays all the Bluetooth BLE beacons for the 2.4-GHz band.</td>
</tr>
<tr>
<td>ble-beacon</td>
<td></td>
</tr>
<tr>
<td>Command Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type BT Discovery for the 2.4-GHz band.</td>
</tr>
<tr>
<td>bt-discovery</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type BT Link for the 2.4-GHz band.</td>
</tr>
<tr>
<td>bt-link</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type Canopy for the 2.4-GHz band.</td>
</tr>
<tr>
<td>canopy</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type Continuous transmitter for the 2.4-GHz band.</td>
</tr>
<tr>
<td>cont-tx</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type DECT Like for the 2.4-GHz band.</td>
</tr>
<tr>
<td>dect-like</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type 802.11FH for the 2.4-GHz band.</td>
</tr>
<tr>
<td>fh</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type Wi-Fi Inverted for the 2.4-GHz band.</td>
</tr>
<tr>
<td>inv</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type Jammer for the 2.4-GHz band.</td>
</tr>
<tr>
<td>jammer</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type MW Oven for the 2.4-GHz band.</td>
</tr>
<tr>
<td>mw-oven</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type Wi-Fi inverted channel for the 2.4-GHz band.</td>
</tr>
<tr>
<td>nonstd</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type Persistent for the 2.4-GHz band.</td>
</tr>
<tr>
<td>persistent</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type SuperAG for the 2.4-GHz band.</td>
</tr>
<tr>
<td>superag</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type TDD Transmit for the 2.4-GHz band.</td>
</tr>
<tr>
<td>tdd-tx</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type Video Camera for the 2.4-GHz band.</td>
</tr>
<tr>
<td>video</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type WiMax Fixed for the 2.4-GHz band.</td>
</tr>
<tr>
<td>wimax-fixed</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type WiMax Mobile for the 2.4-GHz band.</td>
</tr>
<tr>
<td>wimax-mobile</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type Xbox for the 2.4-GHz band.</td>
</tr>
<tr>
<td>xbox</td>
<td></td>
</tr>
<tr>
<td>show ap dot11 24ghz clean device type</td>
<td>Displays CleanAir interferers of type Zigbee for the 2.4-GHz band.</td>
</tr>
<tr>
<td>zigbee</td>
<td></td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ap dot11 5ghz cleanair air-quality summary</td>
<td>Displays CleanAir AQ data for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz cleanair air-quality worst</td>
<td>Displays CleanAir AQ worst data for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz cleanair config</td>
<td>Displays CleanAir configuration for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz cleanair device type all</td>
<td>Displays all the CleanAir interferers for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz cleanair device type canopy</td>
<td>Displays CleanAir interferers of type Canopy for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz cleanair device type cont-tx</td>
<td>Displays CleanAir interferers of type Continuous TX for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz cleanair device type dect-like</td>
<td>Displays CleanAir interferers of type DECT Like for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz cleanair device type inv</td>
<td>Displays CleanAir interferers of type Wi-Fi Inverted for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz cleanair device type jammer</td>
<td>Displays CleanAir interferers of type Jammer for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz cleanair device type nonstd</td>
<td>Displays CleanAir interferers of type Wi-Fi inverted channel for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz cleanair device type persistent</td>
<td>Displays CleanAir interferers of type Persistent for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz cleanair device type superag</td>
<td>Displays CleanAir interferers of type SuperAG for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz cleanair device type tdd-tx</td>
<td>Displays CleanAir interferers of type TDD Transmit for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz cleanair device type video</td>
<td>Displays CleanAir interferers of type Video Camera for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz cleanair device type wimax-fixed</td>
<td>Displays CleanAir interferers of type WiMax Fixed for the 5-GHz band.</td>
</tr>
<tr>
<td>show ap dot11 5ghz cleanair device type wimax-mobile</td>
<td>Displays CleanAir interferers of type WiMax Mobile for the 5-GHz band.</td>
</tr>
</tbody>
</table>
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.

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. Can I merge two monitor-mode access points using a device?
A. No, you cannot merge two monitor-mode access points using a device.

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

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)

Q. What are the debug commands available for CleanAir?
A. The debug commands for CleanAir are:

- debug cleanair {bringup | event | logdebug | low | major | nsi | offchan}
- debug rrm {neighbor | off-channel | reports}
Bluetooth Low Energy

- Information About Bluetooth Low Energy, on page 963
- Enabling Bluetooth Low Energy Beacon, on page 964

Information About Bluetooth Low Energy

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 is sent to the corresponding back-end server. Relevant advertisements and other important information are then pushed to the devices using this location-specific information.

The BLE feature also provides BLE beacon management support and specifies its behavior when used within the Cisco WLAN system. Using the Cisco CleanAir, an access point can identify an iBeacon signal and decode the payload content. The extracted tag device details are used for better management of the device.

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 whitelist 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.
- The BLE feature on the Cisco Aironet 3700 Series Access Points with Halo module gets deactivated when NTP is configured (This behavior is also observed when Cisco CMX is not present.) So, the legacy BLE does not work when Cisco CMX is present or not configured for Hyperlocation.

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>[no] ap dot11 24ghz cleanair device ble-beacon</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config)# ap dot11 24ghz cleanair device ble-beacon</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>exit</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>show ap dot11 24ghz cleanair config</td>
<td>(Optional) Displays the BLE beacon configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller# show ap dot11 24ghz cleanair config</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interference Device Settings:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interference Device Reporting................ : Enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bluetooth Link............................. : Enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microwave Oven.............................. : Enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BLE Beacon.................................... : Enabled</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show ap dot11 24ghz cleanair device type ble-beacon</td>
<td>(Optional) Displays the BLE beacon device-type information.</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

Controller# show ap dot11 24ghz cleanair device type ble-beacon

<table>
<thead>
<tr>
<th>DC</th>
<th>ISI</th>
<th>RSSI</th>
<th>DevID</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0xa001</td>
<td>-74</td>
<td>unknown</td>
<td>BLE Beacon</td>
</tr>
<tr>
<td>5508_3_AP3600_f839</td>
<td>--</td>
<td>--74</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

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
Persistent Device Avoidance

Persistent device avoidance (PDA) feature is a part of spectrum management. Some interference devices such as outdoor bridges and microwave ovens transmit signals only when required. These devices can cause significant interference to the local WLAN, since short duration and periodic operation remain largely undetected by normal RF management metrics. With Cisco CleanAir (CleanAir) the RRM dynamic channel allocation (DCA) algorithm can detect, measure, register, and remember the impact and adjust the RRM DCA algorithm. This process minimizes the use of channels affected by the persistent devices in the channel plan, local to the interference source. CleanAir detects and stores persistent device information in the controller. This information is used to mitigate interfering channels.

**Persistent Devices Detection** - CleanAir-capable monitor mode APs collect information about persistent devices on all configured channels and stores the information in the controller. Local or bridge mode APs detect interference devices on the serving channels only.

The PDA feature works seamlessly on all platforms. All the AP models that are capable of CleanAir and Spectrum Intelligence support the PDA feature.

The supported platforms are:

- Cisco Aironet 1852 Access Point
- Cisco Aironet 1832 Access Point
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points
- Cisco Catalyst 9115 Access Points
- Cisco Catalyst 9117 Access Points
• Cisco Catalyst 9120 Access Points
• Cisco Catalyst 9130 Access Points

Configuring Persistent Device Avoidance (CLI)

You can enable and disable the PDA feature and PDA propagation configuration mode through the RRM manager.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>[no] ap dot11 {24ghz</td>
<td>5ghz} rrm channel device</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# [no] ap dot11 24ghz rrm channel device</td>
<td></td>
</tr>
</tbody>
</table>

Verifying Persistent Device Avoidance

To verify the current state of Device Aware, use the following command:

Device#sh ap dot11 24ghz channel
Leader Automatic Channel Assignment
  Channel Assignment Mode : AUTO
  Channel Update Interval : 600 seconds
  Anchor time (Hour of the day) : 0
  Channel Update Contribution
    Noise : Enable
    Interference : Enable
    Load : Disable
  **Device Aware** : **Enable**
CleanAir Event-driven RRM option : Disabled
Channel Assignment Leader : saji-vwlc (9.9.39.73)
Last Run : 166 seconds ago

DCA Sensitivity Level : MEDIUM : 10 dB
DCA Minimum Energy Limit : -95 dBm
Channel Energy Levels
  Minimum : -82 dBm
  Average : -82 dBm
  Maximum : -82 dBm
Channel Dwell Times
  Minimum : 8 days 0 hour 43 minutes 13 seconds
  Average : 8 days 0 hour 43 minutes 13 seconds
  Maximum : 8 days 0 hour 43 minutes 13 seconds

802.11b 2.4 GHz Auto-RF Channel List
Allowed Channel List: 1, 6, 11
Unused Channel List: 2, 3, 4, 5, 7, 8, 9, 10

To verify all the reported interferers along with the class type, use the following command:

```
Device#show ap dot11 24ghz cleanair device type all
DC = Duty Cycle (%), NA for SI APs
ISI = Interference Severity Index (1-Low Interference, 100-High Interference), NA for SI APs
RSSI = Received Signal Strength Index (dBm)
DevID = Device ID
```

<table>
<thead>
<tr>
<th>ClusterID</th>
<th>Mac Address</th>
<th>DevID</th>
<th>Type</th>
<th>AP Name</th>
<th>ISI</th>
<th>RSSI</th>
<th>DC Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>a100.0000.0000</td>
<td>42f3.38e8.0001</td>
<td>0xa001</td>
<td>MW Oven</td>
<td>CA</td>
<td>11</td>
<td>-81</td>
<td>9 11</td>
</tr>
<tr>
<td>a100.0000.0002</td>
<td>8bc5.4740.3001</td>
<td>0x3001</td>
<td>MW Oven</td>
<td>CA</td>
<td>13</td>
<td>-21</td>
<td>14 11</td>
</tr>
<tr>
<td>a100.0000.0001</td>
<td>e647.20e0.3001</td>
<td>0x3001</td>
<td>MW Oven</td>
<td>CA</td>
<td>18</td>
<td>-31</td>
<td>12 11</td>
</tr>
</tbody>
</table>

To verify the persistent device information under Auto-RF, use the following command:

```
Device#show ap auto-rf dot11 24ghz
Number of Slots: 2
AP Name: VANC-AP
MAC Address: d4c9.3ce5.c760
Slot ID: 0
Radio Type: 802.11n - 2.4 GHz
```

<table>
<thead>
<tr>
<th>Persistent Interference Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Type</td>
</tr>
<tr>
<td>MW Oven</td>
</tr>
<tr>
<td>MW Oven</td>
</tr>
<tr>
<td>MW Oven</td>
</tr>
<tr>
<td>MW Oven</td>
</tr>
</tbody>
</table>

To verify the persistent device information under Auto-RF for specific Cisco APs, use the following command:

```
Device#show ap name ap_name auto-rf dot11 24ghz
Number of Slots: 2
AP Name: VANC-AP
MAC Address: d4c9.3ce5.c760
Slot ID: 0
Radio Type: 802.11n - 2.4 GHz
```

<table>
<thead>
<tr>
<th>Persistent Interference Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Type</td>
</tr>
<tr>
<td>MW Oven</td>
</tr>
<tr>
<td>MW Oven</td>
</tr>
<tr>
<td>MW Oven</td>
</tr>
<tr>
<td>MW Oven</td>
</tr>
</tbody>
</table>
Verifying Persistent Device Avoidance
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 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

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 DNA 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.
- 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:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ap dot11 {24ghz</td>
<td>5ghz} SI</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap dot11 24ghz SI</td>
<td>Add no form of the command to disable SI on the 802.11a or 802.11b network.</td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>DC</th>
<th>ISI</th>
<th>RSSI</th>
<th>DC</th>
<th>Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>-----</td>
<td>------</td>
<td>----</td>
<td>---------</td>
</tr>
<tr>
<td>133</td>
<td>69</td>
<td>-69</td>
<td>133</td>
<td>-69</td>
</tr>
</tbody>
</table>

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 977
CHAPTER 112

Mesh Access Points

- Introduction to Mesh, on page 978
- Restrictions, on page 979
- MAC Authorization, on page 979
- Preshared Key Provisioning, on page 980
- EAP Authentication, on page 980
- Bridge Group Names, on page 981
- Background Scanning, on page 981
- Mesh Backhaul at 2.4-GHz and 5-GHz, on page 982
- Dynamic Frequency Selection, on page 982
- Country Codes, on page 982
- Intrusion Detection System, on page 982
- Mesh Interoperability Between Controllers, on page 983
- Mesh Convergence, on page 983
- Ethernet Bridging, on page 984
- Multicast Over Mesh, on page 984
- Radio Resource Management on Mesh, on page 985
- Air Time Fairness on Mesh, on page 985
- Spectrum Intelligence for Mesh, on page 986
- Indoor Mesh Interoperability with Outdoor Mesh, on page 986
- Workgroup Bridge, on page 987
- Link Test, on page 987
- Mesh Daisy Chaining, on page 987
- Mesh Leaf Node, on page 988
- Flex+Bridge Mode, on page 988
- Backhaul Client Access, on page 988
- GPS Support for Outdoor APs, on page 989
- Mesh AP Battery Status, on page 989
- Mesh CAC, on page 989
- Configuring MAC Authorization, on page 990
- Configuring PSK Provisioning, on page 991
- Configuring a Bridge Group Name, on page 992
- Configuring Background Scanning, on page 993
- Configuring Backhaul Client Access, on page 993
Introduction to Mesh

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 a 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

This 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 1572 Mesh Access Points

- Indoor APs
  - Cisco Aironet 2700 Mesh Access Points
  - Cisco Aironet 3700 Mesh Access Points

- Cisco Wave 2 APs
  - Cisco Aironet 1542 Mesh Access Points
  - Cisco Aironet 1562 Mesh 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.

---

MAC Authorization

The MAC address of an AP should be entered 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 access point.

MAC authorization for MAPs connected to the controller over Ethernet takes place during the CAPWAP join process. For MAPs that join the controller over radio, MAC authorization takes place when the corresponding AP tries to secure a WPP link with the parent MAP.

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 wildcard 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.

## 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 802.11a. 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 an 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.

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.

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>
<thead>
<tr>
<th>Mesh Convergence</th>
<th>Parent Loss Detection / Keepalive Timers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>21 / 3 seconds</td>
</tr>
<tr>
<td>Fast</td>
<td>7 / 3 seconds</td>
</tr>
<tr>
<td>Very Fast</td>
<td>4 / 2 seconds</td>
</tr>
<tr>
<td>Noise-tolerant-fast</td>
<td>21 / 3 seconds</td>
</tr>
</tbody>
</table>

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 two 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, using `ap exec` commands. 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

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 video camera broadcasts 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:
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 EDRRM.

Note that no specific configuration options are available to enable or disable CleanAir for MAPs.

**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.

An autonomous AP functions as a workgroup bridge. Only one radio interface is used for controller connectivity, Ethernet interface for wired client connectivity, and other radio interface for wireless client connectivity.

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**

The Cisco Aironet 1530 Series Access Points 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 Cisco Aironet 1530 Series Access Point 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 Master AP to the PoE in a port of the Slave AP.

The following are the guidelines for the daisy chaining mode:
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.

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 slave AP and its child APs in daisy-chained deployment, reboot.
GPS Support for Outdoor APs

In an expanding network, keeping track of the location of outdoor APs is quite a task for the operators. As a solution to this problem, some of the Cisco Aironet APs are shipped with GPS receiver and antenna. The coordinates of the GPS in an AP is used by the controller or management system to locate each device on a map. Use the `show` commands to get information about the location of the APs.

Mesh AP Battery Status

Some of the Cisco outdoor APs, such as Cisco Aironet 1532, comes with the option of battery backup. The APs also have a PoE out that can power the video surveillance camera. The integrated battery can be used for temporary backup power during external power interruptions.

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 and video 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

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>username user-name mac</code></td>
<td>Configures user name authentication for MAC filtering where username is MAC address.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# username 11:22:33:44:55:66 mac</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>aaa authorization credential-download method-name local</code></td>
<td>Configures a named authorization list for downloading EAP credential from the local database.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# aaa authorization credential-download list1 local</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>aaa authorization dot1x method-name local</code></td>
<td>Sets authentication lists for IEEE 802.1x as local username authentication.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# aaa authentication dot1x auth1 local</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>aaa authorization dot1x method-name radius group server-group-name</code></td>
<td>Sets authentication lists for IEEE 802.1x for authentication using the RADIUS server group.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# aaa authentication dot1x auth1 radius group radius-server-1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>aaa authorization credential-download method-name radius group server-group-name</code></td>
<td>Downloads EAP credentials from the RADIUS server for authorization using the server group.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# aaa authorization credential-download auth1 radius group radius-server-1</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring PSK Provisioning

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 is pushed to all the APs that are configured with PSK as mesh security.

- 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td><code>wireless profile mesh profile-name</code></td>
<td>Configures a mesh profile and enters mesh profile configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td><code>security eap</code></td>
<td>Configures the mesh security EAP for mesh AP.</td>
</tr>
<tr>
<td>4</td>
<td><code>method authentication method-name</code></td>
<td>Configures the authorization method for mesh AP authentication.</td>
</tr>
<tr>
<td>5</td>
<td><code>method authorization method-name</code></td>
<td>Configures the authorization method for mesh AP authorization.</td>
</tr>
</tbody>
</table>
### Configuring a Bridge Group Name

**Before you begin**

- 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>wireless profile mesh profile-name</code></td>
<td>Configures a mesh profile and enters mesh profile configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# wireless profile mesh profile-name</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Background Scanning

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device(config)# wireless profile mesh mesh1</code></td>
<td>Configures a mesh profile and enters mesh profile configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures background scanning in mesh deployments.</td>
</tr>
<tr>
<td><code>Device(config-wireless-mesh-profile)# bridge-group name bgn1</code></td>
<td>Configures a bridge group name.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures background scanning in mesh deployments.</td>
</tr>
<tr>
<td><code>Device(config)# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>Device(config)# wireless profile mesh profile-name</code></td>
<td>Configures a mesh profile and enters mesh profile configuration mode.</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>Device(config)# wireless profile mesh profile-name</code></td>
<td>Configures a mesh profile and enters mesh profile configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures background scanning in mesh deployments.</td>
</tr>
<tr>
<td><code>Device(config-wireless-mesh-profile)# background-scanning</code></td>
<td>Configures background scanning in mesh deployments.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Backhaul Client Access

Follow the procedure given below to enable backhaul client access on a mesh profile:

**Before you begin**

Backhaul client access is disabled by default. After it is enabled, all the MAPs, except slave AP and its child APs in daisy-chained deployment, reboot.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device(config)# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>Device(config)# wireless profile mesh profile-name</code></td>
<td>Configures a mesh profile and enters mesh profile configuration mode.</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td>Configures background scanning in mesh deployments.</td>
</tr>
<tr>
<td><code>Device(config-wireless-mesh-profile)# background-scanning</code></td>
<td>Configures background scanning in mesh deployments.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Configuring Wireless Backhaul Data Rate

Backhaul is used to create wireless connection between the 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 higher data rates, for example, 1300 Mbps. As a result, the data rate affects cell coverage, and consequently, the number of APs required.

Follow the procedure given below to configure wireless backhaul data rate in privileged EXEC mode or in mesh profile configuration mode.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures backhaul transmission rate.</td>
</tr>
<tr>
<td>ap name ap-name mesh backhaul rate {auto</td>
<td>dot11abg</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# #ap name ap1 mesh backhaul rate auto</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures a mesh profile and enters mesh profile configuration mode.</td>
</tr>
<tr>
<td>wireless profile mesh profile-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless profile mesh mesh1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures backhaul transmission rate.</td>
</tr>
<tr>
<td>backhaul rate dot11 {24ghz</td>
<td>5ghz} dot11n RATE_6M</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-mesh-profile)# backhaul rate dot11 5ghz dot11n RATE_6M</td>
</tr>
</tbody>
</table>
Configuring Dynamic Frequency Selection

DFS specifies the types of radar waveforms that should be detected along with certain timers for an unlicensed operation in the DFS channel.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless profile mesh profile-name</td>
<td>Configures a mesh profile and enters mesh profile configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless profile mesh mesh1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> full-sector-dfs</td>
<td>Enables DFS.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-mesh-profile)# full-sector-dfs</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the Intrusion Detection System

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless profile mesh profile-name</td>
<td>Configures a mesh profile and enters mesh profile configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless profile mesh mesh1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ids</td>
<td>Configures intrusion detection system reporting for outdoor mesh APs.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-mesh-profile)# ids</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Ethernet Bridging

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 bridge VLAN aware. Ensure that VLAN transparency is disabled.
- 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+Bridge APs, configure the native VLAN ID under the corresponding flex profile.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
- enable
  
  Example: Device# enable
  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. |
### Configuring Multicast over Mesh

#### Before you begin
- 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless profile mesh profile-name</td>
<td>Configures a mesh profile and enters mesh profile configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# wireless profile mesh mesh1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>multicast {in-only</td>
<td>in-out</td>
</tr>
<tr>
<td>Example: Device(config-wireless-mesh-profile)# multicast regular</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring RRM on Mesh Backhaul

Follow the procedure given below to enable RRM in the mesh backhaul:

#### Before you begin
The RRM measurement in the mesh AP backhaul is enabled based on the following conditions:
Mesh Access Points

- Mesh AP has the Root AP role.
- Root AP has joined using an Ethernet link.
- Root AP is not serving any child AP.

### Selecting a Preferred Parent

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>wireless mesh backhaul rrm</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config)# wireless mesh backhaul rrm</td>
</tr>
</tbody>
</table>

### Changing an AP's Role

Follow the procedure to change the AP to RAP or vice-versa:

By default, APs join the controller in a mesh AP role.
### Configuring the Mesh Leaf Node

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ap name ap-name role {mesh-ap</td>
<td>root-ap}</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# ap name ap1 root-ap</td>
<td></td>
</tr>
</tbody>
</table>

#### 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.

Follow the procedure given below to configure subset channel synchronization for mobility group:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Provisioning LSC for Bridge-Mode and Mesh APs

Follow the procedure given below to configure LSC for bridge-mode and mesh APs:

**Before you begin**
- 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.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>ap lsc-provision</code></td>
<td>Configures LSC provisioning on an AP.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ap lsc-provision</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>ap lsc-provision provision-list</code></td>
<td>(Optional) Configures LSC provision for all the APs in the provision list.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ap lsc-provision provision-list</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>aaa authentication dot1x auth-list radius group radius-server-grp</code></td>
<td>Configures named authorization list for downloading EAP credential from radius group server.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# aaa authentication dot1x list1 radius group sg1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>wireless profile mesh profile-name</code></td>
<td>Configures a mesh profile and enters mesh profile configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless profile mesh mesh1</td>
<td></td>
</tr>
</tbody>
</table>
Specifying the Backhaul Slot for the Root AP

Follow the procedure given below to set the mesh backhaul rate:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Sets the mesh backhaul rate as auto.</td>
</tr>
<tr>
<td>ap name ap-name  mesh backhaul rate {auto</td>
<td>dot11abg</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# ap name ap1 mesh backhaul rate auto</td>
<td></td>
</tr>
</tbody>
</table>

Using a Link Test on Mesh Backhaul

Follow the procedure given below to trigger linktest between neighbor mesh APs:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
</tbody>
</table>

**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.
Purpose
Command or Action | Purpose
---|---
Sets link test parameters.
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

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
Step 1 | configure terminal
Example:
Device# configure terminal
Eners 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 Mesh CAC

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
Step 1 | configure terminal
Example:
Device# configure terminal
Eners global configuration mode.|
Step 2 | wireless mesh cac
Example: Enables mesh CAC mode.|

Configuring ATF on Mesh

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 ap dot11 {24ghz</td>
<td>5ghz} rf-profile rf-profile</td>
</tr>
<tr>
<td>Example: Device(config)# ap dot11 24ghz rf-profile rfprof24_1</td>
<td></td>
</tr>
<tr>
<td>Step 3 airtime-fairness bridge-client-access airtime-allocation allocation-weight-weight-percentage</td>
<td>Configures airtime allocation weight percentage on mesh APs.</td>
</tr>
<tr>
<td>Example: Device(config-rf-profile)# airtime-fairness bridge-client-access airtime-allocation 10</td>
<td></td>
</tr>
</tbody>
</table>

Create an ATF Policy for a MAP

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 wireless profile policy profile-policy</td>
<td>Configures WLAN policy profile and enters wireless policy configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# wireless profile policy rr-xyz-policy-1</td>
<td></td>
</tr>
<tr>
<td>Step 3 dot11 24ghz airtime-fairness atf-policy</td>
<td>Enables ATF in the existing RF profile.</td>
</tr>
<tr>
<td>Example: Device(config-wireless-policy)# dot11 24ghz airtime-fairness atf-policy</td>
<td></td>
</tr>
</tbody>
</table>
Creating an ATF Policy (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Configuration &gt; Air Time Fairness &gt; Profiles.</td>
</tr>
<tr>
<td>2</td>
<td>On the Profiles window, click Add.</td>
</tr>
<tr>
<td>3</td>
<td>In the Add ATF Policy window, specify a name, ID, and weight for the ATF policy.</td>
</tr>
<tr>
<td>Note</td>
<td>Weighted ratio is used instead of percentages so that the total can exceed 100. The minimum weight that you can set is 5.</td>
</tr>
<tr>
<td>4</td>
<td>Use the slider to enable or disable the Client Sharing feature.</td>
</tr>
<tr>
<td>5</td>
<td>Click Save &amp; Apply to Device to save your ATF configuration.</td>
</tr>
<tr>
<td>6</td>
<td>(Optional) To delete a policy, check the check box next to the appropriate policy and click Delete.</td>
</tr>
<tr>
<td>7</td>
<td>(Optional) To edit an existing ATF policy, select the check box next to the policy you want to edit.</td>
</tr>
</tbody>
</table>

In the Edit ATF Policy window that is displayed, you can modify the weight and client sharing details for the policy.

Adding an ATF to a Policy Profile (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Configuration &gt; Tags &amp; Profiles &gt; Policy.</td>
</tr>
<tr>
<td>2</td>
<td>Click the name of the corresponding policy profile.</td>
</tr>
<tr>
<td>3</td>
<td>Click the Advanced tab.</td>
</tr>
<tr>
<td>4</td>
<td>In the Air Time Fairness Policies section, choose the appropriate status for the following: 2.4-GHz Policy and 5-GHz Policy.</td>
</tr>
<tr>
<td>5</td>
<td>Click Update &amp; Apply to Device.</td>
</tr>
</tbody>
</table>

Enabling ATF Mode in an RF Profile (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Configuration &gt; Tags &amp; Profiles &gt; RF.</td>
</tr>
<tr>
<td>2</td>
<td>Click the name of the corresponding RF profile.</td>
</tr>
</tbody>
</table>
Step 3 In the RF Profile window, click the Advanced tab.

Step 4 In the ATF Configuration section, choose the appropriate status for the following:

- **Status**—If you choose Enabled as the status, select the Mode as either Monitor or Enforced. Also, you can enable or disable optimization for this mode.

- **Bridge Client Access**

- **Airtime Allocation**—Enter the allocation value. You can set the value only after you enable the Bridge Client Access.

Step 5 Click Update & Apply to Device.

---

### Verifying ATF Configuration on Mesh

You can verify Cisco ATF configurations on mesh APs using the following commands.

Use the following `show` command to display the ATF configuration summary of all the radios:

```
Device# show ap airtime-fairness summary
```

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Optimization</th>
<th>MAC Address</th>
<th>Slot</th>
<th>Admin</th>
<th>Oper</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap1/2</td>
<td>Enabled</td>
<td>6c:99:89:0c:73:a0 0</td>
<td>ENABLED</td>
<td>DOWN</td>
<td>Enforce-Policy</td>
<td></td>
</tr>
<tr>
<td>ap1/2</td>
<td>Enabled</td>
<td>6c:99:89:0c:73:a0 1</td>
<td>ENABLED</td>
<td>UP</td>
<td>Enforce-Policy</td>
<td></td>
</tr>
<tr>
<td>ap1/3</td>
<td>Enabled</td>
<td>6c:99:89:0c:73:a1 0</td>
<td>ENABLED</td>
<td>DOWN</td>
<td>Enforce-Policy</td>
<td></td>
</tr>
<tr>
<td>ap1/3</td>
<td>Enabled</td>
<td>6c:99:89:0c:73:a1 1</td>
<td>ENABLED</td>
<td>UP</td>
<td>Enforce-Policy</td>
<td></td>
</tr>
</tbody>
</table>

Use the following `show` command to display the ATF configuration for a 2.4-GHz radio:

```
Device# show ap dot11 24ghz airtime-fairness
```

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Optimization</th>
<th>MAC Address</th>
<th>Slot</th>
<th>Admin</th>
<th>Oper</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap1/2</td>
<td>Enabled</td>
<td>6c:99:89:0c:73:a0 1</td>
<td>ENABLED</td>
<td>UP</td>
<td></td>
<td>Enforce-Policy</td>
</tr>
</tbody>
</table>

Use the following `show` command to display the ATF WLAN statistics:

```
Device# show ap name ap1 dot11 24ghz airtime-fairness wlan 12 statistics
```

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Optimization</th>
<th>MAC Address</th>
<th>Slot</th>
<th>Admin</th>
<th>Oper</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap1/2</td>
<td>Enabled</td>
<td>6c:99:89:0c:73:a0 0</td>
<td>ENABLED</td>
<td>DOWN</td>
<td></td>
<td>Enforce-Policy</td>
</tr>
<tr>
<td>ap1/2</td>
<td>Enabled</td>
<td>6c:99:89:0c:73:a0 1</td>
<td>ENABLED</td>
<td>UP</td>
<td></td>
<td>Enforce-Policy</td>
</tr>
</tbody>
</table>

Use the following `show` command to display the wireless mesh summary:
Device# show wireless profile mesh summary

Number of Profiles: 2

<table>
<thead>
<tr>
<th>Profile-Name</th>
<th>BGN</th>
<th>Security</th>
<th>Bh-access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mesh1</td>
<td></td>
<td>EAP</td>
<td>DISABLED</td>
<td></td>
</tr>
<tr>
<td>default-mesh-profile</td>
<td></td>
<td>EAP</td>
<td>DISABLED</td>
<td>default mesh profile</td>
</tr>
</tbody>
</table>

Device# show mesh atf client-access

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Client Access Allocation Default %</th>
<th>Override</th>
<th>Current %</th>
<th>Current nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAP</td>
<td></td>
<td></td>
<td>25</td>
<td>4</td>
</tr>
<tr>
<td>RAP</td>
<td></td>
<td></td>
<td>33</td>
<td>3</td>
</tr>
</tbody>
</table>

Verifying Mesh Configuration

Use the following show commands to verify the various aspects of mesh configuration.

For details about these commands, see the Cisco Catalyst 9800 Series Wireless Controller Command Reference document.

- 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
Verifying Mesh Configuration
PART XIII

VideoStream

• VideoStream, on page 1011
CHAPTER 113

VideoStream

- Information about Media Stream, on page 1011
- Prerequisites for Media Stream, on page 1011
- How to Configure Media Stream, on page 1012
- Monitoring Media Streams, on page 1017
- Adding Media Stream (GUI), on page 1017
- Adding Media Stream (CLI), on page 1018
- Enabling a Media Stream per WLAN (GUI), on page 1019
- Enabling a Media Stream per WLAN, on page 1019
- Configuring the General Parameters for a Media Stream (GUI), on page 1020
- Configuring the General Parameters for a Media Stream, on page 1020
- Configuring Multicast Direct Admission Control, on page 1021
- Viewing Media Stream Information, on page 1022

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.

Note

Support for IPv6 was added from Cisco IOS XE Gibraltar 16.12.1. You can use IPv6 multicast addresses in place of IPv4 multicast addresses to enable media stream on the IPv6 networks.

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.
How to Configure Media Stream

Configuring Multicast-Direct Globally for Media Stream

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless multicast</td>
<td>Enables multicast for wireless forwarding.</td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless multicast</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ip igmp snooping</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip igmp snooping</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>ip igmp snooping querier</td>
<td>Configures a snooping querier on an interface when there is no multicast router in the VLAN to generate queries.</td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip igmp snooping querier</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>wireless media-stream multicast-direct</td>
<td>Configures the global multicast-direct on the controller.</td>
</tr>
<tr>
<td></td>
<td>(config)#wireless media-stream multicast-direct</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>wireless media-stream message</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>(config)#wireless media-stream message ?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Email Configure Session Announcement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Notes Configure Session Announcement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL Configure Session Announcement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>phone Configure Session Announcement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;cr&gt;</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Media Stream for 802.11 Bands

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ap dot11 {24ghz</td>
<td>5ghz} media-stream multicast-direct</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ap dot11 24ghz media-stream multicast-direct</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ap dot11 {24ghz</td>
<td>5ghz} media-stream video-redirect</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ap dot11 24ghz media-stream video-redirect</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} media-stream multicast-direct admission-besteffort`</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# ap dot11 24ghz media-stream multicast-direct admission-besteffort</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} media-stream multicast-direct client-maximum [value]`</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# ap dot11 24ghz media-stream multicast-direct client-max 15</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} media-stream multicast-direct radio-maximum [value]`</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# ap dot11 24ghz media-stream multicast-direct radio-maximum 20</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} cac multimedia max-bandwidth [bandwidth]`</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# ap dot11 24ghz cac multimedia max-bandwidth 60</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} cac media-stream multicast-direct min_client_rate [dot11_rate]`</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# ap dot11 24ghz cac media-stream multicast-direct min_client_rate</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ap dot11 5ghz cac media-stream</code></td>
<td>Configures Call Admission Control (CAC) parameters for media stream access category.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# ap dot11 5ghz cac media-stream</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ap dot11 5ghz cac multimedia</code></td>
<td>Configures CAC parameters for media access category: used for voice and video.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# ap dot11 5ghz cac multimedia</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ap dot11 5ghz cac video</code></td>
<td>Configures CAC parameters for video access category: used for voice signaling.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# ap dot11 5ghz cac video</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a WLAN to Stream Video (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configuration &gt; Wireless &gt; WLANs &gt; Wireless Networks</strong>.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Select a <strong>WLAN</strong> to view the <strong>Edit WLAN</strong> window.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Advanced</strong> tab.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Check the <strong>Media Stream Multicast-Direct</strong> check box to enable the feature.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Update &amp; Apply to Device</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring a WLAN to Stream Video (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>wlan wlan_name</strong></td>
<td>Enters WLAN configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>(config)# wlan wlan50</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>shutdown</strong></td>
<td>Disables the WLAN for configuring its parameters.</td>
</tr>
<tr>
<td>Example:</td>
<td>(config-wlan)# shutdown</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>media-stream multicast-direct</strong></td>
<td>Configures the multicast-direct on media stream for the WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>(config)# media-stream multicast-direct</td>
<td></td>
</tr>
</tbody>
</table>

**Purpose**

- Configures CAC parameters for voice access category.
- 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 adjacent 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

Before you begin

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> no wireless media-stream group</td>
<td>Deletes the media stream that bears the name mentioned in the command.</td>
</tr>
<tr>
<td>media_stream_name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# no wireless media-stream grp1</td>
<td></td>
</tr>
</tbody>
</table>
Purpose
Command or Action | Purpose
--- | ---
Step 3 end | Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Monitoring Media Streams

Table 48: Commands for monitoring media streams

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless media-stream client detail <em>group name</em></td>
<td>Displays media stream client details of the particular group.</td>
</tr>
<tr>
<td>show wireless media-stream client summary</td>
<td>Displays the media stream information of all the clients.</td>
</tr>
<tr>
<td>show wireless media-stream group detail <em>group name</em></td>
<td>Displays the media stream configuration details of the particular group.</td>
</tr>
<tr>
<td>show wireless media-stream group summary</td>
<td>Displays the media stream configuration details of all the groups.</td>
</tr>
<tr>
<td>show wireless media-stream message details</td>
<td>Displays the session announcement message details.</td>
</tr>
<tr>
<td>show wireless multicast</td>
<td>Displays the multicast-direct configuration state.</td>
</tr>
<tr>
<td>show ap dot11 {24ghz</td>
<td>5ghz} media-stream rrc</td>
</tr>
</tbody>
</table>

Adding 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.
Adding Media Stream (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>wireless media-stream group groupName startIpAddr endIpAddr</code></td>
<td>Configures each media stream and its parameters, such as expected multicast destination addresses, stream bandwidth consumption, and stream priority parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# wireless media-stream group group1 224.0.0.0 224.0.0.223</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>avg-packet-size packetsize</code></td>
<td>Configures the average packet size.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(media-stream)# avg-packet-size 100</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>max-bandwidth bandwidth</code></td>
<td>Configures the maximum expected stream bandwidth, in Kbps.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(media-stream)# max-bandwidth 80</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`policy { admit</td>
<td>deny }`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(media-stream)# policy admit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>qos video</code></td>
<td>Configures over-the-air QoS class, as 'video'.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(media-stream)# qos video</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>`violation { drop</td>
<td>fallback }`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(media-stream)# violation drop</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>`rrc-evaluation { initial</td>
<td>periodic }`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(media-stream)# rrc-evaluation initial</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>priority priority-value</code></td>
<td>Sets the priority value. The valid range is from 1-8, with 1 being the lowest.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(media-stream)# priority 6</code></td>
<td></td>
</tr>
</tbody>
</table>
# Enabling a Media Stream per WLAN (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configuration &gt; Tags &amp; Profiles &gt; WLANs</strong>.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>On the <strong>WLANs</strong> page, click the name of the <strong>WLAN</strong> or click <strong>Add</strong> to create a new one.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Add/Edit WLAN</strong> window that is displayed, click the <strong>Advanced</strong> tab.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Check the <strong>Enabling a Media Stream for each WLAN</strong> check box to enable Media Stream on the WLAN.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Save the configuration.</td>
<td></td>
</tr>
</tbody>
</table>

---

# Enabling a Media Stream per WLAN

Follow the procedure given below to enable a media stream for each WLAN:

**Procedure**

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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

Follow the procedure given below to configure the general parameters for a media stream:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless media-stream message { URL url</td>
<td>Configures various message configuration parameters, such as phone, URL, email, and notes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>notes }</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# wireless media-stream message url <a href="http://www.xyz.com">www.xyz.com</a></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>wireless media-stream multicast-direct</td>
<td>Enables multicast direct globally for local mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# wireless media-stream multicast-direct</td>
<td>Note: This configuration will not impact flex and fabric media-stream configurations.</td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Multicast Direct Admission Control

Follow the procedure given below to configure multicast direct admission control:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} shutdown`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# ap dot11 24ghz shutdown</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} media-stream video-redirect`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# ap dot11 24ghz media-stream video-redirect</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} cac media-stream acm`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# ap dot11 24ghz cac media-stream acm</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} cac media-stream max-bandwidth bandwidth`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# ap dot11 24ghz cac media-stream max-bandwidth 65</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} cac multimedia max-bandwidth bandwidth`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# ap dot11 24ghz cac multimedia max-bandwidth 65</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>`ap dot11 {24ghz</td>
<td>5ghz} cac media-stream multicast-direct min-client-rate dot11Rate`</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Device(config)# ap dot11 24ghz cac media-stream multicast-direct min-client-rate 800</td>
<td>Typically, this PHY rate is equal to or higher than the rate at which multicast frames are sent.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> ap dot11 {24ghz</td>
<td>5ghz} cac media-stream multicast-direct max-retry-percent retryPercent</td>
<td>Configures CAC parameter maximum retry percent for multicast-direct streams.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ap dot11 24ghz cac media-stream multicast-direct max-retry-percent 50</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> ap dot11 {24ghz</td>
<td>5ghz} media-stream multicast-direct radio-maximum value</td>
<td>Configures the maximum number of radio streams. The range is from 1 to 20. Default is 0. Value 0 denotes unlimited streams.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ap dot11 24ghz media-stream multicast-direct radio-maximum 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> ap dot11 {24ghz</td>
<td>5ghz} media-stream multicast-direct client-maximum value</td>
<td>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.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ap dot11 24ghz media-stream multicast-direct client-maximum 12</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> ap dot11 {24ghz</td>
<td>5ghz} media-stream multicast-direct admission-besteffort</td>
<td>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.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ap dot11 24ghz media-stream multicast-direct admission-besteffort</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> no ap dot11 {24ghz</td>
<td>5ghz} shutdown</td>
<td>Enables the 802.11b network.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# no ap dot11 24ghz shutdown</td>
<td></td>
</tr>
</tbody>
</table>

**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:
```

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x
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 mediastream 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 blacklisted clients in the 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
PART XIV

Software-Defined Access Wireless

- Software-Defined Access Wireless, on page 1027
- Configuring Passive Client on Software Defined Access [SDA-Wireless], on page 1037
- Configuring Encrypted Traffic Analytics on Software Defined Access (SDA-Wireless), on page 1045
Software-Defined Access Wireless

- Information to Software-Defined Access Wireless, on page 1027
- Configuring SD-Access Wireless, on page 1030
- Verifying SD-Access Wireless, on page 1034

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 DNA Center, and Host Tracking Database (HDB).
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 topology 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 topology 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 topology is depicted in the right-most part of the figure.

**Cisco DNA Center**: Is an open, software-driven architecture built on a set of design principles with the objective of configuring and managing 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 49: Supported Platforms for Software-Defined Access Wireless*

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 9300</td>
<td>Yes</td>
</tr>
<tr>
<td>Catalyst 9400</td>
<td>Yes</td>
</tr>
<tr>
<td>Catalyst 9500H</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Catalyst 9800 Series Wireless Controller for Cloud</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Catalyst 9800-40 Series Wireless Controller</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Catalyst 9800-80 Series Wireless Controller</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*Table 50: Multi-Instance Support*

<table>
<thead>
<tr>
<th>Multi-instance</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple LISP sessions</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Multi-instance Support

<table>
<thead>
<tr>
<th>Feature</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emulated database support</td>
<td>Yes</td>
</tr>
<tr>
<td>Client roaming between WNCD instances</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*Table 51: Feature Support*

<table>
<thead>
<tr>
<th>Feature</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inter-WLC roam for IRCM</td>
<td>Only L2 mobility is supported as VLAN is stretched across the fabric.</td>
</tr>
<tr>
<td>DNS-IPv4-ACL</td>
<td>• ACLs are enforced at AP.</td>
</tr>
<tr>
<td></td>
<td>• Controller needs to push the DNS-ACL information to AP.</td>
</tr>
<tr>
<td>IPv6 ACL for clients</td>
<td>Yes. Open, 802.11x, WebbAuth, PSK WLANs, IPv6 address visibility are also supported.</td>
</tr>
<tr>
<td>Location tracking/Hyperlocation</td>
<td>Yes</td>
</tr>
<tr>
<td>Multicast Video-Stream (IPv4)</td>
<td>Yes</td>
</tr>
<tr>
<td>Smart Licensing</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*Table 52: Outdoor Access Points Support*

<table>
<thead>
<tr>
<th>AP</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>1542</td>
<td>Yes</td>
</tr>
<tr>
<td>1560</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Configuring SD-Access Wireless

To enable SD-Access wireless globally, you need to execute the following configuration command:

```
wireless fabric
```

### Configuring Default Map Server (GUI)

**Procedure**

1. **Step 1** Click *Configuration > Wireless Plus > Fabric > Fabric Configuration*.
2. **Step 2** In the *Map Server* section, specify the IP address and preshared key details for Server 1.
3. **Step 3** Optionally, you can specify the IP address and preshared key details for Server 2.
Configuring Default Map Server (CLI)

Follow the procedure given below to configure default map server:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wireless fabric control-plane map-server-name</td>
<td>Configures the default map server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless fabric control-plane map-server-name</td>
<td>Here, map-server-name defines a pair of map servers.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip address ip-address key user_password reenter_password</td>
<td>Configures IP address for the default map server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-cp)# ip address 200.0.0.0 key user_password user_password</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-cp)# end</td>
<td></td>
</tr>
</tbody>
</table>

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
Configuring SD-Access Wireless Profile (CLI)

Follow the procedure given below to configure SD-Access wireless profile:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wireless profile fabric fabric-profile-name</code></td>
<td>Configures the SD-Access wireless profile parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless profile fabric fabric-profile-name</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>sgt-tag sgt</code></td>
<td>Configures SGT tag.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Here, <code>sgt</code> refers to the sgt tag value. The valid range is from 2-65519. The default value is 0. Device(config-wireless-fabric)# sgt-tag 2</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>client-l2-vnid client-l2-vnid</code></td>
<td>Configures client L2-VNID.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Here, <code>client-l2-vnid</code> refers to the client L2-VNID value. The valid range is from 0-16777215. Device(config-wireless-fabric)# client-l2-vnid client-l2-vnid</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Alternatively, you can also press Ctrl-Z to exit global configuration mode. Device(config-wireless-fabric)# end</td>
<td></td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configuration &gt; Tags &amp; Profiles &gt; Tags</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the <strong>Manage Tags</strong> page, click the <strong>Site</strong> tab.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the name of the site tag.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless tag site site-tag</td>
<td>Configures site tag.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless tag site</td>
<td>Here, <em>site-tag</em> refers to the site tag name.</td>
</tr>
<tr>
<td>default-site-tag</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> fabric control-plane map-server-name</td>
<td>Configures fabric control plane details.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-site-tag)# fabric</td>
<td>Here, <em>map-server-name</em> refers to the fabric</td>
</tr>
<tr>
<td>control-plane map-server-name</td>
<td>control plane name associated with the site tag.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
<tr>
<td>Device(config-site-tag)# end</td>
<td></td>
</tr>
</tbody>
</table>

---

**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**

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

**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

Here,

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

Verifying SD-Access Wireless

You can verify the SD-Access wireless configurations using the following commands:

**Table 53: Commands for Verifying SD-Access Wireless**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless fabric summary</td>
<td>Displays the fabric status.</td>
</tr>
<tr>
<td>show wireless fabric vnid mapping</td>
<td>Displays all the VNID mapping details.</td>
</tr>
<tr>
<td>show wireless profile fabric detailed fabric_profile_name</td>
<td>Displays the details of a given fabric profile name.</td>
</tr>
<tr>
<td>show ap name AP_name config general</td>
<td>Displays the general details of the Cisco AP.</td>
</tr>
<tr>
<td>show wireless client mac MAC_addr detail</td>
<td>Displays the detailed information for a client by MAC address.</td>
</tr>
<tr>
<td>Commands</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>show wireless tag site detailed site_tag</td>
<td>Displays the detailed parameters for a site tag.</td>
</tr>
</tbody>
</table>
CHAPTER 115

Configuring Passive Client on Software Defined Access [SDA-Wireless]

- Information About Passive Clients, on page 1037
- Enabling Passive Client on WLAN Policy Profile (GUI), on page 1038
- Enabling Passive Client on WLAN Policy Profile (CLI), on page 1038
- Enabling ARP Broadcast on VLAN (GUI), on page 1039
- Enabling ARP Broadcast on VLAN (CLI), on page 1039
- Configuring Passive Client in Fabric Deployment, on page 1039
- Verifying Passive Client Configuration, on page 1043

Information About Passive Clients

Passive Clients are wireless devices, such as printers and devices configured using a static IP address. Such clients when associated to an AP do not transmit any IP information. That is why, the controller does not know the IP address unless they use the DHCP.

In the controller, the clients just show up in the Learn IP state and get timed out because of the DHCP policy-timeout.

To establish TCP or IP communication with such clients, you need to perform the following:

- Configure the Passive Client for each wireless profile.
- Use the WLAN-VLAN mapping to plumb VLAN details to which the WLAN is being mapped.
- Stop the DHCP timer for clients associated to the WLAN.

Note

You need to enable the following for passive client feature to work:

- ARP broadcast on VLANs
- LISP multicast. For information on LISP multicast, see:
  
For information on LISP (Locator ID Separation Protocol), see:

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless profile policy default-policy-profile</td>
<td>Configures the default policy profile.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless profile policy default-policy-profile</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# [no] passive-client</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# end</td>
<td></td>
</tr>
</tbody>
</table>
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)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device# configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong> vlan configuration vlan-id</td>
<td>Configures a VLAN or a collection of VLANs and enters VLAN configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config)# vlan configuration 1</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong> [no] arp broadcast</td>
<td>Enables ARP broadcast on VLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config-vlan)# [no] arp broadcast</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config-vlan)# end</strong></td>
</tr>
</tbody>
</table>

Configuring Passive Client in Fabric Deployment

Enabling Broadcast Underlay on VLAN

**Note**
You can perform the following configuration tasks from Fabric Edge Node only and not from your controller.
### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FabricEdge# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>router lisp</code></td>
<td>Enters LISP configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FabricEdge(config)# router lisp</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>instance-id instance</code></td>
<td>Creates a LISP EID instance to group multiple services. Configurations</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>under this instance-id are applicable to all services underneath it.</td>
</tr>
<tr>
<td></td>
<td>FabricEdge(config-router-lisp)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>instance-id 3</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>service ipv4</code></td>
<td>Enables Layer 3 network services for the IPv4 address family and enters</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>the service submode.</td>
</tr>
<tr>
<td></td>
<td>FabricEdge(config-router-lisp-instance)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>service ipv4</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>database-mapping eid locator-set RLOC</code></td>
<td>Configures EID to RLOC mapping relationship.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FabricEdge(config-router-lisp-instance)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>database-mapping 66.66.66.64/32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>locator-set rloc1</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>map-cache destination-eid map-request</code></td>
<td>Generates a static map request for the destination EID.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FabricEdge(config-router-lisp-instance-service)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>map-cache 0.0.0.0/0 map-request</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>exit-service-ipv4</code></td>
<td>Exits service submode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FabricEdge(config-router-lisp-instance-service)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit-service-ipv4</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>exit-instance-id</code></td>
<td>Exits instance submode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FabricEdge(config-router-lisp-instance)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit-instance-id</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td><code>instance-id instance</code></td>
<td>Creates a LISP EID instance to group multiple services.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FabricEdge(config-router-lisp)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>instance-id 101</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>10</td>
<td>service ethernet</td>
<td>Enables Layer 2 network services and enters service submode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FabricEdge(config-router-lisp-instance)# service ethernet</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>eid-table vlan vlan-number</td>
<td>Associates the LISP instance-id configured earlier with a VLAN through which the endpoint identifier address space is reachable.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FabricEdge(config-router-lisp-instance-service)# eid-table vlan 101</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>broadcast-underlay multicast-group</td>
<td>Specifies the multicast group used by the underlay to carry the overlay Layer 2 broadcast traffic.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FabricEdge(config-router-lisp-instance-service)# broadcast-underlay 239.0.0.1</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>exit-service-ethernet</td>
<td>Exits service sub mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FabricEdge(config-router-lisp-instance-service)# exit-service-ethernet</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>exit-instance-id</td>
<td>Exits instance sub mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FabricEdge(config-router-lisp-instance)# exit-instance-id</td>
<td></td>
</tr>
</tbody>
</table>

### Enabling ARP Flooding

**Note**

You can perform the following configuration tasks from Fabric Edge Node only and not from your controller.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FabricEdge# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>router lisp</td>
<td>Enters LISP configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FabricEdge(config)# router lisp</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>3</td>
<td><code>instance-id instance</code></td>
<td>Creates a LISP EID instance to group multiple services. Configurations under this instance-id are applicable to all services underneath it.</td>
</tr>
<tr>
<td>4</td>
<td><code>service ipv4</code></td>
<td>Enables Layer 3 network services for the IPv4 address family and enters the service submode.</td>
</tr>
<tr>
<td>5</td>
<td><code>database-mapping eid locator-set RLOC name</code></td>
<td>Configures EID to RLOC mapping relationship.</td>
</tr>
<tr>
<td>6</td>
<td><code>map-cache destination-eid map-request</code></td>
<td>Generates a static map request for the destination EID.</td>
</tr>
<tr>
<td>7</td>
<td><code>exit-service-ipv4</code></td>
<td>Exits service submode.</td>
</tr>
<tr>
<td>8</td>
<td><code>exit-instance-id</code></td>
<td>Exits instance submode.</td>
</tr>
<tr>
<td>9</td>
<td><code>instance-id instance</code></td>
<td>Creates a LISP EID instance to group multiple services.</td>
</tr>
<tr>
<td>10</td>
<td><code>service ethernet</code></td>
<td>Enables Layer 2 network services and enters service submode.</td>
</tr>
<tr>
<td>11</td>
<td><code>eid-table vlan vlan-number</code></td>
<td>Associates the LISP instance-id configured earlier with a VLAN through which the endpoint identifier address space is reachable.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 12</th>
<th>flood arp-nd</th>
<th>Enables ARP flooding.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>FabricEdge(config-router-lisp-instance-service)# flood arp-nd</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 13</th>
<th>database-mapping mac locator-set RLOC name</th>
<th>Configures EID to RLOC mapping relationship.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>FabricEdge(config-router-lisp-instance-service)# database-mapping mac locator-set rloc1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 14</th>
<th>exit-service-ethereum</th>
<th>Exits service sub mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>FabricEdge(config-router-lisp-instance-service)# exit-service-ethereum</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 15</th>
<th>exit-instance-id</th>
<th>Exits instance sub mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>FabricEdge(config-router-lisp-instance)# exit-instance-id</td>
<td></td>
</tr>
</tbody>
</table>

### 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
```

```plaintext
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
WLAN ACL
  IPv4 ACL : Not Configured
  IPv6 ACL : Not Configured
  Layer2 ACL : Not Configured
WLAN Timeout
  Session Timeout : 1800
  Idle Timeout : 300
  Idle Threshold : 0
```

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 116

Configuring Encrypted Traffic Analytics on Software Defined Access (SDA-Wireless)

• Information About Encrypted Traffic Analytics, on page 1045
• Exporting Records to IPv4 Flow Export Destination, on page 1046
• Exporting Records to IPv6 Flow Export Destination, on page 1047
• Exporting Records to IPv4 and IPv6 Destination over IPFIX, on page 1047
• Whitelisting Traffic, on page 1048
• Configuring Source Interface for Record Export, on page 1049
• Configuring Source Interface for Record Export Without IPFIX, on page 1050
• Configuring ETA Flow Export Destination (GUI), on page 1051
• Enabling In-Active Timer, on page 1052
• Enabling ETA on WLAN Policy Profile, on page 1052
• Attaching Policy Profile to VLAN (GUI), on page 1053
• Attaching Policy Profile to VLAN, on page 1053
• Verifying ETA Configuration, on page 1054

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.
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.

Starting from Cisco IOS XE Amsterdam 17.1.1s, ETA inspection for IPv6 traffic is supported. ETA inspection for IPv6 traffic is enabled by default and no special configuration is required. This release also supports whitelisting of IPv6 traffic, exporting ETA records to IPv4 or IPv6 export destination, exporting records over IPFIX (netflow v10), and configuring source interface for ETA exports. The records can be exported to IPv4 or IPv6 netflow collector.

## Exporting Records to IPv4 Flow Export Destination

Follow the procedure given below to enable encrypted traffic analytics and configure a flow export destination:

### Procedure

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

| **Step 2**          |                                                   |
| et-analytics        | Enables encrypted traffic analytics.              |
| **Example:**        |                                                   |
| Device(config)# et-analytics |                               |
Exporting Records to IPv6 Flow Export Destination

Follow the procedure given below to enable encrypted traffic analytics and configure an IPv6 flow export destination.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| configure terminal | Enters the global configuration mode. |
| Example: Device# configure terminal |
| **Step 2**
| et-analytics | Enables encrypted traffic analytics. |
| Example: Device(config)# et-analytics |
| **Step 3**
| ipv6 flow-export destination ipv6-address port-number | Specifies netflow record export destination IPv6 address and port. |
| Example: Device(config-et-analytics)# ipv6 flow-export destination 2001:181:181::1 2055 |
| **Note** | The maximum configurable limit for flow-export destinations is four (both IPv4 and IPv6 combined). |
| **Step 4**
| exit | Returns to global configuration mode. |
| Example: Device(config-et-analytics)# exit |

Exporting Records to IPv4 and IPv6 Destination over IPFIX

This procedure provides efficient bandwidth utilization by allowing variable len fields for smaller data packets and also reduces the overall bandwidth requirements for transmission.
### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>et-analytics</td>
<td>Enables encrypted traffic analytics.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# et-analytics</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ip flow-export destination ip-address port-number ipfix</td>
<td>Specifies netflow record export destination IP address, port and format.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-et-analytics)# ip flow-export destination 192.168.19.2 2055 ipfix</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>ipv6 flow-export destination ipv6-address port-number ipfix</td>
<td>Specifies netflow record export destination IPv6 address, port and format.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-et-analytics)# ipv6 flow-export destination 2001:181:181::1 2055 ipfix</td>
<td>IPFIX allows you to collect flow information from network devices that support IPFIX protocol and analyze the traffic flow information by processing it through a netflow analyzer.</td>
</tr>
<tr>
<td>Step 5</td>
<td>exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-et-analytics)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Whitelisting Traffic

Follow the procedure given below to whitelist traffic:

You can add whitelist ACL for both IPv4 and IPv6 traffic. Whitelisted traffic is skipped from ETA inspection and records are not generated for the matching traffic.

**Before you begin**

Configure an IPv4 or IPv6 access list.

- IPv4 ACL: `ip access-list standard acl_name`
  
  `Device(config)# ip access-list standard eta-whitelist_ipv4`
### IPv6 ACL: `ipv6 access-list acl_name`

Device(config)# ipv6 access-list eta-whitelist_ipv6

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>et-analytics</td>
<td>Enables encrypted traffic analytics.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# et-analytics</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>whitelist acl acl-name</td>
<td>Configures whitelist traffic ACL for IPv4 or IPv6.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-et-analytics)# whitelist acl eta-whitelist</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You cannot whitelist both IPv4 and IPv6 client traffic simultaneously, as a single ACL cannot have both IPv4 and IPv6 terms.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-et-analytics)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>sequence sequence-num permit udp any any eq tftp</td>
<td>(Optional) Configures a sequence number and the access conditions to whitelist any IPv6 TFTP traffic.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-ipv6-acl)# sequence 10 permit udp any any eq tftp</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Source Interface for Record Export

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>et-analytics</td>
<td>Enables encrypted traffic analytics.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# et-analytics</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Source Interface for Record Export Without IPFIX

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>et-analytics</td>
<td>Enables encrypted traffic analytics.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# et-analytics</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip flow-export destination <em>ip-address</em> &lt;br&gt;source-interface <em>interface-name</em> &lt;br&gt;interface-number ipfix</td>
<td>Specifies netflow record export destination IP address, source interface and format.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-et-analytics)# ip flow-export destination 192.168.19.2 2055 &lt;br&gt;source-interface loopback0 ipfix</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Source Interface for Record Export Without IPFIX

#### Purpose

- **Step 3**: Specifies netflow record export destination IP address, source interface and format. This allows the ETA export to use the IP address of the specified interface, as against using the IP address of the egress interface as the source address.
- **Note**: Only one source interface can be specified and all exports use this source address.

- **Step 4**: Specifies netflow record export destination IPv6 address, source interface and format. The source interface is applicable for both IPv4 and IPv6 export destinations.

- **Step 5**: Returns to global configuration 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**  
From the **Whitelist ACL** drop-down list, choose the desired option.

**Note**  
To use this option, ensure that you select **Encrypted Traffic Analytics** from the **Netflow Template** drop-down list.

**Step 6**  
Enter a port number in the **Exporter Port** field. You must specify a value between 1 and 65535.

**Step 7**  
Choose the desired option from the **Export Interface IP** drop-down list.

**Step 8**  
Choose any one of the sampling methods from the **Sampling Method** drop-down list. The available options are **Deterministic**, **Random**, and **Full Netflow**.

**Step 9**  
Enter a range for the sample. You must specify a value between 32 and 1032.

**Step 10**  
Select the required interfaces/profile from the **Available** pane and move it to the **Selected** pane.

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

---

**Command or Action**

```
Device(config-et-analytics)# ip
flow-export destination 192.168.19.2 2055
source-interface loopback0 ipfix
```

**Purpose**

Specifies netflow record export destination IPv6 address, source interface and format.

**Step 4**

```
ipv6 flow-export destination ipv6-address
source-interface interface-name
interface-number ipfix
```

**Example:**

```
Device(config-et-analytics)# ipv6
flow-export destination 2001:181:181::1
2055
source-interface Vlan160
```

**Step 5**

```
exit
```

**Example:**

```
Device(config-et-analytics)# exit
```
Enabling In-Active Timer

Follow the procedure given below to enable in-active timer:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>et-analytics</code></td>
<td>Configures the encrypted traffic analytics.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>et-analytics</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>inactive-timeout timeout-in-seconds</code></td>
<td>Specifies the inactive flow timeout value.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-et-analytics)# <code>inactive-timeout 15</code></td>
<td>Here, <code>timeout-in-seconds</code> ranges from 1 to 604800.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-et-analytics)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>

Enabling ETA on WLAN Policy Profile

Follow the procedure given below to enable ETA on WLAN policy profile:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>wireless profile policy profile-name</code></td>
<td>Creates policy profile for the WLAN. The <code>profile-name</code> is the profile name of the policy profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>wireless profile policy default-policy-profile</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>et-analytics enable</code></td>
<td>Enables encrypted traffic analytics on the policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# <code>et-analytics enable</code></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>

### Attaching Policy Profile to VLAN (GUI)

Perform the following steps to attach a policy profile to VLAN.

**Procedure**

**Step 1** Check the **RADIUS Profiling** 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 Multicast 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**

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

**Step 2** Creates policy profile for the WLAN. The **profile-name** is the profile name of the policy profile.

wireless profile policy *profile-name*

Example:

Device(config)# wireless profile policy default-policy-profile

**Step 3** Assigns the policy profile to the VLANs.

vlan *vlan-name*

Example:

Device(config-wireless-policy)# vlan *vlan-name*
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
```

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:
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 SPLIT records exported:
  - initiator->responder: 1285146
  - responder->initiator: 979284
- Total SALT records exported:
  - initiator->responder: 0
  - responder->initiator: 0
- Total BD records exported: 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
```

<table>
<thead>
<tr>
<th>Policy Profile Name</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>default-policy-profile</td>
<td>ENABLED</td>
</tr>
</tbody>
</table>
### Verifying ETA Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>160</td>
</tr>
<tr>
<td>Multicast VLAN</td>
<td>0</td>
</tr>
<tr>
<td>Passive Client</td>
<td>DISABLED</td>
</tr>
<tr>
<td>ET Analytics</td>
<td>DISABLED</td>
</tr>
<tr>
<td>StaticIP Mobility</td>
<td>DISABLED</td>
</tr>
<tr>
<td><strong>WLAN Switching Policy</strong></td>
<td></td>
</tr>
<tr>
<td>Central Switching</td>
<td>ENABLED</td>
</tr>
<tr>
<td>Central Authentication</td>
<td>ENABLED</td>
</tr>
<tr>
<td>Central DHCP</td>
<td>ENABLED</td>
</tr>
<tr>
<td>Flex NAT PAT</td>
<td>DISABLED</td>
</tr>
<tr>
<td>Central Assoc</td>
<td>ENABLED</td>
</tr>
</tbody>
</table>

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
cgac1 w0: 0x0
cgac1 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
```

<table>
<thead>
<tr>
<th>CPP</th>
<th>IF_H</th>
<th>DPIIX</th>
<th>MAC Address</th>
<th>VLAN</th>
<th>AS</th>
<th>MS</th>
<th>WLAN</th>
<th>POA</th>
</tr>
</thead>
<tbody>
<tr>
<td>0X2A</td>
<td>0XA0000001</td>
<td>2c33.7a5b.827b</td>
<td>160</td>
<td>RN</td>
<td>LC</td>
<td>xyz_ssid</td>
<td>0x90000003</td>
<td></td>
</tr>
<tr>
<td>0X2B</td>
<td>0XA0000002</td>
<td>2c33.7a5b.80fb</td>
<td>160</td>
<td>RN</td>
<td>LC</td>
<td>xyz_ssid</td>
<td>0x90000003</td>
<td></td>
</tr>
</tbody>
</table>

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_TV1_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_REFRA (M)
- IPV4_TV1_OUTPUT_FIA >>> ETA FIA Enabled
- WLCLIENT_EGRESS_IPV4_FWD
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

<table>
<thead>
<tr>
<th>Counter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable ETA on wireless client called</td>
<td>0</td>
</tr>
<tr>
<td>Delete ETA on wireless client called</td>
<td>0</td>
</tr>
<tr>
<td>ETA global cfg init cb TVI FIA enable error</td>
<td>0</td>
</tr>
<tr>
<td>ETA global cfg init cb output SB read error</td>
<td>0</td>
</tr>
<tr>
<td>ETA global cfg init cb output SB write error</td>
<td>0</td>
</tr>
<tr>
<td>ETA global cfg init cb input SB read error</td>
<td>0</td>
</tr>
<tr>
<td>ETA global cfg init cb input SB write error</td>
<td>0</td>
</tr>
<tr>
<td>ETA global cfg init cb TVI FIA enable success</td>
<td>0</td>
</tr>
<tr>
<td>ETA global cfg uninit cb ingress feat disable</td>
<td>0</td>
</tr>
<tr>
<td>ETA global cfg uninit cb egress cfg delete e</td>
<td>0</td>
</tr>
<tr>
<td>ETA global cfg uninit cb egress feat disable</td>
<td>0</td>
</tr>
<tr>
<td>ETA global cfg uninit cb egress cfg delete er</td>
<td>0</td>
</tr>
<tr>
<td>ETA pending list insert entry called</td>
<td>4</td>
</tr>
<tr>
<td>ETA pending list insert invalid arg error</td>
<td>0</td>
</tr>
<tr>
<td>ETA pending list insert entry exists error</td>
<td>0</td>
</tr>
<tr>
<td>ETA pending list insert no memory error</td>
<td>0</td>
</tr>
<tr>
<td>ETA pending list insert entry failed</td>
<td>0</td>
</tr>
<tr>
<td>ETA pending list insert entry success</td>
<td>4</td>
</tr>
<tr>
<td>ETA pending list delete entry called</td>
<td>2</td>
</tr>
<tr>
<td>ETA pending list delete invalid arg error</td>
<td>0</td>
</tr>
<tr>
<td>ETA pending list delete entry missing</td>
<td>0</td>
</tr>
<tr>
<td>ETA pending list delete entry remove error</td>
<td>0</td>
</tr>
<tr>
<td>ETA pending list delete entry success</td>
<td>2</td>
</tr>
</tbody>
</table>

To view the whitelist configuration, use the following commands:

```
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

```
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: True
cgac1 w0 : 0xd9ae9c80
cgac1 w1 : 0x20000000

Flow CFG information :
instance ID : 0x0
feature ID : 0x0
feature object ID : 0x0
To view the ETA export statistics, use the following command:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath stats export
```

ET-Analytics 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

To view the ETA datapath runtime detail, 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 : True
cgacl w0 : 0xd9ae1e10
cgacl w1 : 0x20000000
Flow CFG information :
  instance ID : 0x0
  feature ID : 0x0
  feature object ID : 0x0
  chunk ID : 0x4
Verifying ETA Configuration
PART XV

VLAN

• Configuring VLANs, on page 1063
• VLAN Groups, on page 1075
Configuring VLANs

- Prerequisites for VLANs, on page 1063
- Restrictions for VLANs, on page 1063
- Information About VLANs, on page 1064
- How to Configure VLANs, on page 1067
- Monitoring VLANs, on page 1074

### Prerequisites for VLANs

The following are prerequisites and considerations for configuring VLANs:

- Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration for your network.

- If you plan to configure many VLANs on the device and to not enable routing, you can set the Switch Database Management (SDM) feature to the VLAN template, which configures system resources to support the maximum number of unicast MAC addresses.

- A VLAN should be present in the device to be able to add it to the VLAN group.

### 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 number of device per-VLAN spanning-tree (PVST) or rapid PVST is based on the number of trunks on the switch multiplied by the number of active VLANs on the trunks, plus the number of non-trunking interfaces on the switch (trunks * VLANS + non-trunk ports). For MSTP, the maximum number of MST instances supported is 4094.

- The device supports IEEE 802.1Q trunking methods for sending VLAN traffic over Ethernet ports.

- When client VLAN is not configured for a WLAN, AP native VLAN is used.
Before logging into the Web UI, you must change the Virtual Terminal (VTY) lines to 30. 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 get exhausted. Therefore, you must change the VTY lines to 30 before using the Web UI.

**Note**

To increase the VTY lines in a device, run the following command in the configuration mode:

```
Device(config)#line vty 0 30
```

---

# 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 device 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 device supporting fallback bridging. Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of spanning tree.

VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the device is assigned manually on an interface-by-interface basis. When you assign device interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Traffic between VLANs must be routed.

The device can route traffic between VLANs by using device virtual interfaces (SVIs). An SVI must be explicitly configured and assigned an IP address to route traffic between VLANs.

## Supported VLANs

The device 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. VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs. 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 device learns and manages the addresses associated with the port on a per-VLAN basis.
### Table 54: Port Membership Modes and Characteristics

<table>
<thead>
<tr>
<th>Membership Mode</th>
<th>VLAN Membership Characteristics</th>
<th>VTP Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static-access</td>
<td>A static-access port can belong to one VLAN and is manually assigned to that VLAN.</td>
<td>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 device connected to a trunk port of a second device.</td>
</tr>
<tr>
<td>Trunk (IEEE 802.1Q): • IEEE 802.1Q— Industry-standard trunking encapsulation.</td>
<td>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. You can also modify the pruning-eligible list to block flooded traffic to VLANs on trunk ports that are included in the list.</td>
<td>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 devices over trunk links.</td>
</tr>
<tr>
<td>Voice VLAN</td>
<td>A voice VLAN port is an access port attached to a Cisco IP Phone, configured to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone.</td>
<td>VTP is not required; it has no effect on a voice VLAN.</td>
</tr>
</tbody>
</table>

### 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 device 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 device, the device 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.
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**

Normal-range VLANs are VLANs with IDs from 1 to 1005.

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 numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.

- 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 device running configuration file.

- If the device 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.

- Before you can create a VLAN, the device must be in VTP server mode or VTP transparent mode. If the device is a VTP server, you must define a VTP domain or VTP will not function.

- The device does not support Token Ring or FDDI media. The device does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it does propagate the VLAN configuration through VTP.

- A fixed number of spanning tree instances are supported on the device (See the datasheet for the latest information). If the device has more active VLANs than the supported number of spanning tree instances, spanning tree is still enabled only on the supported number of VLANs and disabled on all remaining VLANs.

If you have already used all available spanning-tree instances on a device, adding another VLAN anywhere in the VTP domain creates a VLAN on that device that is not running spanning-tree. If you have the default allowed list on the trunk ports of that device (which is to allow all VLANs), the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that would not be broken, particularly if there are several adjacent devices that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of devices that have used up their allocation of spanning-tree instances.

If the number of VLANs on the device exceeds the number of supported spanning-tree instances, we recommend that you configure the IEEE 802.1s Multiple STP (MSTP) on your device to map multiple VLANs to a single spanning-tree instance.

**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.

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
  • Fiber Distributed Data Interface [FDDI]
  • FDDI network entity title [NET]
  • TrBRF or TrCRF
  • Token Ring
  • Token Ring-Net

• VLAN state (active or suspended)

• Security Association Identifier (SAID)

• Bridge identification number for TrBRF VLANs

• Ring number for FDDI and TrCRF VLANs

• Parent VLAN number for TrCRF VLANs

• Spanning Tree Protocol (STP) type 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 device is in VTP transparent mode, you can assign VLAN IDs greater than 1006, but they are not added to the VLAN database.

The device supports only Ethernet interfaces. Because FDDI and Token Ring VLANs are not locally supported, you only configure FDDI and Token Ring media-specific characteristics for VTP global advertisements to other devices.

Although the device does not support Token Ring connections, a remote device with Token Ring connections could be managed from one of the supported devices. Devices running VTP Version 2 advertise information about these Token Ring VLANs:

- Token Ring TrBRF VLANs
- Token Ring TrCRF VLANs

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  * configure terminal
  * Example:
    * Device# configure terminal |
| Enters global configuration mode. |
| **Step 2**
  * 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 3**
  * 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 4**
  * media { ethernet | fd-net | fddi | tokenring | trn-net }
  * Example:
    * Device(config-vlan)# media ethernet |
| Configures the VLAN media type. Command options include:  
  * ethernet—Sets the VLAN media type as Ethernet.  
  * fd-net—Sets the VLAN media type as FDDI net.  
  * fddi—Sets the VLAN media type as FDDI. |
### Deleting a VLAN

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• tokenring</td>
<td>Sets the VLAN media type as Token Ring.</td>
</tr>
<tr>
<td>• trn-net</td>
<td>Sets the VLAN media type as Token Ring net.</td>
</tr>
</tbody>
</table>

**Step 5**

remote-span

Example:

Device(config-vlan)# remote-span

**Step 6**

end

Example:

Device(config)# end

**Step 7**

show vlan {name vlan-name | id vlan-id}

Example:

Device# show vlan name test20 id 20

### Deleting a VLAN (GUI)

**Procedure**

**Step 1**

Choose **Configuration** > **Layer2** > **VLAN**.

**Step 2**

Choose the **VLAN** tab.

**Step 3**

Check the check box adjacent to the VLAN you want to delete.

To delete multiple VLANs, select multiple VLANs check boxes.

**Step 4**

Click **Delete**.

**Step 5**

Click **Yes** on the confirmation window to delete the VLAN.

### Deleting a VLAN

When you delete a VLAN from a device that is in VTP server mode, the VLAN is removed from the VLAN database for all devices in the VTP domain. When you delete a VLAN from a device that is in VTP transparent mode, the VLAN is deleted only on that specific device.

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.
When you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `enable` | Enables privileged EXEC mode.  
**Example:**  
Device> `enable` |
| | **Example:**  
Device> `enable` |  
- Enter your password if prompted. |
| **Step 2** | `configure terminal` | Enters global configuration mode. |
| **Example:** | Device# `configure terminal` |
| **Step 3** | `no vlan vlan-id` | Removes the VLAN by entering the VLAN ID. |
| **Example:** | Device(config)# `no vlan 4` |
| **Step 4** | `end` | Returns to privileged EXEC mode. |
| **Example:** | Device(config)# `end` |
| **Step 5** | `show vlan brief` | Verifies the VLAN removal. |
| **Example:** | Device# `show vlan brief` |
| **Step 6** | `copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |
| **Example:** | Device# `copy running-config startup-config` |

### 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 the Cisco Catalyst 9500 Series Switches, if you are assigning a port on a cluster member device to a VLAN, first use the `rcommand` privileged EXEC command to log in to the cluster member switch.

If you assign an interface to a VLAN that does not exist, the new VLAN is created.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Enters the interface to be added to the VLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface gigabitethernet2/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> switchport mode access</td>
<td>Defines the VLAN membership mode for the port (Layer 2 access port).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> switchport access vlan vlan-id</td>
<td>Assigns the port to a VLAN. Valid VLAN IDs are 1 to 4094.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# switchport access vlan 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> show running-config interface interface-id</td>
<td>Verifies the VLAN membership mode of the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# show running-config interface</td>
<td></td>
</tr>
</tbody>
</table>
### 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 device 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.

You can change only the MTU size and the remote SPAN configuration state on extended-range VLANs; all other characteristics must remain at the default state.

### Creating an Extended-Range VLAN (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Layer2 &gt; VLAN.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the VLAN page, click <strong>ADD</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the extended range VLAN ID in the <strong>VLAN ID</strong> field. The extended range is between range is 1006 and 4094.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter a VLAN name in the <strong>Name</strong> field.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Save the configuration.</td>
</tr>
</tbody>
</table>

---

### Command or Action | Purpose
---|---
`gigabitethernet2/0/1` | 
**Step 8** | `show interfaces interface-id switchport` Verifies your entries in the **Administrative Mode** and the **Access Mode VLAN** fields of the display. 
**Example:**  
Device# `show interfaces gigabitethernet2/0/1 switchport`

**Step 9** | `copy running-config startup-config` (Optional) Saves your entries in the configuration file. 
**Example:**  
Device# `copy running-config startup-config`
## Creating an Extended-Range VLAN

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: enable (Device&gt; enable)</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: configure terminal (Device# configure terminal)</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>vlan vlan-id</td>
<td>Enters an extended-range VLAN ID and enters VLAN configuration mode. The range is 1006 to 4094.</td>
</tr>
<tr>
<td></td>
<td>Example: vlan 2000 (Device(config)# vlan 2000) (Device(config-vlan)#)</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>remote-span</td>
<td>(Optional) Configures the VLAN as the RSPAN VLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: remote-span (Device(config-vlan)# remote-span)</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>exit</td>
<td>Returns to configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: exit (Device(config-vlan)# exit (Device(config)#)</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: end (Device(config)# end)</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show vlan id vlan-id</td>
<td>Verifies that the VLAN has been created.</td>
</tr>
<tr>
<td></td>
<td>Example: show vlan id 2000 (Device# show vlan id 2000)</td>
<td></td>
</tr>
</tbody>
</table>
Purpose

Command or Action

(Optional) Saves your entries in the configuration file.

**Step 8**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

---

### Monitoring VLANs

#### Table 55: Privileged EXEC show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces [vlan vlan-id]</code></td>
<td>Displays characteristics for all interfaces or for the specified VLAN configured on the device.</td>
</tr>
</tbody>
</table>
| `show vlan [access-map name | brief | dot1q {tag native } | filter [access-map | vlan ] | group [group-name name ] | id vlan-id | ifindex | mtu | name name | remote-span | summary ]` | Displays parameters for all VLANs or the specified VLAN on the device. The following command options are available:  
  - **access-map**—Displays the VLAN access-maps.  
  - **brief**—Displays VTP VLAN status in brief.  
  - **dot1q**—Displays the dot1q parameters.  
  - **filter**—Displays VLAN filter information.  
  - **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.  
  - **remote-span**—Displays the remote SPAN VLANs.  
  - **summary**—Displays a summary of VLAN information. |
CHAPTER 118

VLAN Groups

- Information About VLAN Groups, on page 1075
- Prerequisites for VLAN Groups, on page 1075
- Restrictions for VLAN Groups, on page 1076
- Configuring VLAN Groups, on page 1076

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. This feature also extends the current AP group architecture and AAA override architecture, where the AP groups and AAA override can override a VLAN or a VLAN group to which the WLAN is mapped.

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.

Prerequisites for VLAN Groups

- A VLAN should be present in the device for it to be added to the VLAN group.

- For a VLAN group to function properly, in addition to enabling DHCP snooping globally, you must ensure that DHCP snooping is enabled in all the VLANs.
Restrictions for VLAN Groups

- The number of VLANs mapped to a VLAN group is not limited by Cisco IOS XE software release. However, if the number of VLANs in a VLAN group exceeds the recommended value of 32, the mobility functionality might not work as expected and in the VLAN group, L2 multicast breaks 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 device. The static IP client behavior is not supported.

- The VLAN Groups feature works only in local mode.

Configuring VLAN Groups

The following sections provide information about the various VLAN Group configuration tasks:

Creating a VLAN Group (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Configuration &gt; Layer2 &gt; VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>On the VLAN &gt; VLAN page, click Add.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the VLAN ID in the VLAN ID field.</td>
</tr>
<tr>
<td></td>
<td>The valid range is between 2 and 4094.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the VLAN name in the Name field.</td>
</tr>
<tr>
<td></td>
<td>Configure the other parameters if required.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Update &amp; Apply to Device.</td>
</tr>
</tbody>
</table>

Creating a VLAN Group (CLI)

Procedure

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

Example:

Device# configure terminal
### Creating a VLAN Group

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 recommended number of VLANs in a group is 64.</td>
<td>vlan group \textit{WORD} vlan-list \textit{vlan-ID}</td>
</tr>
</tbody>
</table>
| Exits the global configuration mode and returns to privileged EXEC mode. Alternatively, press 
\textit{CTRL-Z} to exit the global configuration mode. | end |

#### Removing a VLAN Group (GUI)

**Procedure**

1. Choose Configuration > Layer2 > VLAN
2. On the VLAN > VLAN Group page, check the checkbox adjacent to the VLAN Group you want to delete.
   
   To delete multiple VLAN Groups, select multiple VLAN Groups checkboxes.
3. Click Delete.
4. Click Yes on the confirmation window to delete the VLAN Group.

#### Removing a VLAN Group (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enters global configuration mode.</td>
<td>configure terminal</td>
</tr>
<tr>
<td>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 recommended number of VLANs in a group is 64.</td>
<td>vlan group \textit{WORD} vlan-list \textit{vlan-ID}</td>
</tr>
<tr>
<td>Removes the VLAN group with the given group name (vlangrp1).</td>
<td>no vlan group \textit{WORD} vlan-list \textit{vlan-ID}</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Exits global configuration mode and returns to privileged EXEC mode. Alternatively, press <code>CTRL-Z</code> to exit global configuration mode.</td>
</tr>
</tbody>
</table>

Adding a VLAN Group to a WLAN (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 Add to configure the following:
- General
- Access Policies
- QOS and AVC
- Mobility
- Advanced

Step 3 In the General tab, proceed as follows:
a) Enter a name and description for the policy profile.
b) To enable the policy profile, set Status as Enabled.
c) Use the slider to enable or disable Passive Client and Encrypted Traffic Analytics.
d) In the CTS Policy section, choose the appropriate status for the following:
   - Inline Tagging
   - SGACL Enforcement
e) Specify a default SGT. The valid range is from 2 to 65519.
f) In the WLAN Switching Policy section, choose the appropriate status for the following:
   - Central Switching
   - Central Authentication
   - Central DHCP
   - Central Association Enable
   - Flex NAT/PAT
Step 4
In the **Access Policies** tab, proceed as follows:

a) Choose the appropriate status for the following:
   - HTTP TLV Caching
   - RADIUS Profiling
   - DHCP TLV Caching

b) Choose a **Local Subscriber Policy Name**.
c) Choose the required **VLAN/VLAN Group**.
d) Specify the multicast VLAN.
e) Choose the required **IPv4 ACL** and **IPv6 ACL**.
f) Choose the required Pre Auth and Post Auth URL filters.
g) Click **Save & Apply to Device**.

Step 5
In the **QoS and AVC** tab, proceed as follows:

a) Choose the required **Auto QoS**.
b) Specify the **Egress** and **Ingress** details for the following:
   - **QoS SSID Policy**
   - **QoS Client Policy**
   - **Flow Monitor IPv4**
   - **Flow Monitor IPv6**

c) In the **SIP-CAC** section, choose the appropriate status for the following:
   - Call Snooping
   - Send Disassociate
   - Send 486 Busy

d) Click **Save & Apply to Device**.

Step 6
In the **Mobility** tab, proceed as follows:

a) Choose the **Export Anchor** check box to enable export anchor, if required.
b) Use the slider to enable or disable **Static IP Mobility**.
c) From the list of **Available** anchors, select the required anchors and move them to the list of **Selected** anchors.
d) Click **Save & Apply to Device**.

Step 7
In the **Advanced** tab, proceed as follows:

a) Specify the following **WLAN Timeout** details:
   - Session Timeout
   - Idle Timeout
   - Idle Threshold
   - Client Exclusion Timeout
b) In the **DHCP** section, choose **DHCP Enable** check box and enter the DHCP server IP address.

c) Choose the appropriate status for the following:

   - DHCP Option 82 Enable
   - DHCP Option 82 ASCII
   - DHCP Option 82 RID
   - DHCP Option 82 Format
   - DHCP AP MAC
   - DHCP SSID
   - DHCP AP ETH MAC
   - DHCP AP NAME
   - DHCP Policy Tag
   - DHCP AP Location
   - DHCP VLAN ID

d) In the **AAA Policy** section, choose the appropriate status for the following:

   - Allow AAA Override
   - NAC State

e) Choose the policy name and accounting list.

f) If required, enable **Fabric Profile** and choose from the list of profiles available.

g) From the **Umbrella Parameter Map**, choose an appropriate parameter map.

h) In the **WLAN Flex Policy** section, choose the appropriate status for the following:

   - VLAN Central Switching
   - Split MAC ACL

i) In the **Air Time Fairness Policies** section, choose the appropriate status for the following:

   - 2.4 GHz Policy
   - 5 GHz Policy

j) Click **Save & Apply to Device**.
Adding a VLAN Group to a WLAN (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wireless profile policy wlan-policy-profile-name</code></td>
<td>Configures the WLAN policy profile.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Device(config)# <code>wireless profile policy my-wlan-policy</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>vlan vlan-group1</code></td>
<td>Maps the VLAN group to the WLAN by entering the group name.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Device(config-wireless-policy)# <code>vlan myvlan-group</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
<td>Exits global configuration mode and returns to privileged EXEC mode. Alternatively, press <code>CTRL-Z</code> to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Device(config-wlan)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>

### Viewing the VLANs in a VLAN Group (CLI)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show vlan group</code></td>
<td>Displays the list of VLAN groups with name and the VLANs that are available.</td>
</tr>
<tr>
<td><code>show vlan group group-name group_name</code></td>
<td>Displays the specified VLAN group details.</td>
</tr>
<tr>
<td><code>show wireless client mac-address client-mac-addr detail</code></td>
<td>Displays the VLAN group assigned to the client.</td>
</tr>
<tr>
<td><code>show wireless vlan details</code></td>
<td>Displays VLAN details.</td>
</tr>
</tbody>
</table>
Viewing the VLANs in a VLAN Group (CLI)
PART XVI

WLAN

• WLANs, on page 1085
• Remote LANs, on page 1099
• Network Access Server Identifier, on page 1113
• DHCP for WLANs, on page 1117
• WLAN Security, on page 1133
• Workgroup Bridges, on page 1145
• Peer-to-Peer Client Support, on page 1149
• Wireless Guest Access, on page 1151
• Wired Guest Access, on page 1177
• 802.11r BSS Fast Transition, on page 1193
• Information about BSS Coloring and Spatial Reuse, on page 1203
• Assisted Roaming, on page 1209
• 802.11v, on page 1215
• 802.11w, on page 1219
• Management Frame Protection, on page 1227
• Deny Wireless Client Session Establishment Using Calendar Profiles, on page 1231
• Ethernet over GRE, on page 1241
• Link Aggregation Control Protocol and Port Aggregation Protocol, on page 1259
• Hotspot 2.0, on page 1267
• Express Wi-Fi by Facebook, on page 1281
Information About WLANs

This feature enables you to control up to 4096 WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All devices publish up to 16 WLANs to each connected access point. However, you can create till the maximum number of supported WLANs and then selectively publish these WLANs (using profiles and tags) to different access points for managing your wireless network in a better way.

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

Band Selection

Band selection enables client radios that are capable of dual-band (2.4 and 5-GHz) operations to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of 3 nonoverlapping channels. To prevent these sources of interference and improve overall network performance, configure band selection on the 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 milliseconds. Therefore, when RRM is about to perform an off-channel scan, a data frame marked with UP 4, 5, or 6 is received within the last 100 milliseconds, RRM defers going off-channel. The AP radio does not go off-channel when a voice call sending and receiving audio samples are marked as UP class 6 for every active 20 milliseconds.

Off-channel scanning deferral does come with a tradeoff. Off-channel scanning can impact throughput by 2 percent or more, depending on the configuration, traffic patterns, and so on. Throughput can be slightly improved if you enable off-channel scanning deferral for all traffic classes and increase the time threshold. However, by not going off-channel, RRM can fail to identify AP neighbors and rogues, resulting in negative impact to security, DCA, TPC, and 802.11k messages.

We recommend that you do not change the default off-channel scanning deferral settings.

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

---

**Note**

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

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

---

**Session Timeouts**

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

This section contains the following subsections:

---

**Cisco Client Extensions**

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

- The software supports CCX versions 1 through 5, which enables 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.

This section contains the following subsections:
**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**

- 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.
- The WLAN name and SSID can have up to 32 characters.
- Special characters are not supported for the WLAN name.
- WLAN name cannot be a keyword; for example, if you try to create a WLAN with the name as 's' by entering the `wlan s` command, it results in shutting down all WLANs because 's' is used as a keyword for shutdown.
- You cannot map a WLAN to VLAN 0. Similarly, you cannot map a WLAN to VLANs 1002 to 1006.
- Dual stack clients with a static-IPv4 address is not supported.
- When creating a WLAN with the same SSID, you must create a unique profile name for each WLAN.
- 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 interface per wlan feature is not supported.
- Downloadable ACL (DACL) is not supported in the flexconnect mode or the local mode.

**Caution**

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

### 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.

**Step 3**

Click **Save & Apply to Device**.

#### Creating WLANs (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**

  - `configure terminal`
  
  **Example:**
  
  `Device# configure terminal`

  Enters global configuration mode.

  | **Step 2**

  - `wlan profile-name wlan-id [ssid]`
  
  **Example:**
  
  `Device(config)# wlan mywlan 34 mywlan-ssid`

  Specifies the WLAN name and ID:

  - For the **profile-name**, enter the profile name. The range is from 1 to 32 alphanumeric characters.
  
  - For the **wlan-id**, enter the WLAN ID. The range is from 1 to 512.
  
  - For the **ssid**, enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not
Purpose
Command or Action | Purpose
---|---
| specified, the WLAN profile name is set as the SSID.
| By default, the WLAN is disabled.

Note
Step 3 | 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

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

Example:
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.
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

<table>
<thead>
<tr>
<th>WLAN Profile Name</th>
<th>SSID</th>
<th>VLAN Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 test1</td>
<td>test1-ssid</td>
<td>137 UP</td>
</tr>
<tr>
<td>3 test2</td>
<td>test2-ssid</td>
<td>136 UP</td>
</tr>
<tr>
<td>2 test3</td>
<td>test3-ssid</td>
<td>1 UP</td>
</tr>
<tr>
<td>45 test4</td>
<td>test4-ssid</td>
<td>1 DOWN</td>
</tr>
</tbody>
</table>
```

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

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

**Step 3**

**Example:**

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

**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**

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

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

| **Step 2** wlan profile-name | Enters WLAN configuration submode. The profile-name is the profile name of the configured WLAN. |
| Example: Device# wlan test4 |                                      |

| **Step 3** shutdown | Disables the WLAN. |
| Example: Device(config-wlan)# shutdown |                                      |
### Step 4

**Command or Action**: end

**Example**:  
Device(config)# end

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

### Step 5

**Command or Action**: show wlan summary

**Example**:  
Device# show wlan summary

**Purpose**: 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
- Call Snooping
- Radio
- Interface
- Status

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | configure terminal  
Example: Device# configure terminal |
| **Step 2** | wlan profile-name  
Example: Device# wlan test4 |
| **Step 3** | shutdown  
Example: Device# shutdown |
| **Step 4** | broadcast-ssid  
Example: Device(config-wlan)# broadcast-ssid |
| **Step 5** | radio {all | dot11a | dot11ag | dot11bg | dot11g}  
Example: |

**Procedure**

- Enters global configuration mode.
- Enters WLAN configuration submode. The profile-name is the profile name of the configured WLAN.
- Disables the WLAN before configuring the parameters.
- Broadcasts the SSID for this WLAN.
- Enables radios on the WLAN. The keywords are as follows:
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# radio all</td>
<td>• all—Configures the WLAN on all radio bands.</td>
</tr>
<tr>
<td></td>
<td>• dot1a—Configures the WLAN on only 802.11a radio bands.</td>
</tr>
<tr>
<td></td>
<td>• dot11g—Configures the WLAN on 802.11ag radio bands.</td>
</tr>
<tr>
<td></td>
<td>• dot11bg—Configures the WLAN on only 802.11b/g radio bands (only 802.11b if 802.11g is disabled).</td>
</tr>
<tr>
<td></td>
<td>• dot11ag—Configures the wireless LAN on 802.11g radio bands only.</td>
</tr>
</tbody>
</table>

### Step 6

**client vlan vlan-identifier**  
Example:  
Device# client vlan test-vlan

Enables an interface group on the WLAN.  
*vlan-identifier*—Specifies the VLAN identifier.  
This can be the VLAN name, VLAN ID, or VLAN group name.

### Step 7

**ip multicast vlan vlan-name**  
Example:  
Device(config-wlan)# ip multicast vlan test

Enables IP multicast on a WLAN. The keywords are as follows:  
• vlan—Specifies the VLAN ID.  
• vlan-name—Specifies the VLAN name.

### Step 8

**media-stream multicast-direct**  
Example:  
Device(config-wlan)# media-stream multicast-direct

Enables multicast VLANs on this WLAN.

### Step 9

**call-snoop**  
Example:  
Device(config-wlan)# call-snoop

Enables call-snooping support.

### Step 10

**no shutdown**  
Example:  
Device(config-wlan)# no shutdown

Enables the WLAN.

### Step 11

**end**  
Example:  
Device(config)# end

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

## Configuring Advanced WLAN Properties (CLI)

You can configure the following advanced properties:
• AAA Override
• Coverage Hole Detection
• Session Timeout
• Cisco Client Extensions
• Diagnostic Channels
• Interface Override ACLs
• P2P Blocking
• Client Exclusion
• Maximum Clients Per WLAN
• Off Channel Scan Defer

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wlan profile-name</code></td>
<td>Enters WLAN configuration submode. The profile-name is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>wlan test4</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# wlan test4</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>aaa-override</code></td>
<td>Enables AAA override.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>aaa-override</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-wlan)# aaa-override</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>chd</code></td>
<td>Enables coverage hole detection for this WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>chd</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-wlan)# chd</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>session-timeout time-in-seconds</code></td>
<td>Sets the session timeout in seconds. The range and default values vary according to the security configuration.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>session-timeout 450</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-wlan)# session-timeout 450</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>ccx aironet-iesupport</code></td>
<td>Enables support for Aironet IEs for this WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>ccx aironet-iesupport</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-wlan)# ccx aironet-iesupport</code></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>7</td>
<td>diag-channel</td>
<td>Enables diagnostic channel support to troubleshoot client communication issues on a WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# diag-channel</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>ip access-group web acl-name</td>
<td>Configures the IPv4 WLAN web ACL. The variable acl-name specifies the user-defined IPv4 ACL name.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip access-group acl-name</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>peer-blocking [allow-private-group</td>
<td>Configures peer to peer blocking parameters. The keywords are as follows:</td>
</tr>
<tr>
<td></td>
<td>drop</td>
<td>forward-upstream]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# peer-blocking drop</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>exclusionlist time-in-seconds</td>
<td>Specifies the clients added or deleted from the exclusion list. The valid time-in-seconds ranges from 0 to 2147483647. Enter 0 for no timeout. A zero (0) timeout indicates that the client is permanently added to the exclusion list.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# exclusionlist 10</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>client association limit max-number-of-clients</td>
<td>Sets the maximum number of clients that can be configured on a WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# client association limit 200</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>channel-scan defer-priority defer-priority defer-time</td>
<td>Sets the channel scan defer priority and defer time. The arguments are as follows:</td>
</tr>
<tr>
<td></td>
<td>0-7</td>
<td>0 - 6000]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# channel-scan defer-priority 6</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Configuration &gt; Tags &amp; Profiles &gt; WLANs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Add.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Under the Advanced tab, check the Coverage Hole Detection check box.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Check the Aironet IE check box to enable Aironet IE on the WLAN.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Check the Diagnostic Channel check box to enable diagnostic channel on the WLAN.</td>
</tr>
<tr>
<td>Step 6</td>
<td>From the P2P Blocking Action drop-down list, choose the required value.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Set the Multicast Buffer toggle button as enabled or disabled.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Check the Media Stream Multicast-Direct check box to enable the feature.</td>
</tr>
<tr>
<td>Step 9</td>
<td>In the Max Client Connections section, specify the maximum number of client connections for the following:</td>
</tr>
<tr>
<td></td>
<td>• In the Per WLAN field, enter a value. The valid range is between 0 and 10000.</td>
</tr>
<tr>
<td></td>
<td>• In the Per AP Per WLAN field, enter a value. The valid range is between 0 and 400.</td>
</tr>
<tr>
<td></td>
<td>• In the Per AP Radio Per WLAN field, enter a value. The valid range is between 0 and 200.</td>
</tr>
<tr>
<td>Step 10</td>
<td>In the 11v BSS Transition Support section, perform the following configuration tasks:</td>
</tr>
<tr>
<td></td>
<td>a) Check the BSS Transition check box to enable 802.11v BSS Transition support.</td>
</tr>
<tr>
<td></td>
<td>b) In the Disassociation Imminent field, enter a value. The valid range is between 0 and 3000.</td>
</tr>
<tr>
<td></td>
<td>c) In the Optimized Roaming Disassociation Timer field, enter a value. The valid range is between 0 and 40.</td>
</tr>
<tr>
<td></td>
<td>d) Select the check box to enable the following:</td>
</tr>
<tr>
<td></td>
<td>• BSS Max Idle Service</td>
</tr>
<tr>
<td></td>
<td>• BSS Max Idle Protected</td>
</tr>
<tr>
<td></td>
<td>• Disassociation Imminent Service</td>
</tr>
<tr>
<td></td>
<td>• Directed Multicast Service</td>
</tr>
<tr>
<td></td>
<td>• Universal Admin</td>
</tr>
<tr>
<td></td>
<td>• Load Balance</td>
</tr>
<tr>
<td></td>
<td>• Band Select</td>
</tr>
<tr>
<td></td>
<td>• IP Source Guard</td>
</tr>
<tr>
<td>Step 11</td>
<td>From the WMM Policy drop-down list, choose the policy as Allowed, Disabled, or Required. By default, the WMM policy is Allowed.</td>
</tr>
</tbody>
</table>
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 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 120

Remote LANs

- Information About Remote LANs, on page 1099
- Configuring Remote LANs (RLANs), on page 1100

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.

Note

RLAN is supported in APs that have more than one Ethernet port.

The supported AP models are:
- Cisco Aironet OEAP 1810 and 1815T series
- Cisco Aironet 1810w and 1815w series

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

**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.

**Configuring Remote LANs (RLANs)**

### Enabling or Disabling all RLANs

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>[no] ap remote-lan shutdown</td>
<td>Enables or disables all RLANs.</td>
</tr>
<tr>
<td></td>
<td>Example: [no] ap remote-lan shutdown</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# [no] ap remote-lan shutdown</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: end</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Creating RLAN Profile

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ap remote-lan profile-name remote-lan-profile-name rlan-id</td>
<td>Configures remote LAN profile.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ap remote-lan profile-name rlan_profile_name 3</td>
<td></td>
</tr>
</tbody>
</table>

- **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 > Wireless > 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.

b) Set the number of client connections per RLAN in the **Client Association Limit** field.

   The range is between 0 and 10000. 0 refers to unlimited client connections.

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

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>client association limit client-connections</td>
<td>Configures client connections per RLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-remote-lan)# client association limit 1</td>
<td>client-connections—Is the maximum client connections per RLAN. Range is from 0 to 10000. 0 refers to unlimited.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip access-group web IPv4-acl-name</td>
<td>Configures RLAN IP configuration commands.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-remote-lan)# ip access-group web acl_name</td>
<td>IPv4-acl-name—Refers to the IPv4 ACL name or ID.</td>
</tr>
<tr>
<td>Step 3</td>
<td>local-auth profile name</td>
<td>Sets EAP Profile on an RLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-remote-lan)# local-auth profile_name</td>
<td>profile-name—Is the EAP profile on an RLAN.</td>
</tr>
<tr>
<td>Step 4</td>
<td>mac-filtering mac-filter-name</td>
<td>Sets MAC filtering support on an RLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-remote-lan)# mac-filtering mac_filter</td>
<td>mac-filter-name—Is the authorization list name.</td>
</tr>
<tr>
<td>Step 5</td>
<td>security dot1x authentication-list list-name</td>
<td>Configures 802.1X for an RLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-remote-lan)# security dot1x authentication-list dot1_auth_list</td>
<td>list-name—Is the authentication list name.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 6** security web-auth authentication-list list-name | Configures web authentication for an RLAN. 
*list-name*—Is the authentication list name. 

**Example:**

```plaintext
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.

<table>
<thead>
<tr>
<th><strong>Step 7</strong> [no] shutdown</th>
<th>Enables or disables RLAN profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-remote-lan)# shutdown</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 8</strong> end</th>
<th>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-remote-lan)# end</code></td>
</tr>
</tbody>
</table>

**Note** 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.

### Creating RLAN Policy Profile

**Procedure**

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

<table>
<thead>
<tr>
<th><strong>Step 2</strong> ap remote-lan-policy policy-name profile name</th>
<th>Configures RLAN policy profile and enters wireless policy configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# ap remote-lan-policy policy-name rlan_policy_prof_name</code></td>
</tr>
</tbody>
</table>

### Configuring RLAN Policy Profile Parameters (GUI)

**Procedure**

1. **Step 1** Choose Configuration > Wireless > Remote LAN.
2. **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.

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.

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.
## Configuring RLAN Policy Profile Parameters

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>central switching</code></td>
<td>Configures central switching.</td>
</tr>
</tbody>
</table>
|      | **Example:**  
|      | `Device(config-remote-lan-policy)# central switching` | |
| 2    | `central dhcp` | Configures central DHCP. |
|      | **Example:**  
|      | `Device(config-remote-lan-policy)# central dhcp` | |
| 3    | `exclusionlist timeout timeout` | Sets exclusion-listing on RLAN.  
|      | **Example:**  
|      | `Device(config-remote-lan-policy)# exclusionlist timeout 200` | *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. |
| 4    | `vlan vlan` | Configures VLAN name or ID.  
|      | **Example:**  
|      | `Device(config-remote-lan-policy)# vlan vlan1` | *
|      | `- vlan`—Is the vlan name. | |
| 5    | `Example:`  
|      | `Device(config-remote-lan-policy)# ipv6 acl ipv6_acl` | |
| 6    | `aaa-override` | Configures AAA policy override. |
|      | **Example:**  
|      | `Device(config-remote-lan-policy)# aaa-override` | |
| 7    | `session-timeout timeout in seconds` | Configures client session timeout.  
|      | **Example:**  
|      | `Device(config-remote-lan-policy)# session-timeout 21` | *timeout in seconds*—Defines the duration of a session. Range is from 20 to 86400 seconds. |
| 8    | `host-mode {multidomain voice domain | multihost | singlehost}` | Configures host mode for remote-LAN 802.1x.  
|      | **Example:**  
|      | `Device(config-remote-lan-policy)# host-mode multidomain` | *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: | |
### Configuring RLAN Policy Profile Parameters

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 9**

`violation-mode {protect | replace | shutdown}
Example:
Device(config-remote-lan-policy)# violation-mode protect

Confirms 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 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.
### Configuring Policy Tag and Mapping an RLAN Policy Profile to an RLAN Profile

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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.  
• *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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | ap name *ap name* lan port-id *lan port id* {disable | enable}  
*Example:*  
Device(config)# ap name lan port-id disable |
| | 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>ap ap-ethernet-mac</td>
<td>Configures MAP address for an AP and enters AP configuration mode.</td>
</tr>
<tr>
<td>policy-tag policy-tag-name</td>
<td>Attaches policy tag to the access point.</td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Verifying RLAN Configuration

To view the summary of all RLANs, use the following command:

```
Device# show remote-lan summary
```

Number of RLANs: 1
<table>
<thead>
<tr>
<th>RLAN Profile Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>rlan_test_1</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

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
Verifying RLAN Configuration

Device# show remote-lan policy summary
Number of Policy Profiles: 1

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>rlan_named_pp1</td>
<td>Testing RLAN policy profile</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

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  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

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>AP Name</th>
<th>WLAN</th>
<th>State</th>
<th>Protocol</th>
<th>Method</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>d8eb.97b6.fcc6</td>
<td>L2_1815w_1</td>
<td>1</td>
<td>Run</td>
<td>Ethernet</td>
<td>None</td>
<td>Local</td>
</tr>
</tbody>
</table>

To view the client details with the specified username, use the following command:

Device# show wireless client username cisco

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>AP Name</th>
<th>Status</th>
<th>WLAN</th>
<th>Auth Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>0014.d1da.a977</td>
<td>L2_1815w_1</td>
<td>Run 1</td>
<td>Yes</td>
<td>Ethernet</td>
</tr>
<tr>
<td>d8eb.97b6.fcc6</td>
<td>L2_1815w_1</td>
<td>Run 1</td>
<td>Yes</td>
<td>Ethernet</td>
</tr>
</tbody>
</table>

To view the detailed information for a client by MAC address, use the following command:

Device# show wireless client mac-address <mac_address> detail
Client MAC Address: d8eb.97b6.fcc6
Client IPv4 Address: 9.2.20.78
Client IPv6 Addresses: fe80::1863:1292: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
Verifying RLAN Configuration

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

<table>
<thead>
<tr>
<th>AP Name</th>
<th>AP Mac</th>
<th>Site Tag Name</th>
<th>Policy Tag Name</th>
<th>RF</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2_1810d_1</td>
<td>0008.3296.24c0</td>
<td>default-site-tag</td>
<td>default-policy-tag</td>
<td></td>
</tr>
<tr>
<td></td>
<td>default-rf-tag</td>
<td>No</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>L2_1810w_2</td>
<td>00b0.e18c.5880</td>
<td>rlan-site-tag</td>
<td>rlan_pt_1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>default-rf-tag</td>
<td>No</td>
<td>Static</td>
<td></td>
</tr>
</tbody>
</table>

To view the summary of all policy tags, use the following command:

Device# show wireless tag policy summary
Number of Policy Tags: 2

<table>
<thead>
<tr>
<th>Policy Tag Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rlan_pt_1</td>
<td>default policy-tag</td>
</tr>
<tr>
<td>default-policy-tag</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>REMOTE-LAN Profile Name</th>
<th>Policy Name</th>
<th>Port Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>rlan_test_1</td>
<td>rlan_named_pp1</td>
<td>1</td>
</tr>
<tr>
<td>rlan_test_1</td>
<td>rlan_named_pp1</td>
<td>2</td>
</tr>
</tbody>
</table>
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 a NAS-ID 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.

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)
Creating a NAS ID Policy

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, wireless 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 wireless aaa policy policy-name</td>
<td>Configures a new AAA policy.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Purpose

Command or Action

Device(config)# wireless aaa policy test

<table>
<thead>
<tr>
<th>Step 3</th>
<th>nas-id option1 sys-name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-aaa-policy)# nas-id option1 sys-name</td>
<td></td>
</tr>
</tbody>
</table>

Configures NAS ID for option1.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>nas-id option2 sys-ip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-aaa-policy)# nas-id option2 sys-ip</td>
<td></td>
</tr>
</tbody>
</table>

Configures NAS ID for option2.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>nas-id option3 sys-mac</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-aaa-policy)# nas-id option3 sys-mac</td>
<td></td>
</tr>
</tbody>
</table>

Configures NAS ID for option3.

---

**Attaching a Policy to a Tag (GUI)**

**Procedure**

1. Choose Configuration > Tags & Profiles > Tags page, click Policy tab.
2. Click Add to view the Add Policy Tag window.
3. Enter a name and description for the policy tag.
4. Click Add to map WLAN profile and Policy profile.
5. Choose the WLAN Profile to map with the appropriate Policy Profile, and click the tick icon.
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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

Enters global configuration mode.
### Purpose

**Command or Action**

- `wireless profile policy policy-name`
- `aaa-policy aaa-policy-name`
- `exit`
- `wireless tag policy policy-tag`
- `wlan wlan1 policy policy-name`

**Purpose**

- Configures a WLAN policy profile.
- Configures a AAA policy profile.
- Returns to global configuration mode.
- Configures a wireless policy tag.
- Maps a WLAN profile to a policy profile.

### Example

**Step 2**

```
Device(config)# wireless profile policy test1
```

**Step 3**

```
Device(config-wireless-policy)# aaa-policy policy-aaa
```

**Step 4**

```
Device(config-wireless-policy)# exit
```

**Step 5**

```
Device(config)# wireless tag policy policy-tag1
```

**Step 6**

```
Device(config)# wlan wlan1 policy test1
```

**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
```

<table>
<thead>
<tr>
<th>Policy Profile Name</th>
<th>Description</th>
<th>Status</th>
<th>VLAN</th>
<th>Client count</th>
</tr>
</thead>
<tbody>
<tr>
<td>:</td>
<td>:</td>
<td>ENABLED</td>
<td>:</td>
<td>:</td>
</tr>
</tbody>
</table>

AAA Policy Params

- AAA Override : DISABLED
- NAC : DISABLED
- AAA Policy name : test

---

**Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x**
DHCP for WLANs

- Information about Dynamic Host Configuration Protocol, on page 1117
- Restrictions for Configuring DHCP for WLANs, on page 1120
- How to Configure DHCP for WLANs, on page 1120
- Configuring Internal DHCP Server, on page 1122

Information about Dynamic Host Configuration Protocol

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

This section contains the following subsections:

Internal DHCP Servers

The devices contain an internal DHCP server. This server is typically used in branch offices that do not already have a DHCP server.

The internal server provides DHCP addresses to wireless clients, direct-connect APs, and DHCP requests that are relayed from APs. Only lightweight access points are supported. When you want to use the internal DHCP server, ensure that you configure SVI for client VLAN and set the IP address as DHCP server IP address.

DHCP option 43 is not supported on the internal server. Therefore, the access point must use an alternative method to locate the management interface IP address of the 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 device appears as a DHCP Relay agent to the DHCP server and as a DHCP server at the virtual IP address to wireless clients. Because the device captures the client IP address that is obtained from a DHCP server, it maintains the same IP address for that client during intra-device, inter-device, and inter-subnet client roaming.

---

**Note**

External DHCP servers can support DHCPv6.

**DHCP Assignments**

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

You can assign DHCP servers for individual interfaces. You can configure the management interface, AP-manager interface, and dynamic interface for a primary and secondary DHCP server, and you can configure the service-port interface to enable or disable DHCP servers. You can also define a DHCP server on a WLAN. In this case, the server overrides the DHCP server address on the interface assigned to the WLAN.

**Security Considerations**

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

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

### DHCP Option 82

DHCP option 82 provides additional security when DHCP is used to allocate network addresses. It enables the device to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. You can configure the device to add option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server.

*Figure 30: DHCP Option 82*

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

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

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

This section contains the following subsections:
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 device.

You can configure DHCP service in either of the following ways:

- Configuring the DHCP pool on the device.

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

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 as either IPv4 or IPv6.
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 on the Interfaces page.
Step 6  In the Subnet Mask field, enter the subnet mask assigned to all 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  Choose the Reserved Only as enabled or disabled.
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 the DHCP Scope, click Advanced and perform the following tasks.
Step 12  Check the Enable DNS Proxy check box to enable DNS proxy.
Step 13  In the Default Router(s) fields, enter the IP address of the optional router or router(s) that connect to the device and click the + icon to add 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(s) and click the + icon to add to the list. Each DNS server must be able to update a client’s DNS entry to match the IP address assigned by this DHCP scope.
Step 15  In the NetBios Name Server(s) field, enter the IP address of the optional Microsoft NetBIOS name servers, such as a Microsoft Windows Internet Naming Service (WINS) server and click the + icon to add to the list.
Step 16 In the **Domain** field, enter the optional domain name of this 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 as DHCP options, to 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 you want to add.

Step 19 Click **Save & Apply to Device**.

### Configuring DHCP Scopes (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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(config)# end
  | Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. |
Configuring Internal DHCP Server

Configuring Internal DHCP Server Under Client VLAN SVI

Before you begin

- To use the internal DHCP server for both wireless and wired client VLAN, an IP address must be configured under the client VLAN switched virtual interfaces (SVI) interface.

- For wireless clients, the IP address of the internal DHCP server must be different from the address of the wireless client VLAN SVI interface (in DHCP helper address configuration).

- For wireless clients, the internal DHCP server can be configured under the client VLAN SVI interface or under the wireless policy profile.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface loopback interface-number</td>
<td>Creates a loopback interface and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# interface Loopback0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip address ip-address</td>
<td>Configures the IP address for the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# ip address 10.10.10.1 255.255.255.255</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> interface vlan vlan-id</td>
<td>Configures the VLAN ID.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# interface vlan 32</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ip address ip-address</td>
<td>Configures the IP address for the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# ip address 192.168.32.100 255.255.255.0</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Internal DHCP Server Under Client VLAN SVI

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td><code>ip helper-address ip-address</code></td>
<td>Configures the destination address for UDP broadcasts. <strong>Note</strong>: If the IP address used in the <code>ip helper-address</code> command is an internal address of the controller, an internal DHCP server is used. Otherwise, the external DHCP server is used.</td>
</tr>
<tr>
<td>8</td>
<td><code>no mop enabled</code></td>
<td>Disables the Maintenance Operation Protocol (MOP) for an interface.</td>
</tr>
<tr>
<td>9</td>
<td><code>no mop sysid</code></td>
<td>Disables the task of sending MOP periodic system ID messages.</td>
</tr>
<tr>
<td>10</td>
<td><code>exit</code></td>
<td>Exits the interface configuration mode.</td>
</tr>
<tr>
<td>11</td>
<td><code>ip dhcp excluded-address ip-address</code></td>
<td>Specifies the IP address that the DHCP server should not assign to DHCP clients.</td>
</tr>
<tr>
<td>12</td>
<td><code>ip dhcp excluded-address ip-address</code></td>
<td>Specifies the IP addresses that the DHCP server should not assign to DHCP clients.</td>
</tr>
<tr>
<td>13</td>
<td><code>ip dhcp pool pool-name</code></td>
<td>Configures the DHCP pool address.</td>
</tr>
<tr>
<td>14</td>
<td><code>network network-name mask-address</code></td>
<td>Specifies the network number in dotted-decimal notation, along with the mask address.</td>
</tr>
<tr>
<td>15</td>
<td><code>default-router ip-address</code></td>
<td>Specifies the IP address of the default router for a DHCP client.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>16</td>
<td>exit</td>
<td>Exits DHCP configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(dhcp-config)# exit</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>wireless profile policy profile-policy</td>
<td>Configures the WLAN policy profile and enters the wireless policy configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless profile policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>default-policy-profile</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>central association</td>
<td>Configures central association for locally switched clients.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# central association</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>central dhcp</td>
<td>Configures the central DHCP for locally switched clients.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# central dhcp</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>central switching</td>
<td>Configures WLAN for central switching.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# central switching</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>description policy-profile-name</td>
<td>Adds a description for the policy profile</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# description</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;default policy profile&quot;</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>vlan vlan-name</td>
<td>Assigns the profile policy to the VLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# vlan 32</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>no shutdown</td>
<td>Enables the profile policy.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>
# Configuring the Internal DHCP Server Under a Wireless Policy Profile

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface loopback interface-number</td>
<td>Creates a loopback interface and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# interface Loopback0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip address ip-address</td>
<td>Configures the IP address for the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-if)# ip address 10.10.10.1 255.255.255.255</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>interface vlan vlan-id</td>
<td>Configures the VLAN ID.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# interface vlan 32</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>ip address ip-address</td>
<td>Configures the IP address for the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-if)# ip address 192.168.32.100 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>no mop enabled</td>
<td>Disables the Maintenance Operation Protocol (MOP) for an interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-if)# no mop enabled</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>no mop sysid</td>
<td>Disables the task of sending MOP periodic system ID messages.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-if)# no mop sysid</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>exit</td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>ip dhcp excluded-address ip-address</td>
<td>Specifies the IP addresses that the DHCP server should not assign to DHCP clients.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 11**  
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**  
Device(config)# ip dhcp pool pool-vlan32 | Configures the DHCP pool address. |
| **Step 13**  
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**  
Device(dhcp-config)# default-router 192.168.32.1 | Specifies the IP address of the default router for a DHCP client. |
| **Step 15**  
Device(dhcp-config)# exit | Exits DHCP configuration mode. |
| **Step 16**  
Device(config)# wireless profile policy default-policy-profile | Configures a WLAN policy profile and enters wireless policy configuration mode. |
| **Step 17**  
Device(config-wireless-policy)# central association | Configures central association for locally switched clients. |
| **Step 18**  
Device(config-wireless-policy)# central switching | Configures local switching. |
| **Step 19**  
Device(config-wireless-policy)# description "default policy profile" | Adds a description for the policy profile. |
### Configuring the Internal DHCP Server Globally

#### Procedure

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

<table>
<thead>
<tr>
<th>Step 20</th>
<th><code>ipv4 dhcp opt82</code></th>
<th>Enables DHCP Option 82 for the wireless clients.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Device(config-wireless-policy)# ipv4 dhcp opt82</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 21</th>
<th><code>ipv4 dhcp opt82 ascii</code></th>
<th>Enables ASCII on DHCP Option 82.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Device(config-wireless-policy)# ipv4 dhcp opt82 ascii</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 22</th>
<th><code>ipv4 dhcp opt82 format vlan_id</code></th>
<th>Enables VLAN ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Device(config-wireless-policy)# ipv4 dhcp opt82 format vlan32</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 23</th>
<th><code>ipv4 dhcp opt82 rid vlan_id</code></th>
<th>Supports the addition of Cisco 2-byte Remote ID (RID) for DHCP Option 82.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Device(config-wireless-policy)# ipv4 dhcp opt82 rid</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 24</th>
<th><code>ipv4 dhcp server ip-address</code></th>
<th>Configures the WLAN's IPv4 DHCP server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Device(config-wireless-policy)# ipv4 dhcp server 10.10.10.1</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 25</th>
<th><code>vlan vlan-name</code></th>
<th>Assigns the profile policy to the VLAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Device(config-wireless-policy)# vlan 32</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 26</th>
<th><code>no shutdown</code></th>
<th>Enables the profile policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Device(config-wireless-policy)# no shutdown</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Step 2 interface loopback interface-num</td>
<td>Creates a loopback interface and enters interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# interface Loopback0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3 ip address ip-address</td>
<td>Configures the IP address for the interface.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-if)# ip address 10.10.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>255.255.255.255</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4 exit</td>
<td>Exits interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-if)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5 interface vlanvlan-id</td>
<td>Configures the VLAN ID.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# interface vlan 32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 6 ip address ip-address</td>
<td>Configures the IP address for the interface.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-if)# ip address 192.168.32.100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 7 no mop enabled</td>
<td>Disables the Maintenance Operation Protocol (MOP) for an interface.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-if)# no mop enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 8 no mop sysid</td>
<td>Disables the task of sending MOP periodic system ID messages.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-if)# no mop sysid</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 9 exit</td>
<td>Exits the interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-if)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 10 ip dhcp-server ip-address</td>
<td>Specifies the target DHCP server parameters.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# ip dhcp-server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.10.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 11 ip dhcp excluded-address ip-address</td>
<td>Specifies the IP address that the DHCP server should not assign to DHCP clients.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# ip dhcp excluded-address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.32.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>12</td>
<td>ip dhcp excluded-address ip-address</td>
<td>Specifies the IP address that the DHCP server should not assign to DHCP clients.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# ip dhcp excluded-address 192.168.32.100</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>ip dhcp pool pool-name</td>
<td>Configures the DHCP pool address.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# ip dhcp pool pool-vlan32</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>network network-name mask-address</td>
<td>Specifies the network number in dotted-decimal notation along with the mask address.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(dhcp-config)# network 192.168.32.0 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>default-router ip-address</td>
<td>Specifies the IP address of the default router for a DHCP client.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(dhcp-config)# default-router 192.168.32.1</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>exit</td>
<td>Exits DHCP configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(dhcp-config)# exit</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>wireless profile policy profile-policy</td>
<td>Configures a WLAN policy profile and enters wireless policy configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# wireless profile policy default-policy-profile</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>central association</td>
<td>Configures central association for locally switched clients.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)# central association</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>central dhcp</td>
<td>Configures central DHCP for locally switched clients.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)# central dhcp</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>central switching</td>
<td>Configures local switching.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)# central switching</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>description policy-profile-name</td>
<td>Adds a description for the policy profile.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)# description &quot;default policy profile&quot;</td>
<td></td>
</tr>
</tbody>
</table>
### Verifying Internal DHCP Configuration

To verify the client binding, use the following command:

```
Device# show ip dhcp binding
```

```plaintext
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 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
DHCPPACK : 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 wireless dhcp statistic
```

```
DHCP Statistic
--------------
DHCPDISCOVER : 1
BOOTP FORWARD : 137
BOOTP REPLY : 0
DHCPOFFER : 0
DHCPREQUEST : 54
DHCPPACK : 0
DHCPNAK : 0
DHCPDECLINE : 0
DHCPRELEASE : 0
DHCPINFORM : 82

Tx/Rx Time :
-------------
LastTxTime : 18:42:18
LastRxTime : 00:00:00

Drop Counter :
-------------
TxDropCount : 0
```
Device# `show platform hardware chassis active qfp feature wireless punt statistics`

CPP Wireless Punt stats:

<table>
<thead>
<tr>
<th>App Tag</th>
<th>Packet Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPWAP_PKT_TYPE_DOT11_PROBE_REQ</td>
<td>14442</td>
</tr>
<tr>
<td>CAPWAP_PKT_TYPE_DOT11_MGMT</td>
<td>50</td>
</tr>
<tr>
<td>CAPWAP_PKT_TYPE_DOT11_IAPP</td>
<td>9447</td>
</tr>
<tr>
<td>CAPWAP_PKT_TYPE_DOT11_RFID</td>
<td>0</td>
</tr>
<tr>
<td>CAPWAP_PKT_TYPE_DOT11_RRM</td>
<td>0</td>
</tr>
<tr>
<td>CAPWAP_PKT_TYPE_DOT11_DOT1X</td>
<td>0</td>
</tr>
<tr>
<td>CAPWAP_PKT_TYPE_CAPWAP_KEEPALIVE</td>
<td>2191</td>
</tr>
<tr>
<td>CAPWAP_PKT_TYPE_MOBILITY_KEEPALIVE</td>
<td>0</td>
</tr>
<tr>
<td>CAPWAP_PKT_TYPE_CAPWAP_CNTRL</td>
<td>7034</td>
</tr>
<tr>
<td>CAPWAP_PKT_TYPE_CAPWAP_DATA</td>
<td>0</td>
</tr>
<tr>
<td>CAPWAP_PKT_TYPE_MOBILITY_CNTRL</td>
<td>0</td>
</tr>
<tr>
<td>WLS_SMD_WEBAUTH</td>
<td>0</td>
</tr>
<tr>
<td>SISF_PKT_TYPE_ARP</td>
<td>5292</td>
</tr>
<tr>
<td>SISF_PKT_TYPE_DHCP</td>
<td>140</td>
</tr>
<tr>
<td>SISF_PKT_TYPE_DHCP6</td>
<td>1213</td>
</tr>
<tr>
<td>SISF_PKT_TYPE_IPV6_ND</td>
<td>350</td>
</tr>
<tr>
<td>SISF_PKT_TYPE_DATA_GLEAN</td>
<td>44</td>
</tr>
<tr>
<td>SISF_PKT_TYPE_DATA_GLEAN_V6</td>
<td>51</td>
</tr>
<tr>
<td>SISF_PKT_TYPE_DHCP_RELAY</td>
<td>122</td>
</tr>
<tr>
<td>CAPWAP_PKT_TYPE_CAPWAP_RESERVED</td>
<td>0</td>
</tr>
</tbody>
</table>
Verifying Internal DHCP Configuration
WLAN Security

- Information About WPA1 and WPA2, on page 1133
- Information About AAA Override, on page 1134
- Prerequisites for Layer 2 Security, on page 1137
- How to Configure WLAN Security, on page 1138

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.
- CCKM—Cisco Centralized Key Management (CCKM) uses a fast rekeying technique that enables clients to roam from one access point to another without going through the controller, typically in under 150 milliseconds (ms). CCKM reduces the time required by the client to mutually authenticate with the new access point and derive a new session key during reassociation. CCKM fast secure roaming ensures that there is no perceptible delay in time-sensitive applications, such as wireless Voice over IP (VoIP), Enterprise Resource Planning (ERP), or Citrix-based solutions. CCKM is a CCXv4-compliant feature. If CCKM is selected, only CCKM clients are supported.

When CCKM is enabled, the behavior of access points differs from the controller’s for fast roaming in the following ways:

- If an association request sent by a client has CCKM enabled in a Robust Secure Network Information Element (RSN IE) but CCKM IE is not encoded and only PMKID is encoded in RSN IE, then the controller does not do a full authentication. Instead, the controller validates the PMKID and does a four-way handshake.
• If an association request sent by a client has CCKM enabled in RSN IE and CCKM 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 CCKM is enabled in RSN IE.

• 802.1X+CCKM—During normal operation, 802.1X-enabled clients mutually authenticate with a new access point by performing a complete 802.1X authentication, including communication with the main RADIUS server. However, when you configure your WLAN for 802.1X and CCKM fast secure roaming, CCKM-enabled clients securely roam from one access point to another without the need to reauthenticate to the RADIUS server. 802.1X+CCKM is considered as an optional CCKM because both CCKM and non-CCKM clients are supported when this option is selected.

On a single WLAN, you can allow WPA1, WPA2, and 802.1X/PSK/CCKM/802.1X+CCKM clients to join. All of the access points on such a WLAN advertise WPA1, WPA2, and 802.1X/PSK/CCKM/802.1X+CCKM information elements in their beacons and probe responses. When you enable WPA1 and/or WPA2, you can also enable one or two ciphers, or cryptographic algorithms, designed to protect data traffic. Specifically, you can enable AES and/or TKIP data encryption for WPA1 and/or WPA2. TKIP is the default value for WPA1, and AES is the default value for WPA2.

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.

Configuring AAA Override

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless profile policy profile-policy</td>
<td>Configures WLAN policy profile and enters the wireless policy configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless profile policy test-wgb</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>aaa-override</td>
<td>Configures AAA policy override.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-policy)# aaa-override</td>
<td>Note: If VLAN is not pushed from the RADIUS server, the VLAN Override feature can be disabled from the RADIUS server.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Purpose

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

---

### Information About VLAN Override

The VLAN override requires the AAA Override to be enabled under the Policy Profile.

You can assign VLAN from the RADIUS server in two ways:

- Using IETF RADIUS attributes 64, 65, and 81—The attribute 81 can be a VLAN ID, VLAN name, or VLAN group name. Both VLAN name and VLAN group are supported. Therefore, VLAN ID does not need to be predetermined on RADIUS.

  The RADIUS user attributes used for the VLAN ID assignment are:
  
  - 64 (Tunnel-Type)—Must be set to VLAN (Integer = 13).
  - 65 (Tunnel-Medium-Type)—Must be set to 802 (Integer = 6).
  - 81 (Tunnel-Private-Group-ID)—Must be set to the corresponding VLAN ID, VLAN name, or VLAN group name.

- Using Aire-Interface-Name attribute—Use this attribute to assign a successfully authenticated user to a VLAN interface name (or VLAN ID) as per the user configuration. When you use this attribute, the VLAN name is returned as a string.

  The VLAN ID is 12-bits, and takes a value between 1 and 4094, inclusive. Because the Tunnel-Private-Group-ID is of type string, as defined in RFC2868 for use with IEEE 802.1X, the VLAN ID integer value is encoded as a string. When these tunnel attributes are sent, it is necessary to fill in the Tag field.

### Configuring Override VLAN for Central Switching

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> vlan vlan-id</td>
<td>Defines VLANs that can be pushed from the RADIUS server.</td>
</tr>
<tr>
<td>Example: Device(config)# vlan 20</td>
<td>Note: The valid VLAN ID ranges from 1 to 4094.</td>
</tr>
<tr>
<td><strong>Step 3</strong> name vlan-name</td>
<td>(Optional) Changes the default name of the VLAN.</td>
</tr>
<tr>
<td>Example: Device(config-vlan)# name vlan_ascii</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Override VLAN for Local Switching

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless profile flex flex_profile_name</td>
<td>Configures a Flex profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless profile flex rr-xyz-flex-profile</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vlan-name vlan_name</td>
<td>Defines VLANs that can be pushed from the RADIUS server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-flex-profile)# vlan-name vlan_123</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> vlan-id vlan_id</td>
<td>Configures VLAN ID.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>The valid VLAN ID ranges from 1 to 4096.</td>
</tr>
<tr>
<td>Device(config-wireless-flex-profile-vlan)# vlan-id 23</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Device(config-wireless-flex-profile-vlan)# end</td>
<td></td>
</tr>
</tbody>
</table>

#### VLAN Override on Layer 3 Web Authentication

The VLAN override can be pushed from the RADIUS server upon Layer3 authentication.

When a client gets connected to the controller and authenticated using the RADIUS server for Local Web Authentication (LWA) and Central Web Authentication (CWA), the RADIUS server pushes back in access-accept the new VLAN. If the RADIUS server pushes back a new VLAN in the access-accept, the client goes back to IP learn state on the controller. The controller de-associates the client while maintaining the client state for 30 seconds. Once the client re-associates, the client lands immediately to the new VLAN and re-triggers a new DHCP request. The client then learns a new IP and moves to the RUN state on the controller.

The VLAN Override on Layer 3 Web authentication supports the following:
• Local clients
• Anchored clients
• FlexConnect central authentication, central or local switching

Verifying VLAN Override on Layer 3 Web Authentication

To display the VLAN override after L3 authentication, use the following command:

```
Device# show wireless client mac <mac> detail
[...]
  Vlan Override after L3 Auth: True
```

To display the statistics about client, use the following command:

```
Device# show wireless stats client detail
[...]
  Total L3 VLAN Override vlan change received : 1
  Total L3 VLAN Override disassociations sent : 1
  Total L3 VLAN Override re-associations received : 1
  Total L3 VLAN Override successful VLAN change : 1
[...]
  L3 VLAN Override connection timeout : 0
```

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**

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

Example:

```
Device# configure terminal
```
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><code>wlan profile-name wlan-id SSID_Name</code></td>
<td>Enters the WLAN configuration submode. <code>profile-name</code> is the profile name of the configured WLAN. <code>wlan-id</code> is the wireless LAN identifier. The range is 1 to 512. <code>SSID_Name</code> is the SSID which can contain 32 alphanumeric characters. <strong>Note</strong> If you have already configured this command, enter <code>wlan profile-name</code> command.</td>
</tr>
<tr>
<td>3</td>
<td><code>disable ft</code></td>
<td>Disables fast transition.</td>
</tr>
<tr>
<td>4</td>
<td><code>no security ft over-the-ds</code></td>
<td>Disables fast transition over the data source on the WLAN.</td>
</tr>
<tr>
<td>5</td>
<td><code>no security ft</code></td>
<td>Disables 802.11r Fast Transition on the WLAN.</td>
</tr>
<tr>
<td>6</td>
<td>`no security wpa{akm</td>
<td>wpa1</td>
</tr>
</tbody>
</table>
| 7    | `security static-wep-key [authentication {open | shared}]` | 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. |
| 8    | `security static-wep-key [encryption {104 | 40} {ascii | hex} [0 | 8]]` | The keywords are as follows:  
- **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
### Configuring WPA + WPA2 Layer 2 Security Parameters (GUI)

**Procedure**

1. Click **Configuration > Tags and Profiles > WLANs**.
2. Click **Add** to add a new WLAN Profile or click the one you want to edit.
3. In the **Edit WLAN** window, click **Security > Layer2**.
4. From **Layer 2 Security Mode** drop-down menu, select **WPA + WPA2**.
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
Configuring WPA + WPA2 Layer 2 Security Parameters (CLI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><strong>wlan profile-name wlan-id SSID_Name</strong></td>
<td>Enters the WLAN configuration submode. <em>profile-name</em> is the profile name of the configured WLAN. <em>wlan-id</em> is the wireless LAN identifier. The range is 1 to 512. <em>SSID_Name</em> is the SSID that contains 32 alphanumeric characters. <strong>Note</strong>: If you have already configured this command, enter <strong>wlan profile-name</strong> command.</td>
</tr>
<tr>
<td>3</td>
<td>**security wpa {akm</td>
<td>wpa1</td>
</tr>
<tr>
<td>4</td>
<td><strong>security wpa wpa1</strong></td>
<td>Enables WPA.</td>
</tr>
</tbody>
</table>
| 5    | **security wpa wpa1 ciphers [aes | tkip]** | 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 multicast interface by entering the following command: **encryption mode ciphers tkip**. |
<p>| 6    | <strong>security wpa akm {cckm | dot1x | dot1x-sha256 | ft | psk | psk-sha256</strong>} | Enable or disable CCKM, 802.1x, 802.1x with SHA256 key derivation type, Fast Transition, PSK or PSK with SHA256 key derivation type. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>You cannot enable 802.1x and PSK with SHA256 key derivation type simultaneously.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>security wpa akm psk set-key {ascii</td>
</tr>
<tr>
<td></td>
<td>Enter this command to specify a preshared key, if you have enabled PSK.</td>
</tr>
<tr>
<td></td>
<td>WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>security wpa akm ft {dot1x</td>
</tr>
<tr>
<td></td>
<td>Enable or disable authentication key management suite for fast transition.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>security wpa wpa2</td>
</tr>
<tr>
<td></td>
<td>Enables WPA2.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# security wpa</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>security wpa wpa2 ciphers aes</td>
</tr>
<tr>
<td></td>
<td>Configure WPA2 cipher.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# security wpa wpa2 ciphers aes</td>
</tr>
<tr>
<td></td>
<td>aes—Specifies WPA/AES support.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>show wireless pmk-cache</td>
</tr>
<tr>
<td></td>
<td>Displays the remaining time before the PMK cache lifetime timer expires.</td>
</tr>
<tr>
<td></td>
<td>If you have enabled WPA2 with 802.1X authenticated key management or WPA1 or WPA2 with CCKM authenticated key management, the PMK cache lifetime timer is used to trigger reauthentication with the client when necessary. The timer is based on the timeout value received from the AAA server or the WLAN session timeout setting.</td>
</tr>
<tr>
<td></td>
<td>If you have enabled WPA2 with 802.1X authenticated key management, the controller supports both opportunistic PMKID caching and sticky (or non-opportunistic) PMKID caching. In sticky PMKID caching (SKC), the client stores multiple PMKIDs, that is, a different PMKID for every AP it associates with. Opportunistic PMKID Caching (OKC) stores only one PMKID per client. By default, the controller supports OKC.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The command will show VLAN ID with VLAN pooling feature in VLAN-Override field.</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <strong>end</strong></td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
</tbody>
</table>
Configuring WPA + WPA2 Layer 2 Security Parameters (CLI)
Workgroup Bridges

- Information About Cisco Workgroup Bridges, on page 1145
- Configuring Workgroup Bridge on a WLAN, on page 1146
- Verifying the Status of a Workgroup Bridge, on page 1147

Information About Cisco Workgroup Bridges

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

Figure 31: Example of a WGB

The modes that are supported in WGB are:

- Local Mode: Central authentication, central switching.
- Flex Mode: Central authentication, local switching on Cisco Wave 2 APs.

The following table shows the supported and unsupported APs:
Table 56: WGB Support on APs

<table>
<thead>
<tr>
<th>WGB WLAN Support</th>
<th>Cisco Wave 1 APs</th>
<th>Cisco Wave 2 APs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Authentication</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Central Switching</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Local Authentication</td>
<td>Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Local Switching</td>
<td>Not Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Restrictions

- Central and local authentication is not supported for WGB wired clients on the controller or AP.
- 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.

Configuring Workgroup Bridge on a WLAN

Follow the procedure given below to configure a WGB on a WLAN:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>wireless profile policy profile-policy</td>
<td>Configures WLAN policy profile and enters the wireless policy configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# wireless profile policy test-wgb</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>aaa-override</td>
<td>Configures AAA policy override.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)# aaa-override</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>no central authentication</td>
<td>Configures the WLAN for local authentication.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-wireless-policy)# no central authentication</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> description description</td>
<td>Adds a description for the policy profile.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# description “test-wgb”</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> idle-timeout value</td>
<td>Sets the idle timeout value.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# idle-timeout 3600</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> session-timeout value</td>
<td>Sets the session timeout value.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# session-timeout 300</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> vlan vlan-no</td>
<td>Assigns the profile policy to the VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# vlan 48</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> wgb vlan</td>
<td>Configures WGB VLAN client support.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# wgb vlan</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> wgb broadcast-tagging</td>
<td>Configures WGB broadcast tagging on a WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# wgb broadcast-tagging</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> no shutdown</td>
<td>Restarts the WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-policy)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>

### Verifying the Status of a Workgroup Bridge

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:
Verifying the Status of a Workgroup Bridge

Device# show wireless wgb mac-address 00:0d:ed:dd:25:82 detail
Peer-to-Peer Client Support

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 the local switching WLAN.

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.
- Unified solution for central switching clients supports peer-to-peer upstream-forward. However, this is not supported in the FlexConnect solution; it is treated as peer-to-peer drop and client packets are dropped.

Configure Peer-to-Peer Client Support

Follow the procedure given below to configure Peer-to-Peer Client Support:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters WLAN configuration submode. The <em>profile-name</em> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td><em>wlan profile-name</em></td>
<td>Example: Device(config)# wlan wlan1</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures peer-to-peer blocking parameters.</td>
</tr>
<tr>
<td>*peer-blocking [drop</td>
<td>Enables peer-to-peer blocking on the drop action.</td>
</tr>
<tr>
<td>forward-upstream ]*</td>
<td><em>forward-upstream</em>—Enables peer-to-peer blocking on the forward upstream action.</td>
</tr>
<tr>
<td>Example: Device(config-wlan)# peer-blocking drop</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><em>end</em></td>
<td>Example: Device(config)# end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Displays the details of the selected WLAN.</td>
</tr>
<tr>
<td><em>show wlan id wlan-id</em></td>
<td>Example: Device# show wlan id 12</td>
</tr>
</tbody>
</table>
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.

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 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.

To use IRCM with AireOS in your network, contact Cisco TAC for assistance.

<table>
<thead>
<tr>
<th>Controller Name</th>
<th>Supported as Guest Anchor</th>
<th>Supported as Guest Foreign</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Catalyst 9800-40 Wireless Controller</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Catalyst 9800-80 Wireless Controller</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Catalyst 9800-CL Wireless Controller</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Catalyst 9800 Embedded Wireless Controller for Switch</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

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 + LWA
  - PSK + CWA
  - PSK + LWA
  - iPSK + CWA

- 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.

---

**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.
Guidelines and Limitations for Wireless Guest Access

- This feature is supported from Cisco AireOS 8.8.111.0 onwards.
- 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.

IPv6 Limitations

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
    - Nexus platform—has solicited unicast RA enabled by default to help with wireless deployment.
    - IOS-XE platform—Use the following configuration knob 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 knob to enable solicited unicast RA then a work around does not exist.

Configure Mobility Tunnel for Guest Access (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Click Configure &gt; Tags and Profiles &gt; WLANs.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Wireless Networks area, click the relevant WLAN or RLAN and click Mobility Anchor.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Wireless Network Details section, choose a device from the Switch IP Address drop-down list.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Apply.</td>
</tr>
</tbody>
</table>
Configure Mobility Tunnel for Guest Access

Follow the procedure given below to configure a mobility tunnel

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>wireless mobility group name <code>group name</code></td>
<td>Configures a mobility group.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# wireless mobility group name mtunnelgrp</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wireless mobility mac-address <code>mac address</code></td>
<td>Configures a mobility MAC address.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# wireless mobility mac-address 0d:4c:da:3a:f2:21</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>wireless mobility group member mac <code>mac address</code> ip <code>ip address</code> group <code>group name</code></td>
<td>Configures a mobility peer.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# wireless mobility group member mac-address df:07:a1:a7:a8:55 ip 206.223.123.2 group mtgrp</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Guest Access Policy

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**

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

**Step 2**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>wireless profile policy wlan_policy_profile</strong></td>
<td>Configures the policy profile and enters wireless profile configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless profile policy guest-test-policy</td>
</tr>
</tbody>
</table>

**Note**
- You can use the `default-policy-profile` to configure the profile policy.

**Step 3**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>shutdown</strong></td>
<td>Shuts down the policy if it exists before configuring the anchor.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# shutdown</td>
</tr>
</tbody>
</table>

**Step 4**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>central switching</strong></td>
<td>(Optional) Enables central switching.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# central switching</td>
</tr>
</tbody>
</table>

**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

**Step 6**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>idle-timeout timeout</strong></td>
<td>(Optional) Configures duration of idle timeout, in seconds.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# idle-timeout 1000</td>
</tr>
</tbody>
</table>

**Step 7**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vlan vlan-id</strong></td>
<td>Configures VLAN name or VLAN Id.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# vlan 2</td>
</tr>
</tbody>
</table>

**Note**
- VLAN is optional for a Guest Foreign controller.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>no shutdown</td>
<td>Enables policy profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# no shutdown</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>end</td>
<td>Exits the configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# end</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>show wireless profile policy summary</td>
<td>(Optional) Displays the configured profiles.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show wireless profile policy summary</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>show wireless profile policy detailed policy-profile-name</td>
<td>(Optional) Displays detailed information of a policy profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show wireless profile policy detailed guest-test-policy</td>
<td></td>
</tr>
</tbody>
</table>

### 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
  ```
Configuring Site Tag

Follow the procedure given below to configure the site tag:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wireless tag site site-tag-name</code></td>
<td>Configures the site tag and enters the site tag profile configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device (config)# wireless tag site site-tag-name</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ap profile ap-profile</code></td>
<td>Maps the AP profile to the site.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device (config-site-tag)# ap profile temp-ap-profile</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>description site-tag-name</code></td>
<td>Adds the description to the site tag.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device (config-site-tag)# description &quot;description-of-site-tag&quot;</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code></td>
<td>Exits the configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device (config-site-tag)# end</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>show wireless tag site summary</code></td>
<td>Displays the number of site tags.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# show wireless tag site summary</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>show wireless tag site detailed site-tag-name</code></td>
<td>Displays detailed information of a site tag.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# show wireless tag site detailed site-tag-name</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Policy Tag

Follow the procedure given below to configure the policy tag.
Configuring a policy tag is not required for anchors if not used along with AVC.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 wireless tag policy policy-tag-name</td>
<td>Configures the policy tag and enters the policy tag profile configuration mode.</td>
</tr>
<tr>
<td>Example: Device (config)# wireless tag policy guest-tag-policy</td>
<td></td>
</tr>
<tr>
<td>Step 3 wlan wlan-name policy profile-policy-name</td>
<td>Maps a policy profile to a WLAN profile.</td>
</tr>
<tr>
<td>Example: Device (config-policy-tag)# wlan test-wlan policy guest-test-policy</td>
<td></td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Exits the configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device (config-policy-tag)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5 show wireless tag policy summary</td>
<td>Displays the configured policy tags.</td>
</tr>
<tr>
<td>Example: Device# show wireless tag policy summary</td>
<td></td>
</tr>
<tr>
<td>Step 6 show wireless tag policy detailed policy-profile-name</td>
<td>Displays detailed information of a policy tag.</td>
</tr>
<tr>
<td>Example: Device# show wireless tag policy detailed guest-test-policy</td>
<td></td>
</tr>
</tbody>
</table>

### Associating Policy Tag to an AP

You have the option to include the mobility anchor in the default policy profile.
### Attaching Site Tag and Policy Tag to an AP

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap filter name &lt;filter-name&gt;</td>
<td>Configures an AP filter.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# ap filter name guest-ap-filter Device(config-ap-filter)# ap name-regex ap-name</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> tag policy &lt;policy-tag-name&gt;</td>
<td>Configures a policy tag for the filter.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-ap-filter)# tag policy policy-tag-name</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> wlan &lt;wlan-name&gt; policy &lt;profile-policy-name&gt;</td>
<td>Maps a policy profile to a WLAN profile.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-policy-tag)# wlan test-wlan policy guest-test-policy</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits the configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-policy-tag)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show wireless tag policy summary</td>
<td>Displays the configured policy tags.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# show wireless tag policy summary</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> show wireless tag policy detailed &lt;policy-profile-name&gt;</td>
<td>Displays detailed information of a policy tag.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# show wireless tag policy detailed guest-test-policy</td>
<td></td>
</tr>
</tbody>
</table>
Configure Guest Access Using Different Security Methods

Open Authentication

To configure the guest access with open authentication, follow the steps:

1. Configure the WLAN Profile.
2. Applying Policy Profile on a WLAN

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**  
`ap mac-address`  
**Example:**  
Device (config)# ap e2:d0:f3:d3:c0:8e  
**Note**  
Use the Ethernet MAC address.

**Step 3**  
`policy-tag policy-tag-name`  
**Example:**  
Device (config-ap-tag)# policy-tag guest-tag-policy  
Maps a policy tag to an AP.

**Step 4**  
`site-tag site-tag-name`  
**Example:**  
Device (config-ap-tag)# site-tag site-tag-name  
Maps a site tag to an AP.

**Step 5**  
`end`  
**Example:**  
Device (config-ap-tag)# end  
Exits the configuration mode and returns to privileged EXEC mode.

**Step 6**  
`show ap tag summary`  
**Example:**  
Device# show wireless tag policy summary  
Displays the ap details and tags that are associated to it.
## Configure WLAN Profile For Guest Access with Open Authentication

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wlan profile-name wlan-id ssid-name.</td>
<td>Configures the WLAN and SSID.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wlan mywlan 34 mywlan-ssid</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>no security wpa</td>
<td>Disables WPA security.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# no security wpa</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>no security wpa akm dot1x</td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# no security wpa akm dot1x</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>no security wpa wpa2</td>
<td>Disables WPA2 security.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# no security wpa wpa2</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>no security wpa wpa2 ciphers aes</td>
<td>Disables WPA2 ciphers for AES.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# no security wpa wpa2 ciphers aes</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>no shutdown</td>
<td>Saves the configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring the Policy Profile

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>wireless profile policy  wlan-policy-profile</td>
<td>Configures WLAN policy profile and enters the wireless policy configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# wireless profile policy open_it</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Choose the first option to configure a Guest Foreign or second option to configure a Guest Anchor: • mobility anchor anchor-ip-address • mobility anchor</td>
<td>Configures Guest Foreign or Guest Anchor.</td>
</tr>
<tr>
<td></td>
<td>Example: For Guest Foreign: Device(config-wireless-policy)# mobility anchor 19.0.2.1 For Guest Anchor: Device(config-wireless-policy)# mobility anchor</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>central switching.</td>
<td>Enables Central switching</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)# central switching</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vlan id</td>
<td>Configures a VLAN name or VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)# vlan 16</td>
<td>Note: VLAN is optional for a Guest Foreign controller.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>no shutdown</td>
<td>Enables the policy profile.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>

**Local Web Authentication**

To configure LWA, follow the steps:

1. Configure the Parameter Map
2. Configure WLAN Profile for Guest Access with Local Web Authentication
3. Applying Policy Profile on a WLAN
4. Configure AAA Server for Local Web Authentication
## Configure the Parameter Map

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> parameter-map type webauth global</td>
<td>Creates a parameter map and enters parameter-map webauth configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# parameter-map type webauth global</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> type webauth</td>
<td>Configures the webauth type parameter.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-params-parameter-map)#type webauth</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> timeout init-state sec timeout-seconds</td>
<td>Configures the WEBAUTH timeout in seconds. Valid range for the time in sec parameter is 60 to 3932100 seconds.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-params-parameter-map)#timeout inti-state sec 3600</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> virtual-ip ipv4 virtual_IP_address</td>
<td>Configures a VLAN name or VLAN ID.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-params-parameter-map)#virtual-ip ipv4 209.165.201.1</td>
<td></td>
</tr>
</tbody>
</table>

## Configure WLAN Profile for Guest Access with Local Web Authentication

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wlan wlan-id ssid-name</td>
<td>Configures the WLAN and SSID.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# Device(config)# wlan mywlan 38 mywlan-ssid1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> security web-auth</td>
<td>Enables web authentication for a WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wlan)# security web-auth</td>
<td></td>
</tr>
</tbody>
</table>
Configure AAA Server for Local Web Authentication

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> aaa authentication login *LWA-AUTHENTICATION* local</td>
<td>Defines the authentication method at login.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# aaa authentication login lwa-authentication local</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa authorization network default local if-authenticated</td>
<td>Sets the authorization method to local if the user has authenticated.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# aaa authorization network default local if-authenticated</td>
<td></td>
</tr>
</tbody>
</table>

**Global Configuration**

Follow the procedure given below for global configuration:
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Enters global configuration mode.</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Sets the clear text password for the user.</strong></td>
</tr>
<tr>
<td><code>username name password 0</code></td>
<td></td>
</tr>
<tr>
<td><code>clear-text-password</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# <code>username base password 0 pass1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>** Enables the HTTP server.**</td>
</tr>
<tr>
<td><code>ip http server</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# <code>ip http server</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Sets the HTTP server authentication method to local.</strong></td>
</tr>
<tr>
<td><code>ip http authentication local</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# <code>ip http authentication local</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You will get the admin access rights regardless of the user privilege, if the <code>ip http authentication local</code> is disabled and username is the same as enable password.</td>
</tr>
</tbody>
</table>

---

### Central Web Authentication

To configure the CWA, follow the steps:

1. Configure WLAN Profile for Guest Access with Central Web Authentication
2. Applying Policy Profile on a WLAN
3. AAA Server Configuration

### Configure WLAN Profile for Guest Access with Central Web Authentication

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Enters global configuration mode.</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Configures the WLAN and SSID.</strong></td>
</tr>
<tr>
<td><code>wlan wlan-id ssid-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# <code>wlan wlan-id ssid-name</code></td>
<td></td>
</tr>
</tbody>
</table>
### AAA Server Configuration

#### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# Device(config)# wlan mywlan 38 mywlan-ssid1</td>
<td>Enables MAB authentication for the remote RADIUS server.</td>
</tr>
<tr>
<td>Step 3 mac-filtering remote_authorization_list_name</td>
<td>Enables MAB authentication for the remote RADIUS server.</td>
</tr>
<tr>
<td>Example: Device(config-wlan)# mac-filtering auth-list</td>
<td></td>
</tr>
<tr>
<td>Step 4 no security wpa</td>
<td>Disables WPA security.</td>
</tr>
<tr>
<td>Example: Device(config-wlan)# no security wpa</td>
<td></td>
</tr>
<tr>
<td>Step 5 no security wpa akm dot1x</td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td>Example: Device(config-wlan)# no security wpa akm dot1x</td>
<td></td>
</tr>
<tr>
<td>Step 6 no security wpa wpa2</td>
<td>Disables WPA2 security.</td>
</tr>
<tr>
<td>Example: Device(config-wlan)# no security wpa wpa2</td>
<td></td>
</tr>
<tr>
<td>Step 7 no security wpa wpa2 ciphers aes</td>
<td>Disables WPA2 ciphers for AES.</td>
</tr>
<tr>
<td>Example: Device(config-wlan)# no security wpa wpa2 ciphers aes</td>
<td></td>
</tr>
<tr>
<td>Step 8 no shutdown</td>
<td>Saves the configuration.</td>
</tr>
<tr>
<td>Example: Device(config-wlan)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>

#### AAA Server Configuration

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 aaa authorization network authorization-list local group Server-group-name</td>
<td>Sets the authorization method to local.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)#aaa authorization network cwa local group ise</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <strong>aaa group server radius server-group-name</strong></td>
<td>Configures RADIUS server group definition. <strong>Note</strong> server-group-name refers to the server group name. The valid range is from 1 to 32 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)#aaa group server radius ise</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <strong>server name radius-server-name</strong></td>
<td>Configures the RADIUS server name.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-sg-radius)#server name ise</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <strong>subscriber mac-filtering security-mode mac</strong></td>
<td>Sets the MAC address as the password.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-sg-radius)#$mac-filtering security-mode mac</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <strong>mac-delimiter colon</strong></td>
<td>Sets the MAC address delimiter to colon.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-sg-radius)#mac-delimiter colon</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> <strong>end</strong></td>
<td>Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-sg-radius)#end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> <strong>radius server name</strong></td>
<td>Sets the RADIUS server name</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)#radius server ISE1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> <strong>address ipv4 radius-server-ipaddress auth-port port-number acct-port port-number</strong></td>
<td>Configures the RADIUS server IP address authentication and accounting ports.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-radius-server)#address ipv4 209.165.201.1 auth-port 1635 acct-port 33</td>
<td></td>
</tr>
</tbody>
</table>
# Configuring 802.1x with Local Web Authentication

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>wlan wlan-profile wlan-id ssid</code></td>
<td>Configures the WLAN and SSID.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wlan testwprofile 22 ssid-3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>security dot1x authentication-list default</code></td>
<td>Configures 802.1X for an WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# security dot1x authentication-list default</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>security web-auth authentication-list authenticate-list-name</code></td>
<td>Enables authentication list for 802.1x security on the WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# security web-auth authentication-list default</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>security web-auth parameter-map global</code></td>
<td>Configures the global parameter map.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# security web-auth parameter-map global</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>no shutdown</code></td>
<td>Enables the WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wlan)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>

# Configuring Local Web Authentication with PSK Protocol

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>wlan wlan-profile wlan-id ssid</code></td>
<td>Configures the WLAN and SSID.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wlan testwprofile 22 ssid-3</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Device(config)# wlan psksec-profile 22 ssid-4</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> no security wpa</td>
<td>Disables WPA security.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# no security wpa</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no security wpa wpa2</td>
<td>Disables WPA2 security.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# no security wpa wpa2</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> no security wpa akm dot1x</td>
<td>Disables security AKM for dot1x.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# no security wpa akm dot1x</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> security wpa psk</td>
<td>Enables the security type as PSK.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# security wpa akm psk</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> security wpa psk set-key { ascii | hex } key</td>
<td>Configures the PSK shared key.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# security wpa akm psk set-key ascii 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> security web-auth</td>
<td>Enables the web authentication for the WLAN.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# security web-auth</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> security web-auth authentication-list default</td>
<td>Enables authentication list for the WLAN.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# security web-auth authentication-list default</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> security web-auth parameter-map global</td>
<td>Configure the global parameter map.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-wlan)# security web-auth parameter-map global</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Central Web Authentication with PSK Protocol

To configure the CWA with PSK security protocol, follow the steps:

1. **Configure WLAN Profile for Central Web Authentication with PSK Protocol**
2. Applying Policy Profile on a WLAN

## Configure WLAN Profile for Central Web Authentication with PSK Protocol

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wlan wlan-profile wlan-id ssid</code></td>
<td>Configures the WLAN and SSID.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wlan cwasec-profile 27 ssid=5</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>no security wpa</code></td>
<td>Disables WPA security.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# no security wpa</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>no security wpa wpa2</code></td>
<td>Disables WPA2 security.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# no security wpa wpa2</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>no security wpa akm dot1x</code></td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# no security wpa akm dot1x</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>security wpa psk</code></td>
<td>Enables the security type as PSK.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# security wpa psk</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>`security wpa psk set-key {ascii</td>
<td>hex} key`</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# security wpa psk set-key ascii 0</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>mac-filtering authorization_list_name</code></td>
<td>Enables MAC filtering for PSK web authentication.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wlan)# mac-filtering cwa-list</td>
<td></td>
</tr>
</tbody>
</table>

## Central Web Authentication with IPSK Protocol

To configure the CWA with IPSK security protocol, follow the steps:
Configure WLAN Profile for Central Web Authentication with iPSK Protocol

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configures guest WLAN.</td>
</tr>
<tr>
<td><code>wlan guest-wlan-name wlan-id ssid</code></td>
<td>Configures guest WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>config # wlan ipsk-cwa-profile 28 ssid-6</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Disables security AKM for 802.1x.</td>
</tr>
<tr>
<td><code>no security wpa akm dot1x</code></td>
<td>Disables security AKM for 802.1x.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-wlan) # no security wpa akm dot1x</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the PSK AKM shared key.</td>
</tr>
<tr>
<td>`security wpa akm psk set-key {ascii</td>
<td>hex} key`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-wlan) # security wpa akm psk set-key ascii 0</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables MAC filtering for iPSK authentication.</td>
</tr>
<tr>
<td><code>mac-filtering authorization_list_name</code></td>
<td>Enables MAC filtering for iPSK authentication.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-wlan) # mac-filtering cwa-list</code></td>
<td></td>
</tr>
</tbody>
</table>

Configure Web Authentication on MAC 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, click **Security > Layer3**.

**Step 4** Click **Show Advanced Settings** and check the **On MAC Filter Failure** checkbox.

Configure Web Authentication on MAC Failure

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:

**Configuring Policy Profile**

**Procedure**

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

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>wireless profile policy policy-name</td>
<td>Configures WLAN policy profile and enters the wireless policy configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless profile policy cwa</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>central switching</td>
<td>Enables Central switching.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# central switching</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Choose the first option to configure a Guest Foreign or second option to configure a Guest Anchor:</td>
<td>Configures Guest Foreign or Guest Anchor.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• mobility anchor anchor-ip-address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• mobility anchor</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>For Guests Foreign:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device (config-wireless-policy)# mobility anchor 19.0.2.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For Guest Anchor:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device (config-wireless-policy)# mobility anchor</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vlan name</td>
<td>Configures a VLAN name or VLAN ID.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# vlan 16</td>
<td></td>
</tr>
</tbody>
</table>

| Note | VLAN is optional for a Guest Foreign controller. |

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>no shutdown</td>
<td>Enables the policy profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>
Configuring WLAN Profile

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>wlan guest-wlan-name wlan-id ssid</code></td>
<td>Configures guest WLAN. <strong>Example:</strong> config# wlan test-wlan-guest 10 wlan-ssid</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>security web-auth</code></td>
<td>Enables web authentication. <strong>Example:</strong> config-wlan# security web-auth</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>security web-auth on-macfilter-failure</code></td>
<td>Enables web authentication if MAC filter authentication fails. <strong>Example:</strong> config-wlan# security web-auth on-macfilter-failure</td>
</tr>
</tbody>
</table>

**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**
  - **Foreign1:** wlanProf1 PolicyProf1
  - **Foreign2:** wlanProf2 PolicyProf2

- **Guest Anchor**
  - 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

This feature while performing as a 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.
CHAPTER 127

Wired Guest Access

• Information About Wired Guest Access, on page 1177
• Restrictions for Wired Guest Access, on page 1180
• Configuring Access Switch for Wired Guest Client, on page 1180
• Configuring Access Switch for Foreign Controller, on page 1181
• Configuring Foreign Controller with Open Authentication, on page 1182
• Configuring Foreign Controller with Local WEB Authentication, on page 1183
• Configuring Anchor Controller with Open Authentication, on page 1185
• Configuring Anchor Controller with Local Web Authentication, on page 1186
• Configuring Session Timeout for a Profile Policy, on page 1188
• Verifying Wired Guest Configurations, on page 1188
• Wired Guest Access—Use Cases, on page 1192

Information About Wired Guest Access

The Wired Guest Access feature enables guest users of an enterprise network that supports both wired and wireless access to connect to the guest access network. The wired guest clients can connect from the designated and configured wired Ethernet ports for the guest access after they complete the configured authentication methods. Wired session guests are directed to a wireless guest controller in a demilitarized zone (DMZ) through a Control And Provisioning of Wireless Access Points (CAPWAP) tunnel.

Wired guest access can be configured in a dual-controller configuration that uses both an anchor controller and a foreign controller. A dual-controller configuration isolates wired guest access traffic from the enterprise user traffic.

The wired session guests are provided open or web-authenticated access from the wireless controller.
IPv6 Router Advertisement Forwarding for a Wired Guest

Wired clients get the IPv6 based connectivity when they receive the IPv6 Router Advertisement (RA) message. The IPv6 router sends these RA messages and it contains information such as IPv6 prefix and router link-local address.

These RA messages are sent as Unicast or Multicast messages. The Unicast RA messages are routed as same as the client directed traffic. The Multicast RA messages are forwarded to all the clients present in the intended VLAN. RA message forwarding is enabled by default and requires no specific configuration.

**Guest Anchor Controller:** Guest anchor controller forwards the RA packets, from the receiving VLAN, to all the foreign controllers using the mobility data tunnel. The RA packets are tagged with the anchor VLAN to ensure the message is forwarded to the correct clients using the foreign controller data path.

**Guest Foreign Controller:** Guest foreign controller forwards the received RAs from the guest anchor to the wired ports on which the wired guest clients are connected. To forward the RAs to the intended clients, the guest foreign controller keeps a track of the wired guest clients–per interface, access VLANS, and anchor VLANS.

**Supported Features**

- Cisco Catalyst 9800 Series Wireless Controllers-Anchor
- Cisco AireOS Wireless Controllers-Anchor
- Cisco Catalyst 9800 Series Wireless Controllers-Foreign
- Cisco AireOS Wireless Controllers-Foreign
- Dual controller solution (foreign + anchor) and access switch
- Trunk Ports
- Open Authentication
- Local Web Authentication
To configure Web Authentication, see Web-based Authentication section of the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.

- **Local Web Authentication (web consent).**

**Note** In AireOS, this is referred to as **web pass-through**.

- Local Web Authentication + ISE (External Web Authentication).
- LWA (local web authentication), with a username and a password.
- Web consent (LWA + consent), that is with a username, a password and the check box of acceptance.

- Scale max 2k clients and 5 guest-LANs (5 VLANs max)
- Client IPv6 support
- Idle Timeout and Session Timeout
- Accounting on Foreign

**Note** Statistics computation not supported.

- Manageability (SNMP/Yang/WebUI)
- QoS Rate-Limiting and MQC Policies (Upstream at foreign, Upstream, and Downstream at the anchor)

**Note** QoS rate-limiting supports bps rate-limiting, pps rate-limiting is not supported.

- QoS support with AireOS Anchor setup
- Stateful Switch Over (SSO)
- Port Channel support on Anchor and Foreign with no restrictions to the controller's role.
- Access Port on Foreign
- Cisco Umbrella (not supported in AireOS Anchor)
- ACL support at anchor
- Fully Qualified Domain Name (FQDN) URL filtering is supported at Anchor controller.
- IP theft detection
- Sleeping Client
Restrictions for Wired Guest Access

- A maximum of five guest LANs are supported on the foreign controller.
- A maximum of 2000 clients per foreign are supported.
- No Multicast or Broadcast support.
- You can map only one wired VLAN to a guest LAN.
- You can map only one guest LAN to one policy profile.
- Every guest LAN has a unique name and this name cannot be shared with RLAN or WLAN.
- Ensure that the Anchor VLAN ID and the wired VLAN ID configured on the Foreign controller is not the same.
- QoS is not supported on VLAN and on physical interfaces of the controller.

Configuring Access Switch for Wired Guest Client

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>(\text{Example:}) Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>(\text{vlan} \quad \text{vlan-id})</td>
<td>Creates the VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>(\text{Example:}) Device(config)#vlan 200</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>exit</td>
<td>Returns to configuration mode.</td>
</tr>
<tr>
<td></td>
<td>(\text{Example:}) Device(config)#exit</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>interface GigabitEthernet(\text{interface number})</td>
<td>Enters the interface to be added to the VLAN.</td>
</tr>
<tr>
<td></td>
<td>(\text{Example:}) Device(config)#interface GigabitEthernet1/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>switchport access vlan (\text{vlan-id})</td>
<td>Assigns the port to a VLAN. The valid VLAN IDs range is between 1 and 4094.</td>
</tr>
<tr>
<td></td>
<td>(\text{Example:}) Device(config-if)#switchport access vlan 200</td>
<td></td>
</tr>
</tbody>
</table>
**Configuring Access Switch for Foreign Controller**

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>vlan vlan-id</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>Device(config)#vlan 200</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>exit</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>Device(config)#exit</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>interface GigabitEthernetinterface number</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>Device(config)#interface GigabitEthernet1/0/2</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>switchport trunk allowed vlan vlan-id</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>Device(config-if)#switchport trunk allowed vlan 200</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>switchport mode trunk</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>Device(config-if)#switchport mode trunk</td>
</tr>
</tbody>
</table>

### Purpose

- **Step 1**: Enters global configuration mode.
- **Step 2**: Creates the VLAN ID.
- **Step 3**: Returns to configuration mode.
- **Step 4**: Enters the interface to be added to the VLAN.
- **Step 5**: Assigns the allowed VLAN ID to the port when it is in trunking mode.
- **Step 6**: Sets the trunking mode to trunk unconditionally.
### Configuring Foreign Controller with Open Authentication

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>wireless profile policy</strong></td>
</tr>
<tr>
<td><strong>wlan-policy-profile-name</strong></td>
<td>Device(config)#wireless profile policy testpro-1</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Configures the WLAN policy profile.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>mobility anchor</strong></td>
</tr>
<tr>
<td><strong>non-local-mobility-cntlr-ip</strong></td>
<td>priority priority 1</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)#mobility anchor 192.168.201.111 priority 1</td>
</tr>
<tr>
<td></td>
<td>Configures the mobility anchor and sets its priority.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>no shutdown</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)#no shutdown</td>
</tr>
<tr>
<td></td>
<td>Enables the configuration.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)#exit</td>
</tr>
<tr>
<td></td>
<td>Returns to configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>guest-lan profile-name</strong></td>
</tr>
<tr>
<td><strong>guest-profile-name</strong></td>
<td><strong>guest-lan-id wired-vlan</strong></td>
</tr>
<tr>
<td><strong>wired-vlan-id</strong></td>
<td><strong>Device(config)#guest-lan profile-name gstpro-1 1 wired-vlan 25</strong></td>
</tr>
<tr>
<td></td>
<td>Configures guest LAN profile with a wired VLAN.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Configure the wired VLAN only for the Guest Foreign controller.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>no security web-auth</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)#no security web-auth</td>
</tr>
<tr>
<td></td>
<td>Disables web-authentication.</td>
</tr>
</tbody>
</table>
Purpose

Command or Action | Purpose
--- | ---
Device(config-guest-lan)#no security web-auth | Enables the guest LAN.

Step 8

no shutdown

Example:
Device(config-guest-lan)#no shutdown

Enables the guest LAN.

Step 9

exit

Example:
Device(config-guest-lan)#exit

Returns to configuration mode.

Step 10

wireless guest LAN map gst-map-name

Example:
Device(config)#wireless guest LAN map gstmap-1

Configures a guest LAN map.

Step 11

guest-lan guest-profile-name policy wlan-policy-profile-name

Example:
Device(config-guest-lan-map)#guest-lan gstpro-1 policy testpro-1

Attaches a guest LAN map to the policy profile.

Step 12

exit

Example:
Device(config-guest-lan-map)#exit

Returns to configuration mode.

Configuring Foreign Controller with Local WEB Authentication

Procedure

Command or Action | Purpose
--- | ---
Step 1 configure terminal | Enters global configuration mode.

Example:
Device# configure terminal

Step 2 wireless profile policy wlan-policy-profile-name | Configures the WLAN policy profile.

Example:
Device(config)#wireless profile policy testpro-1

Step 3 mobility anchor non-local-mobility-cntrl-ip priority priority | Configures the mobility anchor and sets its priority.

Example:
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-wireless-policy)#mobility anchor 192.168.201.111 priority 1</td>
<td>Enables the configuration.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>no shutdown</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)#no shutdown</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)#exit</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>guest-lan profile-name guest-profile-name guest-lan-id wired-vlan wired-vlan-id</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)#guest-lan profile-name gstpro-2 3 wired-vlan 26</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>security web-auth</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-guest-lan)#security web-auth</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>security web-auth authentication-list auth-list-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-guest-lan)#security web-auth authentication-list default</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>security web-auth parameter-map parameter-map-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-guest-lan)#security web-auth parameter-map global</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>no shutdown</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-guest-lan)#no shutdown</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-guest-lan)#exit</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>wireless guest-lan map gst-map-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)#wireless guest-lan map gstmap-2</td>
</tr>
</tbody>
</table>
### Configuring Anchor Controller with Open Authentication

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wireless profile policy wlan-policy-profile-name</td>
<td>Configures the WLAN policy profile.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)#wireless profile policy testpro-2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>mobility anchor</td>
<td>Configures the mobility anchor.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-_wireless-policy)#mobility anchor</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>vlan vlan-id</td>
<td>Configure a VLAN name or a VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config- wireless-policy)#vlan 29</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>no shutdown</td>
<td>Enables the configuration.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config- wireless-policy)#no shutdown</td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

**Configuring Anchor Controller with Local Web Authentication**

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless profile policy</td>
<td>Configures the WLAN policy profile.</td>
</tr>
<tr>
<td></td>
<td>wlan-policy-profile-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)#wireless profile policy testpro-2</td>
<td></td>
</tr>
</tbody>
</table>

---

**Table:**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>exit</td>
<td>Returns to configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-policy)#exit</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>guest-lan profile-name guest-profile-name guest-lan-id</td>
<td>Configures the guest LAN profile with a wired VLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)#guest-lan profile-name testpro-2</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>client association limit guest-lan-client-limit</td>
<td>Configures the maximum client connections per guest LAN. The valid range is between 1 and 2000.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-guest-lan)#client association limit</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td>no security web-auth</td>
<td>Disables web authentication.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-guest-lan)#no security web-auth</td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>no shutdown</td>
<td>Enables the guest LAN.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-guest-lan)#no shutdown</td>
<td></td>
</tr>
<tr>
<td>Step 11</td>
<td>exit</td>
<td>Returns to configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-guest-lan)#exit</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>3</td>
<td>mobility anchor</td>
<td>Configures the mobility anchor. <strong>Example:</strong> Device(config-wireless-policy)#mobility anchor</td>
</tr>
<tr>
<td>4</td>
<td>vlan vlan-id</td>
<td>Configure a VLAN name or a VLAN ID. <strong>Example:</strong> Device(config-wireless-policy)#vlan 30</td>
</tr>
<tr>
<td>5</td>
<td>no shutdown</td>
<td>Enables the configuration. <strong>Example:</strong> Device(config-wireless-policy)#no shutdown</td>
</tr>
<tr>
<td>6</td>
<td>exit</td>
<td>Returns to configuration mode. <strong>Example:</strong> Device(config-wireless-policy)#exit</td>
</tr>
<tr>
<td>7</td>
<td>guest-lan profile-name guest-profile-name guest-lan-id</td>
<td>Configure a guest LAN profile with a wired VLAN. <strong>Example:</strong> Device(config)#guest-lan profile-name testpro-2 1</td>
</tr>
<tr>
<td>8</td>
<td>client association limit guest-lan-client-limit</td>
<td>Configures the maximum client connections per guest LAN. The valid range is between 1 and 2000. <strong>Example:</strong> Device(config-guest-lan)#client association limit</td>
</tr>
<tr>
<td>9</td>
<td>security web-auth</td>
<td>Configures web authentication. <strong>Example:</strong> Device(config-guest-lan)#security web-auth</td>
</tr>
<tr>
<td>10</td>
<td>security web-auth parameter-map parameter-map-name</td>
<td>Configures the security web-auth parameter map. <strong>Example:</strong> Device(config-guest-lan)#security web-auth parameter-map testmap-1</td>
</tr>
<tr>
<td>11</td>
<td>security web-auth authentication-list authentication-list-name</td>
<td>Configures the authentication list for the IEEE 802.1x network. <strong>Example:</strong> Device(config-guest-lan)#security web-auth authentication-list testlwa-1</td>
</tr>
</tbody>
</table>
Configuring Session Timeout for a Profile Policy

Session Timeout for a wired guest is set to infinite by default. Perform the following procedure to configure the timeout values to the wired guest.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless profile policy</td>
<td>Configures the WLAN policy profile.</td>
</tr>
<tr>
<td>wlan-policy-profile-name</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)#wireless profile policy</td>
<td></td>
</tr>
<tr>
<td>testpol-1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> guest-lan enable-session-timeout</td>
<td>Enables the client session timeout on the guest LAN.</td>
</tr>
<tr>
<td>Example: Device(config-wireless-policy)#guest-lan</td>
<td></td>
</tr>
<tr>
<td>enable-session-timeout</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> session-timeout timeout-duration</td>
<td>Configures the client session timeout in seconds. The valid range is between 0 and 86400 seconds.</td>
</tr>
<tr>
<td>Example: Device(config-wireless-policy)#session-timeout</td>
<td></td>
</tr>
<tr>
<td>1000</td>
<td></td>
</tr>
</tbody>
</table>

**Verifying Wired Guest Configurations**

To validate the wireless configuration, use the following command:

```
Device# wireless config validate
```

Wireless Management Trustpoint Name: 'WLC-29c_WLC_TP'
Trustpoint certificate type is WLC-SSC
Wireless management trustpoint config is valid

Jan 22 07:49:15.371: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0: wncmgrd: Error in No record found for VLAN 9, needed by Guest-LAN open-wired

To display the summary of all Guest-LANs, use the following command:

Device# show guest-lan summary

Number of Guest LANs: 1

<table>
<thead>
<tr>
<th>GLAN</th>
<th>GLAN Profile Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>wired_guest_open</td>
<td>UP</td>
</tr>
</tbody>
</table>

To view the detailed output of all Guest-LANs, use the following command:

Device# show guest-lan all

Guest-LAN Profile Name : open

<table>
<thead>
<tr>
<th>Guest-LAN ID</th>
<th>Wired-Vlan</th>
<th>Status</th>
<th>Number of Active Clients</th>
<th>Max Associated Clients</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>200</td>
<td>Enabled</td>
<td>1</td>
<td>2000</td>
<td>WebAuth: Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Webauth Parameter Map: global</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Webauth Authentication List: LWA-AUTHENTICATION</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Webauth Authorization List: LWA-AUTHENTICATION</td>
</tr>
</tbody>
</table>

To view the guest-LAN configuration by ID, use the following command:

Device# show guest-lan id 1

Guest-LAN Profile Name : open

<table>
<thead>
<tr>
<th>Guest-LAN ID</th>
<th>Wired-Vlan</th>
<th>Status</th>
<th>Number of Active Clients</th>
<th>Max Associated Clients</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>200</td>
<td>Enabled</td>
<td>1</td>
<td>2000</td>
<td>WebAuth: Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Webauth Parameter Map: global</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Webauth Authentication List: LWA-AUTHENTICATION</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Webauth Authorization List: LWA-AUTHENTICATION</td>
</tr>
</tbody>
</table>

To view the guest-LAN configuration by profile name, use the following command:

Device# show guest-lan name open

Guest-LAN Profile Name : open

<table>
<thead>
<tr>
<th>Guest-LAN ID</th>
<th>Wired-Vlan</th>
<th>Status</th>
<th>Number of Active Clients</th>
<th>Max Associated Clients</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>200</td>
<td>Enabled</td>
<td>1</td>
<td>2000</td>
<td>WebAuth: Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Webauth Parameter Map: global</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Webauth Authentication List: LWA-AUTHENTICATION</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Webauth Authorization List: LWA-AUTHENTICATION</td>
</tr>
</tbody>
</table>
Verifying Wired Guest Configurations

Webauth Authentication List : LWA-AUTHENTICATION
Webauth Authorization List : LWA-AUTHENTICATION

To view the guest-LAN map summary, use the following command:

Device# show wireless guest-lan-map summary

Number of Guest-Lan Maps: 2

<table>
<thead>
<tr>
<th>WLAN Profile Name</th>
<th>Policy Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>open_wired_guest</td>
<td>open_wired_guest</td>
</tr>
<tr>
<td>lwa_wired_guest</td>
<td>lwa_wired_guest</td>
</tr>
</tbody>
</table>

To view the active clients, use the following command:

Device# show wireless client summary

Number of Local Clients: 1

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>AP Name</th>
<th>Protocol</th>
<th>Method</th>
<th>Role</th>
<th>Type ID</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>000a.bd15.0001</td>
<td>N/A</td>
<td>802.3</td>
<td>Web Auth</td>
<td>Export Foreign</td>
<td>GLAN 1</td>
<td>Run</td>
</tr>
</tbody>
</table>

To view the detailed information about a client by MAC address, use the following command:

Device# show wireless client mac-address 3383.0000.0001 detail

Client MAC Address : 3383.0000.0001
Client IPv4 Address : 155.165.152.151
Client Username: N/A
AP MAC Address: N/A
AP slot : N/A
Client State : Associated
Policy Profile : guestlan_lwa
Flex Profile : N/A

Guest Lan:
  GLAN Id: 2
  GLAN Name: guestlan_lwa
  Wired VLAN: 312

Wireless LAN Network Name (SSID) : N/A
BSSID : N/A
Connected For : 128 seconds
Protocol : 802.3
Channel : N/A
Client IIF-ID : 0xa0000002
Association Id : 0
Authentication Algorithm : Open System
Session Timeout : 1800 sec (Timer not running)
Session Warning Time : Timer not running
Input Policy Name : clsilver
Input Policy State : Installed
Input Policy Source : AAA Policy
Output Policy Name : None
Output Policy State : None
Output Policy Source : None
WMM Support : Disabled
Fastlane Support : Disabled
Power Save : OFF
AAA QoS Rate Limit Parameters:
QoS Average Data Rate Upstream : 0 (kbps)
QoS Realtime Average Data Rate Upstream : 0 (kbps)
QoS Burst Data Rate Upstream : 0 (kbps)
QoS Realtime Burst Data Rate Upstream : 0 (kbps)
QoS Average Data Rate Downstream : 0 (kbps)
QoS Realtime Average Data Rate Downstream : 0 (kbps)
QoS Burst Data Rate Downstream : 0 (kbps)
QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:
Anchor IP Address : 101.0.0.1
Point of Attachment : 0x00000008
Point of Presence : 0xA0000001
AuthC status : Enabled
Move Count : 0
Mobility Role : Export Foreign
Mobility Roam Type : L3 Requested
Mobility Complete Timestamp : 05/07/2019 22:31:45 UTC

Client Join Time:
Join Time Of Client : 05/07/2019 22:31:42 UTC

Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 125 seconds
Policy Type : N/A
Encryption Cipher : N/A
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : default
Multicast VLAN : 0
Access VLAN : 153
Anchor VLAN : 155
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No

Session Manager:
Point of Attachment : TenGigabitEthernet0/0/0
IIF ID : 0x00000008
Authorized : TRUE
Session timeout : 1800
Common Session ID: 00000000000000CB946C8BA3
Acct Session ID : 0x00000000
Last Tried Aaa Server Details:

Server IP : 

Auth Method Status List
Method : Web Auth
Webauth State : Authz
Webauth Method : Webauth

Local Policies:
Service Template : wlan_svc_guestlan_lwa_local (priority 254)
VLAN : 153
Absolute-Timer : 1800

Server Policies:
QOS Level : 0

Resultant Policies:
VLAN Name : VLAN0153
QOS Level : 0
VLAN : 153
Absolute-Timer : 1800

DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
CF Pollable : Not implemented
CF Poll Request : Not implemented
### Wired Guest Access—Use Cases

This feature while performing as a guest access feature can be used to meet different requirements. Some of the possibilities are shared here.

**Scenario One—Equipment Software Update**

This feature can be configured to allow the wired port to connect to the manufacture or vendor website for equipment maintenance, software, or firmware updates.

**Scenario Two—Video Streaming**

This feature can be configured to allow devices that are connected to a wired port to stream video to visitor information screens.
802.11r BSS Fast Transition

- Information About 802.11r Fast Transition, on page 1193
- Restrictions for 802.11r Fast Transition, on page 1194
- Verifying 802.11r Fast Transition (CLI), on page 1195
- Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI), on page 1196
- Configuring 802.11r Fast Transition in an Open WLAN (GUI), on page 1197
- Configuring 802.11r Fast Transition in an Open WLAN (CLI), on page 1198
- Configuring 802.11r Fast Transition on a PSK Security–Enabled WLAN (CLI), on page 1199
- Disabling 802.11r Fast Transition (GUI), on page 1200
- Disabling 802.11r Fast Transition (CLI), on page 1200

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.
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.

• This feature is only supported on open and WPA2-configured WLANs.

• Legacy clients cannot associate with a WLAN that has 802.11r enabled if the driver of the supplicant that is responsible for parsing the Robust Security Network Information Exchange (RSN IE) is old and not aware of the additional AKM suites in the IE. Due to this limitation, clients cannot send association requests to WLANs. These clients, however, can still associate with non-802.11r WLANs. Clients that are 802.11r-capable can associate as 802.11i clients on WLANs that have both 802.11i and 802.11r Authentication Key Management Suites enabled.

The workaround is to enable or upgrade the driver of the legacy clients to work with the new 802.11r AKMs, after which the legacy clients can successfully associate with 802.11r-enabled WLANs.

Another workaround is to have two SSIDs with the same name, but with different security settings (FT and non-FT).

• Fast Transition resource–request protocol is not supported because clients do not support this protocol. Also, the resource–request protocol is an optional protocol.

• To avoid any Denial of Service (DoS) attack, each Cisco WLC allows a maximum of three Fast Transition handshakes with different APs.

• Non-802.11r–capable devices will not be able to associate with FT-enabled WLAN.

• 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:

```plaintext
wlan local-dot1x 24 local-dot1x
no security ft over-the-ds
no security ft adaptive
security dot1x authentication-list spwifi_dot1x
no shutdown
```

### Verifying 802.11r Fast Transition (CLI)

The following command can be used to verify 802.11r Fast Transition:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wlan name wlan-name</td>
<td>Displays a summary of the configured parameters on the WLAN.</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless client mac-address mac-address</code></td>
<td>Displays the summary of the 802.11r authentication key management configuration on a client.</td>
</tr>
</tbody>
</table>

### 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 Failed 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  - `configure terminal`
  **Example:**
  
  Device# configure terminal
| Enters global configuration mode. |
| **Step 2**
  - `wlan profile-name`
  **Example:**
  
  Device# wlan test4
<p>| Enters WLAN configuration submode. The <code>profile-name</code> is the profile name of the configured WLAN. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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 (GUI)

**Procedure**

1. **Step 1**  
Choose Configuration > Tags & Profiles > WLANs.
2. **Step 2**  
Click Add to create WLANs.  
The Add WLAN page is displayed.
3. **Step 3**  
In the Security > Layer2 tab, choose the appropriate status for **Fast Transition** between APs.
4. **Step 4**  
Click Save & Apply to Device.
### Configuring 802.11r Fast Transition in an Open WLAN (CLI)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code>  &lt;br&gt; <strong>Example:</strong>  &lt;br&gt; Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>wlan profile-name</code>  &lt;br&gt; <strong>Example:</strong>  &lt;br&gt; Device# wlan test4</td>
<td>Enters WLAN configuration submode. The <code>profile-name</code> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>client vlan vlan-id</code>  &lt;br&gt; <strong>Example:</strong>  &lt;br&gt; Device(config-wlan)# client vlan 0120</td>
<td>Associates the client VLAN to the WLAN.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>no security wpa</code>  &lt;br&gt; <strong>Example:</strong>  &lt;br&gt; Device(config-wlan)# no security wpa</td>
<td>Disables WPA security.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>no security wpa akm dot1x</code>  &lt;br&gt; <strong>Example:</strong>  &lt;br&gt; Device(config-wlan)# no security wpa akm dot1x</td>
<td>Disables security AKM for dot1x.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>no security wpa wpa2</code>  &lt;br&gt; <strong>Example:</strong>  &lt;br&gt; Device(config-wlan)# no security wpa wpa2</td>
<td>Disables WPA2 security.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>no wpa wpa2 ciphers aes</code>  &lt;br&gt; <strong>Example:</strong>  &lt;br&gt; Device(config-wlan)# no security wpa wpa2 ciphers aes</td>
<td>Disables WPA2 ciphers for AES.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>security ft</code>  &lt;br&gt; <strong>Example:</strong>  &lt;br&gt; Device(config-wlan)# security ft</td>
<td>Specifies the 802.11r Fast Transition parameters.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>no shutdown</code>  &lt;br&gt; <strong>Example:</strong>  &lt;br&gt; Device(config-wlan)# shutdown</td>
<td>Shuts down the WLAN.</td>
</tr>
</tbody>
</table>
### Configuring 802.11r Fast Transition on a PSK Security–Enabled WLAN (CLI)

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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. |
Disabling 802.11r Fast Transition (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose <strong>Configuration &gt; Tags &amp; Profiles &gt; WLANs.</strong></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>On the <strong>WLANs</strong> page, click the WLAN name.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>In the <strong>Edit WLAN</strong> window, click the <strong>Security &gt; Layer2</strong> tab.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>From the <strong>Fast Transition</strong> drop-down list, choose <strong>Disabled</strong></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Click <strong>Update &amp; Apply to Device.</strong></td>
<td></td>
</tr>
</tbody>
</table>

Disabling 802.11r Fast Transition (CLI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td><strong>wlan profile-name</strong></td>
<td>Enters WLAN configuration submode. The <code>profile-name</code> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td>3</td>
<td>**no security ft [over-the-ds</td>
<td>Disables 802.11r Fast Transition on the WLAN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>reassociation-timeout timeout-in-seconds]**</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong>&lt;br&gt;end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Device(config)# end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Disabling 802.11r Fast Transition (CLI)
The 802.11 Wi-Fi standard minimizes the chance of multiple devices interfering with one another by transmitting at the same time. This carrier-sense multiple access with collision avoidance (CSMA/CA) technology was based on static thresholds that allowed Wi-Fi devices to avoid interfering with each other on air. However, with increased density and number of Wi-Fi devices, these static thresholds often lead to CSMA/CA causing devices to defer transmissions unnecessarily.

For example, if two devices associated with different BSSs can hear each transmissions from each other at relatively low signal strengths, each device has to defer its transmission when it receives a transmission from the other. But if both devices were to transmit at the same time, it is likely that neither would cause enough interference at the other BSS's receiver to cause reception failure for either transmission.

Devices today must demodulate packets to look at the MAC header in order to determine whether or not a received packet belongs to their own BSS. This process consumes power, which could have been saved if devices could quickly identify the BSS by looking at the PHY header alone, and subsequently drop packets that are from a different BSS. Prior to Wi-Fi 6, there was no provision for devices to do this.

The new 802.11ax (Wi-Fi 6) standard addresses both of the issues discussed above, through the new BSS Coloring and Spatial Reuse mechanisms. BSS Coloring is a new provision that allows devices operating in the same frequency space to quickly distinguish between packets from their own BSS and packets from an Overlapping BSS (OBSS), by simply looking at the "BSS color" value contained in the HE PHY header. Spatial Reuse allows devices, in certain cases, to transmit at the same time as OBSS packets they receive, instead of having to defer transmissions due to legacy interference thresholds. Since every Wi-Fi 6 device understands the BSS color, it can be leveraged to increase power savings by dropping packets earlier, and to identify spatial reuse opportunities.

- BSS Coloring, on page 1204
- Configuring BSS Color on AP (GUI), on page 1204
- Configuring BSS Color in the Privileged EXEC Mode, on page 1205
- Configuring BSS Color Globally (GUI), on page 1205
- Configuring BSS Color in the Configuration Mode, on page 1205
- Verifying BSS Color, on page 1206
BSS Coloring

BSS (Basic Service Set) Coloring is a method to differentiate between BSSs of access points and their clients on the same RF channel. Wi-Fi 6 enables each AP radio to assign a value (from 1 to 63), known as the BSS color, to be included in the PHY header of all HE transmissions from devices in its BSS. With devices of each BSS transmitting a locally-unique color, a device can quickly and easily distinguish transmissions coming from its BSS from those of a neighboring BSS.

The following platforms support this feature:
• Cisco Catalyst 9800 Series Wireless Controllers
• Cisco Catalyst 9115 Access Points
• Cisco Catalyst 9120 Access Points

Configuring BSS Color on AP (GUI)

Procedure

Step 1  Choose Configuration > Wireless > Access Points.
Step 2  Click the 5 GHz Radios section or the 2.4 GHz Radios section. The list of the AP radios in the band is displayed.
Step 3  Click the required AP name. The Edit Radios window is displayed.
Step 4  From the Edit Radios window, select the Configure tab. The general information, Antenna Parameters, RF Channel Assignment, Tx Power Level Assignment, and BSS Color are displayed.
Step 5  In the BSS Color area and from the BSS Color Configuration drop-down list, choose Custom configuration
   • Custom: To manually select the BSS color configuration for the AP radio.
     a. Click the BSS Color Status field to disable or enable the feature.
     b. In the Current BSS Color field, specify a corresponding BSS color for the AP radio. The valid range is between 1 and 63.
Step 6  Click Update & Apply to Device.
# Configuring BSS Color in the Privileged EXEC Mode

## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;enable&lt;br&gt;Example: Device&gt; enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;ap name ap-name dot11 {24ghz</td>
<td>5ghz</td>
</tr>
</tbody>
</table>

## Configuring BSS Color Globally (GUI)

### Procedure

1. Choose **Configuration > Radio Configurations > Parameters**.
2. In the **11ax Parameters** section, enable BSS color globally for the 5 GHz and 2.4 GHz radios by checking the **BSS Color** check box

## Configuring BSS Color in the Configuration Mode

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;enable&lt;br&gt;Example: Device&gt; enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
</tbody>
</table>
Verifying BSS Color

To verify if the global per-band BSS color is enabled, use the following show command:

```
Device# show ap dot11 24ghz network
802.11b Network : Enabled
11gSupport : Enabled
11nSupport : Enabled
802.11ax : Enabled
DynamicFrag : Enabled
MultiBssid : Enabled
BSS Color : Enabled
802.11ax MCS Settings:
  MCS 7, Spatial Streams = 1 : Supported
```

To view the BSS color configuration of all the AP radios on the band in the summary list along with Channel, TX Power and so on, use the following show command:

```
Device# show ap dot11 24ghz summary extended
AP Name       Mac Address  Slot Admin State Oper State Width
Txpw   Channel  BSS Color
Ed2-JFW-AP1  84b2.61ba.4730 1  Enabled   Up  40
1/6 (17 dBm) (136,132)*
11AX-9120-AP1 d4ad.bda2.3fc0 1  Enabled   Up  20
1/8 (23 dBm) (36)
Ed2-JFW-AP2  f8c2.8885.59f0 1  Enabled   Up  20
1/5 (15 dBm) (40)
```

To view the BSS color configuration and the capability of the AP radio, use the following show commands:

```
Device# show ap name AP7069.5A74.816C config dot11 24ghz
Cisco AP Identifier : 502f.a876.1e60
Cisco AP Name : AP7069.5A74.816C
Attributes for Slot 0
  Radio Type : 802.11b
  Radio Mode : REAP
  Radio Role : Auto
  Radio SubType :
```
Administrative State : Enabled
Operation State : Up

Phy OFDM Parameters
Configuration : Automatic
Current Channel : 6
Channel Width : 20 MHz
TI Threshold : 1157693440
Antenna Type : External
External Antenna Gain (in .5 dBi units) : 8

!BSS color details are displayed below:
802.11ax Parameters
HE Capable : Yes
BSS Color Capable : Yes
BSS Color Configuration : Customized
Current BSS Color : 34

Device# show ap name AP7069.5A74.816C config slot 0
Cisco AP Identifier : 502f.a876.1e60
Cisco AP Name : AP7069.5A74.816C
Country Code : US
AP Country Code : US - United States
AP Regulatory Domain : -A
MAC Address : 7069.5a74.816c
IP Address Configuration : DHCP
IP Address : Disabled

Attributes for Slot 0
Radio Type : 802.11n - 2.4 GHz
Radio Role : Auto
Radio Mode : REAP
Radio SubType : Main
Administrative State : Enabled

Phy OFDM Parameters
Configuration : Automatic
Current Channel : 6
Channel Assigned By : DCA
Extension Channel : NONE
Channel Width : 20
Allowed Channel List : 1,2,3,4,5,6,7,8,9,10,11
TI Threshold : 1157693440
DCA Channel List :
Antenna Type : EXTERNAL_ANTENNA
External Antenna Gain (in .5 dBi units) : 8
Diversity : DIVERSITY_ENABLED
802.11n Antennas
   A : ENABLED
   B : ENABLED
   C : ENABLED
   D : ENABLED

!BSS color details are displayed below:
802.11ax Parameters
Verifying BSS Color

<table>
<thead>
<tr>
<th>HE Capable</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSS Color Capable</td>
<td>Yes</td>
</tr>
<tr>
<td>BSS Color Configuration</td>
<td>Customized</td>
</tr>
<tr>
<td>Current BSS Color</td>
<td>34</td>
</tr>
</tbody>
</table>
Assisted Roaming

The 802.11k standard allows clients to request neighbor reports containing information about known neighbor access points that are candidates for a service set transition. The use of the 802.11k neighbor list can limit the need for active and passive scanning.

The assisted roaming feature is based on an intelligent and client optimized neighbor list.

Unlike the Cisco Client Extension (CCX) neighbor list, the 802.11k neighbor list is generated dynamically on-demand and is not maintained on the device. The 802.11k neighbor list is based on the location of the clients without requiring the mobility services engine (MSE). Two clients on the same device but different APs can have different neighbor lists delivered depending on their individual relationship with the surrounding APs.

By default, the neighbor list contains only neighbors in the same band with which the client is associated. However, a switch exists that allows 802.11k to return neighbors in both bands.

Clients send requests for neighbor lists only after associating with the APs that advertise the RRM (Radio Resource Management) capability information element (IE) in the beacon. The neighbor list includes information about BSSID, channel, and operation details of the neighboring radios.

Assembling and Optimizing the Neighbor List

When the device receives a request for an 802.11k neighbor list, the following occurs:

1. The device searches the RRM neighbor table for a list of neighbors on the same band as the AP with which the client is currently associated with.

2. The device checks the neighbors according to the RSSI (Received Signal Strength Indication) between the APs, the current location of the present AP, the floor information of the neighboring AP from Cisco Prime Infrastructure, and roaming history information on the device to reduce the list of neighbors to six per band. The list is optimized for APs on the same floor.
Assisted Roaming for Non-802.11k Clients

It is also possible to optimize roaming for non-802.11k clients. You can generate a prediction neighbor list for each client without the client requiring to send an 802.11k neighbor list request. When this is enabled on a WLAN, after each successful client association/reassociation, the same neighbor list optimization is applied on the non-802.11k client to generate the neighbor list and store the list in the mobile station software data structure. Clients at different locations have different lists because the client probes are seen with different RSSI values by different neighbors. Because clients usually probe before any association or reassociation, this list is constructed with the most updated probe data and predicts the next AP that the client is likely to roam to.

We discourage clients from roaming to those less desirable neighbors by denying association if the association request to an AP does not match the entries on the stored prediction neighbor list.

Similar to aggressive load balancing, there is a switch to turn on the assisted roaming feature both on a per-WLAN basis and globally. The following options are available:

- Denial count—Maximum number of times a client is refused association.
- Prediction threshold—Minimum number of entries required in the prediction list for the assisted roaming feature to be activated.

Because both load balancing and assisted roaming are designed to influence the AP that a client associates with, it is not possible to enable both the options at the same time on a WLAN.

This section contains the following subsections:

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)

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 > Optimized Roam.
Step 2 On the 5 GHz Band or 2.4 GHz Band page, select the Optimized Roaming Mode check box.
Step 3  In the Optimized Roaming Data Rate Threshold field, enter a value for the threshold data rate of the client. The following data rates are available:

- 802.11a—6, 9, 12, 18, 24, 36, 48, and 54.
- 802.11b—1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, and 54.

Optimized roaming disassociates clients based on the RSSI of the client data packet and data rate. The client is disassociated if the current data rate of the client is lower than the Optimized Roaming Data Rate Threshold.

Step 4  Click Apply.

---

Configuring Assisted Roaming (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wireless assisted-roaming floor-bias dBm</code></td>
<td>Configures neighbor floor label bias. The valid range is from 5 to 25 dBm, and the default value is 15 dBm.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# wireless assisted-roaming floor-bias 20</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>wlan wlan-id</code></td>
<td>Enters the WLAN configuration submode. The <code>wlan-name</code> is the profile name of the configured WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# wlan wlan1</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>assisted-roaming neighbor-list</code></td>
<td>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 <code>no</code> form of the command disables assisted roaming neighbor list.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(wlan)# assisted-roaming neighbor-list</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>assisted-roaming dual-list</code></td>
<td>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 <code>no</code> form of the command disables assisted roaming dual list.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(wlan)# assisted-roaming dual-list</code></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

1. **assisted-roaming prediction**
   - **Example:**
     
     ```
     Device(wlan)# assisted-roaming prediction
     ```

2. **wireless assisted-roaming prediction-minimum count**
   - **Example:**
     
     ```
     Device# wireless assisted-roaming prediction-minimum
     ```

3. **wireless assisted-roaming denial-maximum count**
   - **Example:**
     
     ```
     Device# wireless assisted-roaming denial-maximum 8
     ```

4. **end**
   - **Example:**
     
     ```
     Device(config)# end
     ```

### Step 6

**Purpose**

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

**Purpose**

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.

### Step 8

**Purpose**

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

**Purpose**

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wlan id wlan-id</td>
<td>Displays the WLAN parameters on the WLAN.</td>
</tr>
</tbody>
</table>

### 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
**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 Transition 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.
802.11v BSS Transition 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Tags &amp; Profiles &gt; WLANs.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Add to create WLANs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Add WLAN page is displayed.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Advanced tab and 11v BSS Transition Support section, select the BSS Transition check box to enable BSS transition per WLAN.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the Disassociation Imminent value. The valid range is from 0 to 3000 TBTT.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save &amp; Apply to Device.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring 802.11v BSS Transition Management (CLI)

802.11v BSS Transition is applied in the following three scenarios:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wlan profile-name</td>
<td>Configures WLAN profile and enters the WLAN profile configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wlan test-wlan</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>shut</td>
<td>Shutdown the WLAN profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# shut</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>bss-transition</td>
<td>Configure BSS transition per WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# bss-transition</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>5</td>
<td>bss-transition disassociation-imminent</td>
<td>Configure BSS transition disassociation Imminent per WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# bss-transition disassociation-imminent</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>no shutdown</td>
<td>Enables the WLAN profile.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# no shutdown</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>end</td>
<td>Return to privilege EXEC mode. Alternatively, you can press CTRL + Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# end</td>
<td></td>
</tr>
</tbody>
</table>
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 35: IGTK Exchange in 4-way Handshake*

![Diagram of 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 36: 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 37: 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
The 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 38: 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.

- To configure 802.11w as mandatory, you must enable SHA256 related AKM in addition to WPA AKM.

### 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.
How to Configure 802.11w

Configuring 802.11w (GUI)

Before you begin
WPA and AKM must be configured.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Tags &amp; Profiles &gt; WLANs.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Add to create WLANs.</td>
</tr>
<tr>
<td></td>
<td>The Add WLAN page is displayed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Security &gt; Layer2 tab, navigate to the Protected Management Frame section.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose PMF as Disabled, Optional, or Required. By default, the PMF is disabled.</td>
</tr>
<tr>
<td></td>
<td>If you choose PMF as Optional or Required, you get to view the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Association Comeback Timer—Enter a value between 1 and 10 seconds to configure 802.11w association comeback time.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save &amp; Apply to Device.</td>
</tr>
</tbody>
</table>

Configuring 802.11w (CLI)

Before you begin
WPA and AKM must be configured.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>wlan profile-name wlan-id ssid</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# wlan wlan-test 12 alpha</td>
</tr>
</tbody>
</table>
### Disabling 802.11w

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>wlan profile-name wlan-id ssid</td>
<td>Configures a WLAN and enters configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# wlan wlan-test 12 alpha</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>no security wpa akm dot1x-sha256</td>
<td>Disables 802.1x support.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wlan)# no security wpa akm dot1x-sha256</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>no security pmf association-comeback comeback-interval</td>
<td>Disables the 802.11w association callback time.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wlan)# no security pmf association-comeback 10</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td><code>no security pmf mandatory</code></td>
<td>Disables client negotiation of 802.11w PMF protection on a WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-wlan)# no security pmf mandatory</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>no security pmf saquery-retry-time timeout</code></td>
<td>Disables SQ query retry.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-wlan)# no security pmf saquery-retry-time 100</code></td>
<td></td>
</tr>
</tbody>
</table>

### 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
  ONE : 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 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

WLAN Monitoring 802.11w
Management Frame Protection

Information About Management Frame Protection

Management Frame Protection (MFP) provides security for the management messages passed between access points and clients. MFP provides both infrastructure and client support.

- **Infrastructure MFP**—Protects management frames by detecting adversaries that are invoking denial-of-service attacks, flooding the network with associations and probes, interjecting as rogue access points, and affecting network performance by attacking the QoS and radio measurement frames. Infrastructure MFP is a global setting that provides a quick and effective means to detect and report phishing incidents.

Specifically, infrastructure MFP protects 802.11 session management functions by adding message integrity check information elements (MIC IEs) to the management frames emitted by access points (and not those emitted by clients), which are then validated by other access points in the network. Infrastructure MFP is passive. It can detect and report intrusions but has no means to stop them.

Infrastructure MFP consists of three main components:

- **Management frame protection**—The access point protects the management frames it transmits by adding a MIC IE to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving access point configured to detect MFP frames to report the discrepancy. MFP is supported for use with Cisco Aironet lightweight access points.

- **Management frame validation**—In infrastructure MFP, the access point validates every management frame that it receives from other access points in the network. It ensures that the MIC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE from a BSSID belonging to an access point that is configured to transmit MFP frames, it reports the discrepancy to the network management system. In order for the timestamps to operate properly, all controllers must be Network Time Protocol (NTP) synchronized.

- **Event reporting**—The access point notifies the controller when it detects an anomaly, and the controller aggregates the received anomaly events and can report the results through SNMP traps to the network management system.
Infrastructure MFP is disabled by default and can be enabled globally. When you upgrade from a previous software release, infrastructure MFP is disabled globally if access point authentication is enabled because the two features are mutually exclusive.

- Client MFP—Shields authenticated clients from spoofed frames, preventing many of the common attacks against wireless LANs from becoming effective. Most attacks, such as deauthentication attacks, revert to simply degrading performance by contending with valid clients.

Specifically, client MFP encrypts management frames sent between access points and CCXv5 clients so that both the access points and clients can take preventative action by dropping spoofed class 3 management frames (that is, management frames passed between an access point and a client that is authenticated and associated). Client MFP leverages the security mechanisms defined by IEEE 802.11i to protect the following types of class 3 unicast management frames: disassociation, deauthentication, and QoS (WMM) action. Client MFP protects a client-access point session from the most common type of denial-of-service attack. It protects class 3 management frames by using the same encryption method used for the session’s data frames. If a frame received by the access point or client fails decryption, it is dropped, and the event is reported to the controller.

**Supported Access Point Models**

Cisco MFP is supported on the following AP models:

- Cisco Aironet 2802, 3802, and 4802 series access points
- Cisco Aironet 2800, 3800, 4800, and 1560 series access points
- All Cisco IOS access points

**Unsupported Access Point Models**

Cisco MFP is not supported on the following AP models:

- Cisco Aironet 1800 series access points
- Cisco 802.11ax access points

**Restrictions for Management Frame Protection**

- Lightweight access points support infrastructure MFP in local and monitor modes and in FlexConnect mode when the access point is connected to a controller. They support client MFP in local, FlexConnect, and bridge modes.
- Client MFP is supported for use only with CCXv5 clients using WPA2 with TKIP or AES-CCMP.
- 802.11ax access points do not support MFP.
- Non-CCXv5 clients may associate to a WLAN, if client MFP is disabled or optional.
- Error reports generated on a FlexConnect access point in standalone mode cannot be forwarded to the controller and are dropped.
- Keys are generated using random number generator but you can improve the keys by changing to SHA.
- MFP key for each BSSID is not supported.
Configuring Management Frame Protection (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless wps mfp</td>
<td>Configures a management frame protection.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless wps mfp</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>wireless wps mfp {ap-impersonation</td>
<td>key-refresh-interval}</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless wps mfp</td>
<td>MFP key refresh interval in hours.</td>
</tr>
<tr>
<td></td>
<td>ap-impersonation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless wps mfp</td>
<td>key-refresh-interval—Refers to the MFP key refresh interval in hours.</td>
</tr>
<tr>
<td></td>
<td>key-refresh-interval</td>
<td>The valid range is from 1 to 24. Default value is 24.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Saves the configuration and exits configuration mode and returns to</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Verifying Management Frame Protection Settings

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
```

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.1.x
Verifying Management Frame Protection Settings

AP Impersonation detection : Disabled
Key refresh interval : 15

To view the MFP statistics details, use the following command:

Device# show wireless wps mfp statistics

<table>
<thead>
<tr>
<th>BSSID</th>
<th>Radio Detector</th>
<th>AP</th>
<th>LastSourceAddr</th>
<th>Error</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>aabb.ccdd.eeff</td>
<td>a</td>
<td>AP3800</td>
<td>aabb.ccdd.eeff</td>
<td>Invalid MIC</td>
<td>10</td>
</tr>
<tr>
<td>Beacon, Probe Response</td>
<td></td>
<td>beacon, probe response</td>
<td>beacon, probe response</td>
<td>beacon, probe response</td>
<td>beacon, probe response</td>
</tr>
</tbody>
</table>

To verify if access points support MFP validation and protection, use the following command:

Device# show wireless wps mfp ap summary

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Radio MAC</th>
<th>Validation</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP002A.1087.CBF4</td>
<td>00a2.eefd.bdc0</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>AP58AC.78DE.9946</td>
<td>00a2.eeb8.4ae0</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>APb4de.3196.caac</td>
<td>4c77.6d83.6b90</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Deny Wireless Client Session Establishment Using Calendar Profiles

- Information About Denial of Wireless Client Session Establishment, on page 1231
- Configuring Daily Calendar Profile, on page 1232
- Configuring Weekly Calendar Profile, on page 1233
- Configuring Monthly Calendar Profile, on page 1234
- Mapping a Daily Calendar Profile to a Policy Profile, on page 1235
- Mapping a Weekly Calendar Profile to a Policy Profile, on page 1236
- Mapping a Monthly Calendar Profile to a Policy Profile, on page 1237
- Verifying Calendar Profile Configuration, on page 1238
- Verifying Policy Profile Configuration, on page 1238

Information About Denial of Wireless Client Session Establishment

Denial of client session establishment feature allows the controller to stop client session establishment based on a particular time. This helps control the network in efficient and controlled manner without any manual intervention.

In Cisco Catalyst 9800 Series Wireless Controller, you can deny the wireless client session based on the following recurrences:

- Daily
- Weekly
- Monthly

The Calendar Profiles created are then mapped to the policy profile. By attaching the calendar profile to a policy profile, you will be able to create different recurrences for the policy profile using different policy tag.
You need to create separate Calendar Profile for Daily, Weekly, and Monthly sub-categories.

The following is the workflow for denial of wireless client session establishment feature:

- Create a calendar profile.
- Apply the calendar profile to a policy profile.

Note

A maximum of 100 calendar profile configuration and 5 calendar profile association to policy profile is supported.

Points to Remember

If you boot up your controller, the denial of client session establishment feature kicks in after a minute from the system boot up.

If you change the system time after the calendar profile is associated to a policy profile, you can expect a maximum of 30 second delay to adapt to the new clock timings.

Note

You cannot use the `no action deny-client` command to disable action while associating the calendar profile to a policy profile.

If you want to disable the action command, you need to disassociate the calendar profile from the policy profile, and re-configure again.

### Configuring Daily Calendar Profile

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wireless profile calendar-profile name name</code></td>
<td>Configures a calendar profile.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wireless profile calendar-profile name</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>calendar-profile name daily_calendar_profile</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>start start_time end end_time</code></td>
<td>Configures start and end time for the calendar profile.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Weekly Calendar Profile

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless profile calender-profile name <em>name</em></td>
<td>Configures a calendar profile.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wireless profile calender-profile name weekly_calendar_profile</td>
<td>Here, <em>name</em> refers to the name of the calendar profile.</td>
</tr>
<tr>
<td><strong>Step 3</strong> start <em>start_time</em> end <em>end_time</em></td>
<td>Configures start and end time for the calendar profile.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-calendar-profile)# start 18:00:00 end 19:00:00</td>
<td>Here, <em>start_time</em> is the start time for the calendar profile. You need to enter start time in HH:MM:SS format. <strong>end_time</strong> is the end time for the calendar profile. You need to enter end time in HH:MM:SS format.</td>
</tr>
</tbody>
</table>

---

**Purpose**

- **Purpose**
  - Here,
  - *start_time* is the start time for the calendar profile. You need to enter start time in **HH:MM:SS** format.
  - *end_time* is the end time for the calendar profile. You need to enter end time in **HH:MM:SS** format.

**Step 4** recurrance daily

**Example:**

Device(config-calendar-profile)# recurrance daily

Configures daily recurrences for a calendar profile.

**Step 5** end

**Example:**

Device(config-calendar-profile)# end

Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
### Configuring Monthly Calendar Profile

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>wireless profile calender-profile name name</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless profile calender-profile name monthly_calendar_profile</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>start start_time end end_time</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-calender-profile)# start 18:00:00 end 19:00:00</td>
</tr>
</tbody>
</table>

**Purpose**

- Enters global configuration mode.
- Configures a calendar profile.
- Configures start and end time for the calendar profile.

**Note**

Here, `name` refers to the name of the calendar profile. `start_time` and `end_time` are needed in `HH:MM:SS` format.
### Mapping a Daily Calendar Profile to a Policy Profile

#### Procedure

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

**Example:**

```
Device# configure terminal
```

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>wireless profile policy profile-name</td>
<td>Creates policy profile for the WLAN. The <em>profile-name</em> is the profile name of the policy profile.</td>
</tr>
</tbody>
</table>

**Example:**

```
Device(config)# wireless profile policy default-policy-profile
```

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>calendar-profile name calendar-profile-name</td>
<td>Maps a calendar profile to a policy profile. The <em>calendar-profile-name</em> is the name of the calendar profile name created in <strong>Configuring Daily Calendar Profile</strong>, on page 1232.</td>
</tr>
</tbody>
</table>

**Example:**

```
Device(config-wireless-policy)# calendar-profile name daily_calendar_profile
```

**Note**

You need to disable Policy Profile before associating a calendar profile to a policy profile. The following needs to be done:

```
Device(config-wireless-policy)# shutdown
```
### Mapping a Weekly Calendar Profile to a Policy Profile

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wireless profile policy profile-name</td>
<td>Creates policy profile for the WLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless profile policy default-policy-profile</td>
<td>The profile-name is the profile name of the policy profile.</td>
</tr>
<tr>
<td>Step 3</td>
<td>calendar-profile name calendar-profile-name</td>
<td>Maps a calendar profile to a policy profile.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-policy)# calendar-profile name weekly_calendar_profile</td>
<td>The calendar-profile-name is the name of the calendar profile name created in Configuring Weekly Calendar Profile, on page 1233.</td>
</tr>
<tr>
<td>Note</td>
<td>You need to disable Policy Profile before associating a calendar profile to a policy profile. The following needs to be done:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-policy)# shutdown</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>action deny-client</td>
<td>Configures deny client session establishment during calendar profile interval.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

**Device(config-policy-profile-calender)#**

- **action deny-client**

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong> Client associations are denied daily between timeslot 9:00:00 to 17:00:00. For start and end time details, see Configuring Weekly Calendar Profile, on page 1233.</td>
</tr>
</tbody>
</table>

- On Monday and Tuesday, clients are denied between 17:30:00 and 19:00:00 besides regular time 9:00:00 to 17:00:00.

- On 25th of every month, clients are denied between 18:00:00 and 19:00:00 besides regular time 9:00:00 to 17:00:00.

**Step 5**

- **end**

**Example:**

Device(config-policy-profile-calender)##

- **end**

Returns to privileged EXEC mode.

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

---

## Mapping a Monthly Calendar Profile to a Policy Profile

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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**

- **calendar-profile name** *calendar-profile-name*

**Example:**

Device(config-wireless-policy)#

calendar-profile name monthly_calendar_profile

Maps a calendar profile to a policy profile.

The *calendar-profile-name* is the name of the calendar profile name created in Configuring Monthly Calendar Profile, on page 1234.

| **Step 4**

- **action deny-client**

**Example:**

Configures deny client session establishment for the defined calendar profile interval.
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device(config-policy-profile-calendar)# action deny-client</code></td>
<td>Note: Every day client associations are denied between timeslot 9:00:00 to 17:00:00. For start and end time details, see Configuring Monthly Calendar Profile, on page 1234. On Monday and Tuesday, clients are denied between 17:30:00 and 19:00:00 besides regular time 9:00:00 to 17:00:00. On 25th of every month, clients are denied between 18:00:00 and 19:00:00 besides regular time 9:00:00 to 17:00:00.</td>
</tr>
<tr>
<td><code>Device(config-policy-profile-calendar)# end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>

### Verifying Calendar Profile Configuration

To view the summary of calendar profiles, use the following command:

```
Device# show wireless profile calendar-profile summary
Number of Calendar Profiles: 3
```

<table>
<thead>
<tr>
<th>Profile-Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>monthly_25_profile</td>
</tr>
<tr>
<td>weekly_mon_profile</td>
</tr>
<tr>
<td>daily_calendar_profile</td>
</tr>
</tbody>
</table>

To view the calendar profile details for a specific profile name, use the following command:

```
Device# show wireless profile calendar-profile detailed daily_calendar_profile
Calendar profiles : daily_calendar_profile
Recurrence : DAILY
Start Time : 09:00:00
End Time : 17:00:00
```

### Verifying Policy Profile Configuration

To view the detailed parameters for a specific policy profile, use the following command:

```
Device# show wireless profile policy detailed default-policy-profile
Tunnel Profile
Profile Name : Not Configured
Calendar Profile
```
Profile Name: monthly_25_profile
Wlan Enable: Not Configured
Client Block: Client Block Configured

Profile Name: weekly_mon_profile
Wlan Enable: Not Configured
Client Block: Client Block Configured

Profile Name: daily_calendar_profile
Wlan Enable: Not Configured
Client Block: Client Block Configured

Profile Name: weekly_calendar_profile
Wlan Enable: Not Configured
Client Block: Client Block Configured

Fabric Profile
Profile Name: Not Configured

To view the configured calendar profile information under policy profile, use the following command:

Device# show wireless profile policy all
Tunnel Profile
Profile Name: Not Configured
Calendar Profile
Profile Name: daily_calendar_profile
Wlan Enable: Not Configured
Client Block: Client Block Configured

Profile Name: weekly_calendar_profile
Wlan Enable: Not Configured
Client Block: Client Block Configured

Fabric Profile
Profile Name: Not Configured

Note
The anchor priority is always displayed as local. Priorities can be assigned on the foreign controller.
Verifying Policy Profile Configuration
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 controllers 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 controllers 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 comes 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.
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.

Create a Tunnel Gateway

In the Cisco Catalyst 9800 Series Wireless Controller, a tunnel gateway is modeled as a tunnel interface.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface tunnel tunnel_number</td>
<td>Configures a tunnel interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# interface tunnel 21</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> tunnel source source_intf</td>
<td>Sets the source address of the tunnel interface. The source interface can be VLAN, Gigabit Ethernet or loopback.</td>
</tr>
<tr>
<td>Example: Device(config-if)# tunnel source 22</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> tunnel destination tunnel-address</td>
<td>Sets the destination address of the tunnel.</td>
</tr>
<tr>
<td>Example: Device(config-if)# tunnel destination 10.11.12.13</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> tunnel mode ethernet gre {ipv4</td>
<td>ipv6} p2p</td>
</tr>
<tr>
<td>Example: Device(config-if)# tunnel mode ethernet gre ipv4 p2p</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the Tunnel Gateway (GUI)

Follow the steps given below to configure the tunnel gateway:
Procedure

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

Step 2  Click the **Gateways** tab. The **Add Gateway** window is displayed.

Step 3  In the **Tunnel Id** field, specify the tunnel ID.

Step 4  In the **Destination address(IPv4/IPv6)** field, specify the IPv4 or IPv6 address.

Step 5  From the **Source Interface** drop-down list, select an interface.

Step 6  In the **AAA Proxy** section, slide the **AAA Proxy** slider to **Enabled**. When **AA Proxy** is enabled, complete the following steps:
   a)  From the **Encryption Type** drop-down list, select either **UNENCrypted** or **AES ENCRYPTION**.
   b)  In the **Key Phrase** field, specify the key phrase.

Step 7  Click **Apply to Device**.

---

**Configuring a Tunnel Domain**

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

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

| **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. |

---

**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._
### Configuring Tunnel Domain (GUI)

Follow the steps given below to configure the tunnel domain:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Configuration &gt; Tags &amp; Profiles &gt; EoGRE</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the <strong>Domains</strong> tab. The <strong>Add Domain</strong> window is displayed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Name</strong> field, specify the domain name.</td>
</tr>
<tr>
<td>Step 4</td>
<td>From the <strong>Primary Tunnel Gateway</strong> drop-down list, choose an option.</td>
</tr>
<tr>
<td>Step 5</td>
<td>From the <strong>Secondary Tunnel Gateway</strong> drop-down list, choose an option.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Slide the <strong>Status</strong> button to <strong>Enabled</strong>, to activate the domain status.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Slide the <strong>Revertive Redundancy</strong> button to <strong>Enabled</strong>, to activate revertive redundancy.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Click <strong>Apply to Device</strong>.</td>
</tr>
</tbody>
</table>

### Configuring EoGRE Global Parameters

**Procedure**

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

**Example:**

```
Device# configure terminal
```
### Configuring EoGRE Global Parameters (GUI)

Follow the steps given below to configure the EoGRE global parameters:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 2 | `tunnel eogre heartbeat interval interval-value` | Sets EoGRE tunnel heartbeat periodic interval.  
**Example:**  
Device(config)# tunnel eogre heartbeat interval 600 |
| Step 3 | `tunnel eogre heartbeat max-skip-count skip-count` | Sets the maximum number of tolerable dropped heartbeats.  
**Example:**  
Device(config)# tunnel eogre heartbeat max-skip-count 7  
**Note**  
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` | Sets the tunnel EoGRE source interface.  
**Example:**  
Device(config)# tunnel eogre source loopback 12 |
| Step 5 | `tunnel eogre interface tunnel tunnel-intf aaa proxy key key key-name` | (Optional) Configures AAA proxy RADIUS key for the AAA proxy setup.  
**Example:**  
Device(config)# tunnel eogre interface tunnel 21 aaa proxy key 0 mykey  
**Note**  
When the tunnel gateway is behaving as the AAA proxy server, only this step is required for the configuration. |

---

**Configuring EoGRE Global Parameters (GUI)**

Follow the steps given below to configure the EoGRE global parameters:

**Procedure**

1. Choose Configuration > Tags & Profiles > EoGRE.  
The EoGRE Global Config tab is displayed.
2. In the Heartbeat Interval (seconds) field, specify an appropriate timer value for heartbeat interval. The valid range is between 60 and 600 seconds.
3. In the Max Heartbeat Skip Count field, specify the maximum heartbeat skip count. The valid range is between 3 and 10.
4. From the Interface Name drop-down list, choose an interface name.
5. Click Apply.
## Configuring a Tunnel Profile

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>wireless profile policy <em>profile-policy-name</em></td>
<td>Configures a WLAN policy profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless profile policy eogre_policy</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>tunnel-profile <em>tunnel-profile-name</em></td>
<td>Creates a tunnel profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# tunnel-profile tunnel1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-wireless-policy)# exit</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>wireless profile tunnel <em>tunnel-profile-name</em></td>
<td>Configures a wireless tunnel profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless profile tunnel wl-tunnel-1</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>dhcp-opt82 enable</td>
<td>Activates DHCP Option 82 for the tunneled clients.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-tunnel-profile)# dhcp-opt82 enable</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>dhcp-opt82 remote-id <em>remote-id</em></td>
<td>Configures Remote ID options.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-tunnel-profile)# dhcp-opt82 remote-id vlan</td>
</tr>
<tr>
<td><strong>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.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>aaa-override</td>
<td>Enables AAA policy override.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-tunnel-profile)# aaa-override</td>
</tr>
</tbody>
</table>
### Configuring the Tunnel Profile (GUI)

Follow the steps given below to configure the tunnel profile:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose Configuration &gt; Tags &amp; Profiles &gt; EoGRE.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click the Tunnel Profiles tab.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click the Add button. The Add Tunnel Profile window is displayed.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Click the General tab and complete the following steps:</td>
</tr>
<tr>
<td></td>
<td>a) In the Name field, specify the tunnel profile name.</td>
</tr>
<tr>
<td></td>
<td>b) In the Status field, slide the button to change the status to Enabled.</td>
</tr>
<tr>
<td></td>
<td>c) In the Central Forwarding field, slide the button to Enabled, to enable the feature.</td>
</tr>
<tr>
<td></td>
<td>d) In the DHCP Option-82 section, change the Status field and the ASCII field to Enabled, as per requirement.</td>
</tr>
<tr>
<td></td>
<td>e) In the Delimiter field, specify the delimiter.</td>
</tr>
<tr>
<td></td>
<td>f) From the Circuit ID Available Services list, select an available services and click the &gt; sign to add the services to the assigned list.</td>
</tr>
<tr>
<td></td>
<td>g) From the Remote ID Available Services list, select an available services and click the &gt; sign to add the services to the assigned list.</td>
</tr>
<tr>
<td></td>
<td>h) In the AAA section, choose an appropriate status for the Radius Proxy field, the Accounting Proxy field, and the Override field.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Click the Rules tab, and complete the following steps:</td>
</tr>
<tr>
<td></td>
<td>a) Click the Add Rules button.</td>
</tr>
<tr>
<td></td>
<td>b) In the Priority field, specify the priority of the rule from a range of 1 to 100.</td>
</tr>
</tbody>
</table>
c) In the *Realm* field, specify a realm.
d) From the *Domain* drop-down list, choose a domain.
e) In the *VLAN Id* field, specify the VLAN ID that ranges between 1 and 4094.
f) Click *Save*.

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

---

## Associating WLAN to a Wireless Policy Profile

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
*configure terminal*  
*Example:*  
Device# configure terminal | Enters global configuration mode. |
| **Step 2**  
*ap* *mac-address*  
*Example:*  
Device(config)# ap 80E8.6FD4.0BB0 | Configures an AP and enters AP profile configuration mode. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><code>policy-tag policy-tag-name</code></td>
<td>Maps the EoGRE policy tag to the AP.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-tag)# policy-tag eogre_tag</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>site-tag site-tag-name</code></td>
<td>Maps a site tag to the AP.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-tag)# site-tag sp-flex-site</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>end</code></td>
<td>Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-ap-tag)# end</td>
<td></td>
</tr>
</tbody>
</table>

### 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:

```plaintext
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:

```plaintext
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:

```plaintext
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         
```
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 : Tunnel12
Mode : IPv6
IP : fd09:9:8:21::90
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
```

<table>
<thead>
<tr>
<th>Client MAC</th>
<th>AP MAC</th>
<th>Domain</th>
<th>Tunnel</th>
<th>VLAN</th>
<th>Local</th>
</tr>
</thead>
<tbody>
<tr>
<td>74da.3828.88b0</td>
<td>80e8.6fd4.9520</td>
<td>eogre_domain</td>
<td>N/A</td>
<td>2121</td>
<td>No</td>
</tr>
</tbody>
</table>

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
PT 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
Verifying the EoGRE Tunnel Configuration

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
```

<table>
<thead>
<tr>
<th>AP MAC</th>
<th>Domain</th>
<th>Active Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>80e8.6fd4.9520</td>
<td>eogre_domain</td>
<td>Tunnel1</td>
</tr>
</tbody>
</table>
To view the wireless tunnel profile summary, use the following command:

```plaintext
Device# show wireless profile tunnel summary
```

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>AAA-Override</th>
<th>AAA-Proxy</th>
<th>DHCP Opt82</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>eogre_tunnel</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>eogre_tunnel_set</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>eogre_tunnel_snmp</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

To view a wireless tunnel profile's details, use the following command:

```plaintext
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

<table>
<thead>
<tr>
<th>Priority</th>
<th>Realm</th>
<th>Vlan Domain (Status/Primary GW/Secondary GW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>*</td>
<td>2121 eogre_domain (Enabled/Tunnel1/Tunnel2)</td>
</tr>
</tbody>
</table>

To view detailed information about an EoGRE tunnel domain's status, use the following command:

```plaintext
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:

```plaintext
Device# show ap tunnel eogre events
```

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>#Times</th>
<th>Event</th>
<th>RC Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/18/2019 23:50:26.341</td>
<td>6</td>
<td>IAPP_STATS</td>
<td>0 GW Tunnel2 uptime:0s</td>
</tr>
<tr>
<td>02/18/2019 23:49:40.222</td>
<td>2</td>
<td>CLIENT_JOIN</td>
<td>0 74da.3828.88b0, (eogre_domain/2121)</td>
</tr>
<tr>
<td>02/18/2019 23:48:43.549</td>
<td>1</td>
<td>CLIENT_LEAVE</td>
<td>0 74da.3828.88b0, (eogre_domain/2121)</td>
</tr>
<tr>
<td>02/18/2019 23:47:33.127</td>
<td>1</td>
<td>DOMAIN_STATUS</td>
<td>0 eogre_domain Active GW: Tunnel1</td>
</tr>
<tr>
<td>02/18/2019 23:47:33.124</td>
<td>4</td>
<td>AP_TUNNEL_STATUS</td>
<td>0 Tunnel2 Dn</td>
</tr>
<tr>
<td>02/18/2019 23:47:33.124</td>
<td>1</td>
<td>MSG_CLIENT_DEL</td>
<td>0 GW Tunnel2 (IP: 9.51.1.12)</td>
</tr>
<tr>
<td>02/18/2019 23:47:33.124</td>
<td>2</td>
<td>TUNNEL_ADD</td>
<td>0 GW Tunnel2</td>
</tr>
<tr>
<td>02/18/2019 23:47:33.120</td>
<td>3</td>
<td>MSG_CLIENT_DEL_PD</td>
<td>0 GW Tunnel1 (IP: 9.51.1.11)</td>
</tr>
<tr>
<td>02/18/2019 23:47:31.763</td>
<td>2</td>
<td>AP_DOMAIN_PUSH</td>
<td>0 Delete:eogre_domain_set, 0 GWs</td>
</tr>
</tbody>
</table>
To view the summary information of the EoGRE tunnel gateway, use the following command:

```
Device# show ap tunnel eogre gateway summary
```

<table>
<thead>
<tr>
<th>AP MAC</th>
<th>Gateway</th>
<th>Type</th>
<th>IP</th>
<th>State</th>
<th>Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>80e8.6fd4.9520</td>
<td>Tunnel1</td>
<td>IPv4</td>
<td>9.51.1.11</td>
<td>Up</td>
<td>1</td>
</tr>
<tr>
<td>80e8.6fd4.9520</td>
<td>Tunnel2</td>
<td>IPv4</td>
<td>9.51.1.12</td>
<td>Down</td>
<td>0</td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>AP MAC</th>
<th>Domain</th>
<th>Active Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>80e8.6fd4.9520</td>
<td>eogre_domain</td>
<td>Tunnel1</td>
</tr>
</tbody>
</table>

To view information about EoGRE events on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre events
```

<table>
<thead>
<tr>
<th>AP 80e8.6fd4.9520</th>
<th>Event history</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>#Times</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------</td>
</tr>
<tr>
<td>02/18/2019 23:50:26.341 6</td>
<td>IAPP_STATS</td>
</tr>
<tr>
<td>02/18/2019 23:49:40.222 2</td>
<td>CLIENT_JOIN</td>
</tr>
<tr>
<td>02/18/2019 23:48:43.549 1</td>
<td>CLIENT_LEAVE</td>
</tr>
<tr>
<td>02/18/2019 23:47:33.127 1</td>
<td>DOMAIN_STATUS</td>
</tr>
<tr>
<td>02/18/2019 23:47:33.124 4</td>
<td>AP_TUNNEL_STATUS</td>
</tr>
<tr>
<td>02/18/2019 23:47:33.124 1</td>
<td>MSG_CLIENT_DEL</td>
</tr>
<tr>
<td>02/18/2019 23:47:33.124 2</td>
<td>TUNNEL_ADD</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>AP MAC</th>
<th>Domain</th>
<th>Active Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>80e8.6fd4.9520</td>
<td>eogre_domain</td>
<td></td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Primary GW</th>
<th>Secondary GW</th>
<th>Active GW</th>
<th>Redundancy</th>
<th>AdminState</th>
</tr>
</thead>
<tbody>
<tr>
<td>eogre_domain</td>
<td>Tunnel1</td>
<td>Tunnel2</td>
<td>Tunnel1</td>
<td>Non-Revertive</td>
<td>Up</td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>AP MAC</th>
<th>Gateway</th>
<th>Type</th>
<th>IP</th>
<th>State</th>
<th>Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>80e8.6fd4.9520</td>
<td>Tunnel1</td>
<td>IPv4</td>
<td>9.51.1.11</td>
<td>Up</td>
<td>1</td>
</tr>
<tr>
<td>80e8.6fd4.9520</td>
<td>Tunnel2</td>
<td>IPv4</td>
<td>9.51.1.12</td>
<td>Down</td>
<td>0</td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>Gateway</th>
<th>Mode</th>
<th>IP</th>
<th>State</th>
<th>MTU</th>
<th>AP MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel1</td>
<td>IPv4</td>
<td>9.51.1.12</td>
<td>Down</td>
<td>0</td>
<td>80e8.6fd4.9520</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Number of Wireless Clients</td>
</tr>
<tr>
<td>Traffic</td>
</tr>
<tr>
<td>Total Number of Received Packets</td>
</tr>
<tr>
<td>Total Number of Received Bytes</td>
</tr>
<tr>
<td>Total Number of Transmitted Packets</td>
</tr>
<tr>
<td>Total Number of Transmitted Bytes</td>
</tr>
<tr>
<td>Total Number of Lost Keepalive</td>
</tr>
</tbody>
</table>
Verifying the EoGRE Tunnel Configuration
Link Aggregation Control Protocol and Port Aggregation Protocol

Information About LACP

Link Aggregation Control Protocol (LACP) is a part of an IEEE specification (802.3ad) that allows you to bundle several physical ports together to form a single logical channel. LACP allows a switch to negotiate an automatic bundle by sending LACP packets to the peer. By using the LACP, the Wireless Controller learns the identity of partners capable of supporting LACP, and the capabilities of each port. The LACP then dynamically groups similarly configured ports into a single logical link (channel or aggregate port). Similarly, configured ports are grouped based on hardware, administrative, and port parameter constraints. 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.

Information About Port Aggregation Protocol

Port Aggregation Protocol (PAgP) is a Cisco-proprietary protocol that you can run on controllers. PAgP facilitates the automatic creation of EtherChannels by exchanging PAgP packets between Ethernet ports. PAgP packets are sent between Fast EtherChannel-capable ports in order to form a channel. When any of the active ports fail, a standby port becomes active.

By using PAgP, the controller learns the identity of partners that are capable of supporting PAgP and the capabilities of each port. PAgP then dynamically groups similarly configured ports (on a single device in a
stack) into a single logical link (channel or aggregate port). Similarly, configured ports are grouped based on hardware, administrative, and port parameter constraints.

## Configuring LACP and PAgP

To configure multi-LAG using LACP, multiple port-channel interfaces must be created, and these interfaces should be added to the corresponding port bundle. LACP should also be configured on the uplink switch for the LACP bundle to come up.

- Create a Port-Channel Interface
- Add an Interface to a Port Channel (LACP)
- Adding VLANs Under a LAG

To configure multi-LAG using PAgP, multiple port-channel interfaces must be created, and these interfaces should be added to the corresponding port bundle. PAGP should also be configured on the uplink switch for the PAGP bundle to come up.

- Create a Port-Channel Interface
- Add an Interface to a Port Channel (PAgP)

The Cisco Catalyst 9800-80 Wireless Controller has eight ports, while the Cisco Catalyst 9800-40 and Cisco Catalyst 9800-L wireless controllers have four ports each. You can create multi-LAGs in any combination of ports with a minimum of two ports in one LAG. Each LAG should be connected to a different switching architecture for traffic separation. Using this topology, you can support a use case where guest traffic can be completely isolated to a different switch or network, from the enterprise network.

The following is a sample topology:
Restrictions for LACP and PAgP

- Each LAG must be connected to a single switch.
- Different VLANs must be assigned to different LAGs.
- If the primary LAG fails, automatic failover to secondary LAG is not supported.
## Create a Port-Channel Interface

Follow the procedure given below to create a port-channel interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1.   | `configure terminal`  
    | **Example:**  
    | Device# configure terminal  | Enters global configuration mode. |
| 2.   | `interface port-channel port-channel`  
    | **Example:**  
    | Device(config)# interface port-channel 2 | Configures the port channel and enters interface configuration mode. |
| 3.   | `switchport mode trunk`  
    | **Example:**  
    | Device(config-if)# switchport mode trunk | Configures the port as trunk. |
| 4.   | `no shutdown`  
    | **Example:**  
    | Device(config-if)# no shutdown | Enables the interface. |

## Add an Interface to a Port Channel (LACP)

Follow the procedure given below to add an interface to a port channel.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1.   | `configure terminal`  
    | **Example:**  
    | Device# configure terminal  | Enters global configuration mode. |
| 2.   | `interface TenGigabitEthernet port-slot`  
    | **Example:**  
    | Device(config)# interface TenGigabitEthernet0/0/0 | Configures the port. |
| 3.   | `channel-group group-number {active | passive}`  
    | **Example:** | Assigns the port to a channel group, and specifies the LACP mode. |
Adding VLANs Under a LAG

Follow the procedure given below to add different VLANs under different LAGs.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>interface port-channel port-channel</td>
<td>Configures the port-channel.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface port-channel 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>switchport trunk allowed vlan vlan-id</td>
<td>Sets the VLAN IDs of the allowed VLANs when the port is in trunking mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# switchport trunk allowed vlan 10,30,50</td>
<td></td>
</tr>
</tbody>
</table>

Adding an Interface to a Port Channel (PAgP)

Follow the procedure given below to add an interface to a port channel.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>interface TenGigabitEthernet port-slot</td>
<td>Configures the TenGigabitEthernet interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Removing a Port Channel Group from a Physical Port

Perform this task to remove a port channel group from a physical port.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**

- configure terminal
  
  - Example:
    Device# configure terminal

  Enters global configuration mode. |
| **Step 2**

- interface TenGigabitEthernet port-slot
  
  - Example:
    Device(config)# interface TenGigabitEthernet0/0/0

  Enters the TenGigabitEthernet interface. |
| **Step 3**

- no channel-group channel-group number
  
  - Example:
    Device(config-if)# no channel-group 1

  Removes the port channel group from the physical port. |
| **Step 4**

- end
  
  - Example:
    Device(config-if)# end

  Exits interface configuration mode. |

**Verifying the Configuration**

To view a port channel's state, use the following command:

Device# show etherchannel summary

Flags: D - down  P - bundled in port-channel
I - stand-alone  s - suspended
H - Hot-standby (LACP only)
R - Layer3  S - Layer2
U - in use    f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators: 1

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Po3 (SU)</td>
<td>LACP</td>
<td>Tw0/0/0 (P) Tw0/0/1 (P)</td>
</tr>
<tr>
<td>4</td>
<td>Po4 (SU)</td>
<td>LACP</td>
<td>Tw0/0/2 (P) Tw0/0/3 (P)</td>
</tr>
</tbody>
</table>

To verify an LACP or PAgP configuration, use the following commands:

Device# show running-config interface tenGigabitEthernet 0/0/0

Building configuration...

Current configuration : 114 bytes
!
interface TenGigabitEthernet0/0/0
  switchport mode trunk
  switchport trunk allowed vlan 10,30,50
  no negotiation auto
  channel-group 1 mode active

Device# show running-config interface port-channel 1

Building configuration...

Current configuration : 54 bytes
!
interface Port-channel1
  switchport mode trunk
  switchport trunk allowed vlan 10,30,50
end
Hotspot 2.0

Introduction to Hotspot

The Hotspot feature enables IEEE 802.11 devices to interwork with external networks. The interworking service aids network discovery and selection, enabling information transfer from external networks. It provides information to the stations about the networks before association.

Interworking not only helps users within the home, enterprise, and public access domains, but also assists manufacturers and operators to provide common components and services for IEEE 802.11 customers. These services are configured on a per WLAN basis on the Cisco Wireless Controller (controller).

Hotspot 2.0, also known as HS2 and Wi-Fi Certified Passpoint, is based on the IEEE 802.11u and Wi-Fi Alliance Hotspot 2.0 standards. It seeks to provide a better bandwidth and services-on-demand to end users. The Hotspot 2.0 feature allows mobile devices to join the Wi-Fi network automatically and also during roaming, when the devices enter the Hotspot 2.0 area.

The Hotspot 2.0 feature has four distinct parts:

- Hotspot 2.0 Beacon Advertisement: Allows a mobile device to discover Hotspot 2.0 and 802.11u compatible WLANs.
- Access Network Query Protocol (ANQP) Queries: Queries about the networks from IEEE 802.11 devices, such as network type (private or public); connectivity type (local network, internet connection, and so on), or the network providers supported by a given network.
- Online Sign-up (OSU): Allows a mobile device to obtain credentials to authenticate itself with the Hotspot or WLAN.
- Authentication and Session Management: Authentication (802.1x) and management of the STA session (session expiration, extension, and so on).

In order to mark a WLAN as Hotspot 2.0-compatible, the 802.11u-mandated information element and the Hotspot 2.0 information element is added to the basic service set (BSS) beacon advertised by the corresponding AP and in WLAN probe responses.

The Hotspot 2.0 feature supports only local mode or FlexConnect mode (central switching and central authentication).
Configuring Hotspot 2.0

Configuring an Access Network Query Protocol Server

ANQP is a query and response protocol that defines services offered by an AP, usually at a Wi-Fi hot spot.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wireless hotspot anqp-server server-name</td>
<td>Configures a Hotspot 2.0 Access Network Query Protocol (ANQP) server.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless hotspot anqp-server my_server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>description description</td>
<td>Adds a description for the ANQP server.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-anqp-server)# description &quot;My Hotspot 2.0&quot;</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>3gpp-info mobile-country-code mobile-network-code</td>
<td>Configures a 802.11u 3rd Generation Partnership Project (3GPP) cellular network.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-anqp-server)# 3gpp-info us mcc</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The mobile-country-code should be a 3-digit decimal number. The mobile-network-code should be a 2 or 3-digit decimal number.</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>anqp fragmentation-threshold threshold-value</code></td>
<td>Configures the ANQP reply fragmentation threshold, in bytes. The ANQP protocol can be customized by setting the fragmentation threshold, after which, the ANQP reply will be split into multiple messages. Note We recommend that you use the default values for the deployment.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>anqp-domain-id domain-id</code></td>
<td>Configures the Hotspot 2.0 ANQP domain identifier.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>authentication-type</code></td>
<td>Configures the 802.11u network authentication type. Depending on the authentication type, a URL is needed for HTTP and HTTPS.</td>
</tr>
<tr>
<td>Step 8</td>
<td>`connection-capability ip-protocol port-number { closed</td>
<td>open</td>
</tr>
<tr>
<td>Step 9</td>
<td><code>domain domain-name</code></td>
<td>Configures an 802.11u domain name. You can configure up to 32 domain names. The <code>domain-name</code> should not exceed 220 characters.</td>
</tr>
<tr>
<td>Step 10</td>
<td><code>ipv4-address-type ipv4-address-type</code></td>
<td>Configures an 802.11u IPv4 address type in the hotspot network.</td>
</tr>
<tr>
<td>Step 11</td>
<td><code>ipv6-address-type ipv6-address-type</code></td>
<td>Configures an 802.11u IPv6 address type in the hotspot network.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Device(config-wireless-anqp-server)# ipv6-address-type available</td>
<td>Configures an 802.11u NAI realm profile that identifies the realm that is accessible using the AP.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 12**  
**nai-realm realm-name**  
**Example:**  
Device(config-wireless-anqp-server)# nai cisco.com  

**Step 13**  
**operating-class class-id**  
**Example:**  
Device(config-wireless-anqp-server)# operating-class 25  

**Step 14**  
**operator operator-name language**  
**Example:**  
Device(config-wireless-anqp-server)# operator XYZ-operator EN  

**Step 15**  
**osu-ssid SSID**  
**Example:**  
Device(config-wireless-anqp-server)# osu-ssid test  

**Step 16**  
**roaming-oi OI-value [beacon]**  
**Example:**  
Device(config-wireless-anqp-server)# roaming-oi 24 beacon  

**Step 17**  
**venue venue-name language-code**  
**Example:**  
Device(config-wireless-anqp-server)# venue bank en  

### Configuring the WAN Metrics

This procedure configures the Wide Area Network (WAN) parameters such as uplink and downlink speed, link status, load, and so on.
### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
|      | **Example:**  
Device# configure terminal |         |
| 2    | `wireless hotspot anqp-server server-name` | Configures a Hotspot 2.0 ANQP server. |
|      | **Example:**  
Device(config)# wireless hotspot anqp-server my_server |         |
| 3    | `wan-metrics downlink-load load-value` | Configures the WAN downlink load. |
|      | **Example:**  
Device(config-wireless-anqp-server)# wan-metrics downlink-load 100 |         |
| 4    | `wan-metrics downlink-speed speed` | Configures the WAN downlink speed, in kbps. |
|      | **Example:**  
Device(config-wireless-anqp-server)# wan-metrics downlink-speed 1000 |         |
| 5    | `wan-metrics full-capacity-link` | Sets to operate a WAN link at its maximum capacity. |
|      | **Example:**  
Device(config-wireless-anqp-server)# wan-metrics full-capacity-link |         |
| 6    | `wan-metrics link-status {down | not-configured | test-state | up}` | Sets the WAN link status. |
|      | **Example:**  
Device(config-wireless-anqp-server)# wan-metrics link-status down |         |
| 7    | `wan-metrics load-measurement-duration duration` | Configures the uplink or downlink load measurement duration. |
|      | **Example:**  
Device(config-wireless-anqp-server)# wan-metrics load-measurement-duration 100 |         |
| 8    | `wan-metrics uplink-load load-value` | Configures the WAN uplink load. |
|      | **Example:**  
Device(config-wireless-anqp-server)# wan-metrics uplink-load 100 |         |
| 9    | `wan-metrics uplink-speed speed` | Configures the WAN uplink speed, in kbps. |
|      | **Example:**  
Device(config-wireless-anqp-server)# wan-metrics uplink-speed 1000 |         |
# Configuring an Online Sign-up Provider

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>wireless hotspot anqp-server server-name</code></td>
<td>Configures a Hotspot 2.0 Access Network Query Protocol (ANQP) server.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# <code>wireless hotspot anqp-server my_server</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>osu-provider osu-provider-name</code></td>
<td>Configures a Hotspot 2.0 Online Sign-up (OSU) provider name.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wireless-anqp-server)# <code>osu-provider my-osu</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>name osu-operator-name lang-code description</code></td>
<td>Configures the name of the OSU operator in a given language. The <code>osu-operator-name</code> and <code>description</code> should not exceed 220 characters. The language code should be 2 or 3 lower-case letters (a-z).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-anqp-osu-provider)# <code>name xyz-oper en xyz-operator</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>server-uri server-uri</code></td>
<td>Configures the server Uniform Resource Identifier (URI) of the OSU operator.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-anqp-osu-provider)# <code>server-uri cisco.com</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>`method {oma-dm</td>
<td>soap-xml-spp}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-anqp-osu-provider)# <code>method oma-dm</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>nai-realm nai-realm</code></td>
<td>Configures the Network Access Identifier (NAI) realm of the OSU operator. The <code>nai-realm</code> should not exceed 220 characters.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-anqp-osu-provider)# <code>nai-realm cisco.com</code></td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>icon file-name</code></td>
<td>Configures the icon for the OSU provider. The <code>file-name</code> should not exceed 100 characters.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-anqp-osu-provider)# <code>icon xyz.jpeg</code></td>
<td></td>
</tr>
</tbody>
</table>
## Configuring Hotspot 2.0 WLAN

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>wlan wlan-name wlan-id ssid</code></td>
<td>Configures a WLAN and enters the WLAN configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config)# wlan hs2 1 hs2</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>security wpa wpa2 gtk-randomize</code></td>
<td>Configures random-GTK for hole-196 mitigation.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config-wlan)# security wpa wpa2 gtk-randomize</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>no shutdown</code></td>
<td>Enables the WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config-wlan)# no shutdown</code></td>
<td></td>
</tr>
</tbody>
</table>

## Configuring an Online Subscription with Encryption WLAN

Online subscription with Encryption (OSEN) WLAN is used to onboard a hotspot network (to get the necessary credentials) in a secure manner.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>wlan wlan-name wlan-id ssid</code></td>
<td>Configures a WLAN and enters WLAN configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config)# wlan hs2 1 hs2</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>security wpa osen</code></td>
<td>Enables WPA OSEN security support.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config-wlan)# security wpa osen</code></td>
<td></td>
</tr>
</tbody>
</table>
### Attaching an ANQP Server to a Policy Profile

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless profile policy policy-profile-name ssid</td>
<td>Configures a policy profile.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# wireless profile policy policy-hotspot</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> shutdown</td>
<td>Disables the policy profile.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wireless-policy)# shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> hotspot anqp-server server-name</td>
<td>Attaches the Hotspot 2.0 ANQP server to the policy profile.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wireless-policy)# hotspot anqp-server my-server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> no shutdown</td>
<td>Enables the policy profile.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-wireless-policy)# no shutdown</td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

Attach the policy profile to the WLAN to make the WLAN Hotspot 2.0 enabled.

---

**Purpose**

Device(config-wlan)# security wpa oSEN

**Note**

OSEN and robust security network (RSN) are mutually exclusive. If RSN is enabled on a WLAN, OSEN cannot be enabled on the same WLAN.

**Step 4**

no shutdown

**Example:**

Device(config-wlan)# no shutdown

Enables the WLAN.
Configuring Interworking for Hotspot

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>wireless hotspot anqp-server server-name</code></td>
<td>Configures a Hotspot 2.0 ANQP server.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# wireless hotspot anqp-server my_server</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>`network-type allowed network-type internet-access {allowed</td>
<td>forbidden}`</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-anqp-server)# network-type guest-private internet-access allowed</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>hessid HESSID-value</code></td>
<td>(Optional) Configures a homogenous extended service set.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-anqp-server)# hessid 12.13.14</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>group venue-group venue-type</code></td>
<td>Selects a group type and venue type from the list of available options.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-wireless-anqp-server)# group business bank</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Custom QoS Mapping

For interworking with IP networks, a map is devised between the 802.11e user priorities and the IP differentiated services code point (DSCP).

Mapping is specified as DSCP ranges to individual user priority values, and as a set of exceptions with one-to-one mapping between DSCP values and UP values. If a QoS map is enabled and user-configurable mappings are not added, the default values are used.

The following table shows a QoS Map, where an AP provides the wireless client with the required mapping from IP DSCP to 802.11e user priority.

Table 58: Default DSCP-range-to-user priority Mapping

<table>
<thead>
<tr>
<th>IP DSCP Range</th>
<th>802.11e User Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-7</td>
<td>0</td>
</tr>
</tbody>
</table>
### Configuring DSCP-to-User Priority Mapping Exception

When you configure a QoS mapping or exception, a custom QoS map is created and sent to the corresponding AP.

If there are no DSCP-to-User Priority mapping or exception entries, an empty QoS map is used.

The following table shows the set of exceptions with one-to-one mapping between DSCP values and user priority values.

<table>
<thead>
<tr>
<th>IP DSCP Range</th>
<th>802.11e User Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-15</td>
<td>1</td>
</tr>
<tr>
<td>16-23</td>
<td>2</td>
</tr>
<tr>
<td>24-31</td>
<td>3</td>
</tr>
<tr>
<td>32-39</td>
<td>4</td>
</tr>
<tr>
<td>40-47</td>
<td>5</td>
</tr>
<tr>
<td>48-55</td>
<td>6</td>
</tr>
<tr>
<td>56-63</td>
<td>7</td>
</tr>
</tbody>
</table>

---

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap profile profile-name</td>
<td>Configures an AP profile and enters AP profile configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# ap profile hs2-profile</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> qos-map dscp-to-up-range user-priority up-to-dscp dscp-start dscp-end</td>
<td>Configures DSCP-to-user priority mapping. You can configure up to eight configuration entries; one for each user-priority value. If you do not configure a custom value, a non-configured value (0xFF) is sent to the AP. Use the no form of the command to disable the configuration. To delete all the custom mappings, use the no dscp-to-up-range command.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-ap-profile)# qos-map dscp-to-up-range 6 52 23 62</td>
<td></td>
</tr>
</tbody>
</table>
Table 59: Default DSCP-range-to-User Priority Mapping Exceptions

<table>
<thead>
<tr>
<th>IP DSCP</th>
<th>802.11e User Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>18</td>
<td>3</td>
</tr>
<tr>
<td>20</td>
<td>3</td>
</tr>
<tr>
<td>22</td>
<td>3</td>
</tr>
<tr>
<td>26</td>
<td>4</td>
</tr>
<tr>
<td>34</td>
<td>5</td>
</tr>
<tr>
<td>46</td>
<td>6</td>
</tr>
<tr>
<td>48</td>
<td>7</td>
</tr>
<tr>
<td>56</td>
<td>7</td>
</tr>
</tbody>
</table>

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Example:</td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures an AP profile and enters AP profile configuration mode.</td>
</tr>
<tr>
<td>ap profile <em>profile-name</em></td>
<td>Example:</td>
</tr>
<tr>
<td>Device(config)# ap profile hs2-profile</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures DSCP-to-user priority exception.</td>
</tr>
<tr>
<td>qos-map dscp-to-up-exception <em>dscp-num</em> user-priority</td>
<td>Example:</td>
</tr>
<tr>
<td>Device(config-ap-profile)# qos-map dscp-to-up-exception 42 6</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring Trust Upstream DSCP Value

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ap profile <em>profile-name</em></td>
<td>Configures an AP profile and enters AP profile configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap profile hs2-profile</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>qos-map trust-dscp-upstream</td>
<td>Configures the AP to trust upstream DSCP instead of user priority. Use the no form of the command to disable the configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-ap-profile)# qos-map trust-dscp-upstream</td>
<td></td>
</tr>
</tbody>
</table>

## Configuring Generic Advertisement Service Rate Limit

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ap profile <em>profile-name</em></td>
<td>Configures an AP profile and enters AP profile configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap profile hs2-profile</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>gas-ap-rate-limit <em>request-number</em> <em>interval</em></td>
<td>Configures the number of Generic Advertisement Services (GAS) request action frames sent to the controller by an AP in a given interval.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-ap-profile)# gas-ap-rate-limit 20 120</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-ap-profile)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>wireless hotspot gas-rate-limit <em>gas-requests-to-process</em></td>
<td>Configures the number of GAS request action frames to be processed by the controller.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless hotspot gas-rate-limit 100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Verifying Hotspot 2.0 Configuration**

Use the following `show` commands to verify the QoS and AP GAS rate limit.

To view whether the QoS map ID is user configured or the default one, use the following command:

```
Device# show ap profile <profile name> detailed
```

QoS Map : user-configured

To view the QoS map values used and their source, use the following command:

```
Device# show ap profile <profile name> qos-map
```

QoS Map : default

<table>
<thead>
<tr>
<th>DSCP ranges to User Priorities</th>
<th>User Priority</th>
<th>DSCP low</th>
<th>DSCP high</th>
<th>Upstream UP to DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>16</td>
<td>23</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>24</td>
<td>31</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>32</td>
<td>39</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>40</td>
<td>47</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>48</td>
<td>55</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>56</td>
<td>63</td>
<td>48</td>
</tr>
</tbody>
</table>

DSCP to UP mapping exceptions

<table>
<thead>
<tr>
<th>DSCP</th>
<th>User Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>18</td>
<td>3</td>
</tr>
<tr>
<td>20</td>
<td>3</td>
</tr>
<tr>
<td>22</td>
<td>3</td>
</tr>
<tr>
<td>26</td>
<td>4</td>
</tr>
<tr>
<td>34</td>
<td>5</td>
</tr>
<tr>
<td>46</td>
<td>6</td>
</tr>
<tr>
<td>48</td>
<td>7</td>
</tr>
<tr>
<td>56</td>
<td>7</td>
</tr>
</tbody>
</table>

To view the AP rate limiter configuration, use the following command:

```
Device# show ap name AP0462.73e8.f2c0 config general | i GAS
```

GAS rate limit Admin status : Enabled
Number of GAS request per interval : 30
GAS rate limit interval (msec) : 100
Verifying Hotspot 2.0 Configuration
Information About Express Wi-Fi by Facebook

Express Wi-Fi by Facebook is a cloud-based, low-cost solution for local entrepreneurs and SMBs in emerging countries to provide Wi-Fi access. Using Express Wi-Fi by Facebook, users can buy data packs and find nearby hotspots.

Facebook provides the software (and sometimes hardware) infrastructure while the ISP or SMB provides internet connectivity and deployments to the subscribers. These service providers provision guest access through a captive portal. This can include both free and paid services including paid internet access with quota enforcement.

Express Wi-Fi by Facebook feature is enabled through a FlexConnect deployment based on the cloud-hosted Cisco Catalyst 9800-CL Series Wireless Controller where the Cisco AP performs client-related functions such as web authentication, captive portal redirect, matching and accounting of traffic classes and connection to the RADIUS server. This feature also supports FQDN (DNS ACLs) and IP ACLs as well as MAC authentication on the AP. The controller provisions the AP with the required configuration for these tasks.

If an AP reboots in standalone mode, the flexconnect URL ACL is not retained. This will cause Express Wi-Fi by Facebook to stop working.

The Express Wi-Fi by Facebook solution comprises the following components:

- Cisco Catalyst 9800-CL Series Wireless Controller
Restrictions for Express Wi-Fi by Facebook

- Express Wi-Fi by Facebook is supported only in a FlexConnect deployment with local switching, local authentication, and local association.
- Express Wi-Fi by Facebook is supported only on Cisco Aironet Wave 2 and Catalyst access points.
- Only three traffic classes are supported.
- The AP supports only three ACLs per client.
- All APs forming a roaming domain should have Layer 2 reachability.
- Upto 64 complex rules and 512 simple rules per ACL are supported, where a simple rule comprises of a destination IP address and port. A complex rule contains more than a destination IP address and port information.
- Only RADIUS CoA messages with the Facebook attribute are supported on the AP.

Enabling Express Wi-Fi by Facebook NAC for Policy Profile (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Tags &amp; Profiles &gt; Policy.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Policy page, click the name of the desired Policy Profile.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Edit Policy Profile window, click the Advanced tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the AAA Policy section, select the AAA check box.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Choose Facebook from the NAC Type drop-down list.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Update &amp; Apply to Device.</td>
</tr>
</tbody>
</table>

Enabling Accounting RADIUS Server for Flex Profile (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Tags &amp; Profiles &gt; Flex.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Flex page, click the name of the desired Flex Profile.</td>
</tr>
</tbody>
</table>
Configuring Captive Portal for Express Wi-Fi by Facebook (GUI)

Procedure

Step 1 Choose Configuration > Security > Web Auth.

Step 2 On the Web Auth page, click the name of the desired parameter map.

Step 3 In the Edit Web Auth Parameter window, click the Advanced tab.

Step 4 In the Redirect to External Server section, enter the key in the Express WiFi Key field.

Step 5 Click Update & Apply to Device.

Configuring Captive Portal for Express Wi-Fi by Facebook (CLI)

Before you begin

- Configure the URL filter list.
- Configure the IP ACL.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>parameter-map type webauth</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# parameter-map type</td>
</tr>
<tr>
<td></td>
<td>webauth parameter-map- name</td>
</tr>
<tr>
<td></td>
<td>Parameter-Map Facebook-Map</td>
</tr>
<tr>
<td>Step 3</td>
<td>type webauth</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-params-parameter-map)# type webauth</td>
<td></td>
</tr>
</tbody>
</table>

### Step 4
**redirect for-login url-string**

**Example:**
```
Device(config-params-parameter-map)# redirect for-login https://xwfcisco-us.expresswifi.com/customer/captive_portal
```

Configure the URL string for redirection during login.

### Step 5
**captive-bypass-portal**

**Example:**
```
Device(config-params-parameter-map)# captive-bypass-portal
```

Configure captive bypassing.

### Step 6
**redirect vendor-specific xwf key 0 vendor-key**

**Example:**
```
Device(config-params-parameter-map)# redirect vendor-specific xwf key 0 vendor-key
```

Configure the URL string for redirection during login.

### Step 7
**end**

**Example:**
```
Device(config-params-parameter-map)# end
```

Returns to privileged EXEC mode.

---

**Configuring Express Wi-Fi by Facebook Policy on Controller (CLI)**

**Before you begin**
- Enable web authentication and MAC filtering on the WLAN.
- Configure RADIUS proxy server and accounting server.

**Procedure**

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

**Example:**
```
Device# configure terminal
```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>wireless profile policy policy-profile-name</td>
<td>Configures the wireless profile policy.</td>
</tr>
</tbody>
</table>

**Example:**
```
Device# wireless profile policy policy-profile-name
```
### Command or Action

**Device(config)# wireless profile policy default-policy-profile**

**Purpose**

Configures AAA override to apply policies coming from the AAA or ISE servers.

---

**Step 3**

aaa-override  
**Example:**  
Device(config-wireless-policy)# aaa override

Disables central switching and enables local switching.

---

**Step 4**

no central switching  
**Example:**  
Device(config-wireless-policy)# no central switching

Disables central association and enables local association for locally switched clients.

---

**Step 5**

no central association  
**Example:**  
Device(config-wireless-policy)# no central association

Disables central authentication and enables local authentication.

---

**Step 6**

no central authentication  
**Example:**  
Device(config-wireless-policy)# no central authentication

Configures NAC in the policy profile.

---

**Step 7**

nac xwf  
**Example:**  
Device(config-wireless-policy)# nac xwf

Configures a VLAN name or VLAN ID.

---

**Step 8**

vlan vlan-name  
**Example:**  
Device(config-wireless-policy)# vlan 9

Enables the profile policy.

---

**Step 10**

end  
**Example:**  
Device(config)# end

Returns to privileged EXEC mode.
## Configuring RADIUS Server for Accounting and Authentication in FlexConnect Profile (CLI)

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `configure terminal` | Enters global configuration mode.  
**Example:**  
Device# configure terminal |
| Step 2 | `wireless profile flex flex-profile-name` | Configures the wireless flex profile and enters wireless flex profile configuration mode.  
**Example:**  
Device(config)# wireless profile flex default-flex-profile |
| Step 3 | `local-auth radius-server-group group-name` | Configures the authentication server group name.  
**Example:**  
Device(config-wireless-flex-profile)# local-auth radius-server-group FB_GROUP |
| Step 4 | `local-accounting radius-server-group group-name` | Configures the accounting server group name.  
**Example:**  
Device(config-wireless-flex-profile)# local-accounting radius-server-group group-name |
| Step 5 | `local-roaming` | Enables local roaming.  
**Example:**  
Device(config-wireless-flex-profile)# local-roaming |
| Step 6 | `acl-policy policy-name` | Configures ACL policy.  
**Example:**  
Device(config-wireless-flex-profile)# acl-policy fbs |
| Step 7 | `urlfilter list list-name` | Applies the URL list to the Flex profile.  
**Example:**  
Device(config-wireless-flex-profile)# urlfilter list fbs  
Here, `list-name` refers to the URL filter list name. The list name must not exceed 32 alphanumeric characters.  
**Note:** For a given traffic class, the `list-name` should match the above ACL `policy-name`. |
Verifying Express Wi-Fi by Facebook Configurations on Controller

To view ACLs applied on a specific client and the associated AP’s MAC address, use the following command:

```
Device# show wireless client mac-address 0102.0304.0506 detail
(...)
Local Roaming Client:
Client ACLs: xwf,fbs
Client State Servers: a03d.6f6b.bebe, cc16.7edc.27d8
```

Verifying Express Wi-Fi by Facebook Configurations on the AP

To view client state, use the following command:

```
Device# show flexconnect client
```

To view all ACLs applied to a specific client, use the following command:

```
Device# show client access-list {post-auth | pre-auth} all client_mac_address
Device# show client access-list post-auth all 1C:36:BB:10:1B:2C
Post-Auth URL ACLs for Client: 1C:36:BB:10:1B:2C IPv4 ACL: xwf Fbs
IPv6 ACL:
ACTION URL-LIST
allow cisco.com
allow yahoo.com
allow google.com
allow xwf.facebook.com
allow xwf-static.xx.fbcdn.net allow cisco-us.expresswifi.com allow xwf-scontent.xx.fbcdn.net
allow xwf.cisco-us.expresswifi.com
Resolved IPs for Client: 1C:36:BB:10:1B:2C HIT-COUNT URL ACTION IP-LIST
xwf
rule 0:
rule 1:
rule 2:
rule 3:
rule 4:
rule 5:
rules:
allow true and ip proto 6 and dst port 22
allow true and ip proto 6 and src port 22
allow true and dst 171.70.168.183 mask 255.255.255.255 allow true and src 171.70.168.183
mask 255.255.255.255 allow true and dst 157.240.22.50 mask 255.255.255.255 allow true and
src 157.240.22.50 mask 255.255.255.255 allow true and src 30.1.1.155 mask 255.255.255.255
and dst
30.1.1.18 mask 255.255.255.255 and ip proto 1
```
rule 7: allow true and src 30.1.1.18 mask 255.255.255.255 and dst 30.1.1.155 mask 255.255.255.255 and ip proto 1 rule 8: allow true and ip proto 17 rule 9: allow true and ip proto 17 rule 10: deny all fbs
rule 0: allow true and dst 31.13.0.0 mask 255.255.0.0
rule 1: allow true and dst 66.220.0.0 mask 255.255.0.0
rule 6: allow true and src 31.13.0.0 mask 255.255.0.0
rule 10: allow true and src 179.60.0.0 mask 255.255.0.0
rule 12: allow true and dst 171.70.168.183 mask 255.255.255.255 rule 14: allow true and ip proto 17
rule 16: deny all
No IPv6 ACL found

Device# show client access-list pre-auth all
1C:36:BB:10:1B:2C
Pre-Auth URL ACLs for Client: 1C:36:BB:10:1B:2C
IPv4 ACL: xwf
IPv6 ACL:
ACTION URL-LIST
allow cisco.com
allow yahoo.com
allow google.com
allow xwf.facebook.com
allow xwf=static.xx.fbcdn.net allow cisco-us.expresswifi.com allow xwf-scontent.xx.fbcdn.net
allow xwf=cisco-us.expresswifi.com
Resolved IPs for Client: 1C:36:BB:10:1B:2C
HIT-COUNT URL ACTION IP-LIST
xwf
rule 0: allow true and ip proto 6 and dst port 22
rule 1: allow true and ip proto 6 and src port 22
rule 2: allow true and dst 171.70.168.183 mask 255.255.255.255 rule 3: allow true and src 171.70.168.183 mask 255.255.255.255 rule 4: allow true and dst 157.240.22.50 mask 255.255.255.255 rule 5: allow true and src 157.240.22.50 mask 255.255.255.255 and dst 30.1.1.18 mask 255.255.255.255 and ip proto 1 rule 6: allow true and src 30.1.1.18 mask 255.255.255.255 and dst 30.1.1.155 mask 255.255.255.255 and ip proto 1 rule 7: allow true and dst 30.1.1.155 mask 255.255.255.255 and dst 30.1.1.155 mask 255.255.255.255 and ip proto 1 rule 8: allow true and ip proto 17 rule 9: allow true and ip proto 17 rule 10: deny all
No IPv6 ACL found
Redirect URL for client: 1C:36:BB:10:1B:2C
https://xwf=cisco-us.expresswifi.com/customer/captive_portal

To view authentication server details applied to a specific client, use the following command where the wlan_id ranges from 1 to 15:

Device# show running-config authentication dot11radio {0 | 1} wlan wlan_id

Device# show running-config authentication dot11radio {0 | 1} wlan wlan_id

Device# show controller dot11radio {0 | 1} client client_mac_address

Device# show client access-list pre-auth redirect-url 1C:36:BB:10:1B:2C

Redirect URL for client: 1C:36:BB:10:1B:2C
https://xwf=cisco-us.expresswifi.com/customer/captive_portal

To view client accounting details, use the following command:

Device# show controller dot11Radio {0 | 1} client client_mac_address

Device# show client access-list pre-auth redirect-url 1C:36:BB:10:1B:2C

Redirect URL for client: 1C:36:BB:10:1B:2C
https://xwf=cisco-us.expresswifi.com/customer/captive_portal

To view DCDS (distributed client datastore) or roaming configuration details for an associated client, use the following command:

Device# show dot11 clients data-store details client client_mac_address
Device# `show dot11 clients data-store details 1C:36:BB:10:1B:2C`

First AP Name: APF8B7.E2CC.5D48
Current AP Name: APF8B7.E2CC.5D48
Current AP IP: 30.1.1.169
Current AP BSSID: f8:b7:e2:cd:cb:8e
Current AP SSID: aa_namsoo_webauth
Client VLAN: 1
Client State: 4
Audit Session ID: 3204365612
Accounting Session ID High: 0
Accounting Session ID Low: 0
Client Traffic Class Name: xwf
Client Traffic Class Name: fbs
Verifying Express Wi-Fi by Facebook Configurations on the AP
PART XVII

Multicast Domain Name System

• Multicast Domain Name System, on page 1293
Introduction to mDNS Gateway

Bonjour protocol is an Apple service discovery protocol which locates devices and services on a local network with the use of multicast Domain Name System (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 and 120 seconds.

**Step 5** From the mDNS-AP Service Policy drop-down list, choose an mDNS service policy.

**Step 6** 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Step 2  | configure terminal | Enters global configuration mode. |
| Example:|                   |         |
| Device# configure terminal |         |         |

| Step 3  | mdns-sd gateway   | Enables mDNS gateway. |
| Example:|                   |                     |
| Device(config)# mdns-sd gateway |         |         |

| Step 4  | transport \{ipv4 | ipv6 | both\} | Processes mDNS message on a specific transport. Here, ipv4 signifies that the IPv4 mDNS message processing is enabled. This is the default value. ipv6 signifies that the IPv6 mDNS message processing is enabled. both signifies that the IPv4 and IPv6 mDNS message is enabled for each network. |
| Example:| Device(config-mdns-sd)# transport ipv4 |                     |

| Step 5  | active-query timer active-query-periodicity | Changes the periodicity of mDNS multicast active query. 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. |
| Example:| Device(config-mdns-sd)# active-query timer 15 |                     |

| Step 6  | exit           | Returns to global configuration mode. |
| Example:| Device(config-mdns-sd)# exit |                     |

## Creating Custom Service Definition (GUI)

### Procedure

**Step 1** Choose Configuration > Services > mDNS.
Creating Custom Service Definition

Service definition is a construct that provides an admin friendly name to one or more mDNS service types or 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>mdns-sd service-definition service-definition-name</td>
<td>Configures mDNS service definition.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# mdns-sd service-definition CUSTOM1</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>• All the created custom service definitions are added to the master service list.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Master service list comprises of a list of custom and built-in service definitions.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>service-type string</td>
<td>Configures mDNS service type.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-mdns-ser-def)# service-type _custom1._tcp.local</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Creating Service List (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Configuration &gt; Services &gt; mDNS.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>In the Service List section, click Add.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>In the Quick Setup: Service List page that is displayed, enter a name for the service list.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>From the Direction drop-down list, choose IN or OUT.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Click Add Services.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>From the Available Services drop-down list, choose a service type to match the service list.</td>
<td></td>
</tr>
</tbody>
</table>
| 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. |          |
| 8    | Click Save to add services. |          |
| 9    | Click Apply to Device. |          |

Creating Service List

mDNS service list is a collection of service definitions.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device&gt; enable</td>
<td>Enter your password, if prompted.</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>mdns-sd service-list service-list-name {IN</td>
<td></td>
</tr>
</tbody>
</table>
  OUT} | Configures mDNS service list.  
  - IN: Provides inbound filtering. |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Device(config)# mdns-sd service-list Basic-In IN Device(config)# mdns-sd service-list Basic-Out OUT</td>
<td>• Out: Provides outbound filtering.</td>
</tr>
</tbody>
</table>

**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 master 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**

**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

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td>Enter your password, if prompted.</td>
</tr>
</tbody>
</table>

### Step 2

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

### Step 3

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>mdns-sd service-policy</td>
<td>Enables mDNS service policy.</td>
</tr>
<tr>
<td>service-policy-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# mdns-sd service-policy</td>
</tr>
<tr>
<td></td>
<td>mdns-policy1</td>
</tr>
</tbody>
</table>

### Step 4

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>location {lss</td>
<td>site-tag}</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-mdns-ser-pol)# location</td>
</tr>
<tr>
<td></td>
<td>lss</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>service-list service-list-name {IN</td>
<td>OUT}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
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).

**Note**

Returns to global configuration mode.

### Configuring a Local or Native Profile for an mDNS Policy

The following procedure shows how to configure a local or native profile for an mDNS policy from the service-template:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>service-template template-name</code></td>
<td>Configures the service-template or identity policy.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# service-template mdns</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>mdns-service-policy mdns-policy-name</code></td>
<td>Configures the mDNS policy.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-service-template)# mdns-service-policy mdnsTV</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>exit</code></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-service-template)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Enabling the mDNS Gateway on the VLAN Interface

By configuring a service policy on the VLAN interface, you can configure the mDNS service policy for a specific VLAN.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures a VLAN ID and enters interface configuration mode.</td>
</tr>
<tr>
<td>interface vlan vlan-interface-number</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface vlan 200</td>
<td>Configures a VLAN ID and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the IP address for the interface.</td>
</tr>
<tr>
<td>ip address ip-address subnet-mask</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ip address 111.1.1 255.255.255.0</td>
<td>Configures the IP address for the interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables mDNS configuration on a VLAN interface.</td>
</tr>
<tr>
<td>mdns-sd gateway</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# mdns-sd gateway</td>
<td>Enables mDNS configuration on a VLAN interface.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures the service policy.</td>
</tr>
<tr>
<td>service-policy service-policy-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if-mdns-sd)# service-policy mdns-service-policy-name</td>
<td>Configures the service policy.</td>
</tr>
<tr>
<td>Note</td>
<td>Use the default service policy name, if the service-policy-name is not defined.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if-mdns-sd)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Location-Based Service Filtering

**Prerequisite for Location-Based Service Filtering**

You need to create the Service Definition and Service Policy. For more information, see Creating Custom Service Definition section and Creating Service Policy section.
Configuring mDNS Location-Based Filtering Using SSID

When a service policy is configured with the SSID as the location name, the response to the query will be the services that were learnt on that SSID.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  * configure terminal
  * **Example:**
    
    Device# configure terminal
| Enters global configuration mode. |
| **Step 2**
  * mdns-sd service-policy *service-policy-name*
  * **Example:**
    
    Device(config)# mdns-sd service-policy mdns-policy1
| Configures the service policy. |
| **Step 3**
  * location ssid
  * **Example:**
    
    Device(config-mdns-ser-pol)# location ssid
| Configures location-based filtering using SSID. |
| **Step 4**
  * end
  * **Example:**
    
    Device(config-mdns-ser-pol)# end
| Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode. |

Configuring mDNS Location-Based Filtering Using AP Name

When a service policy is configured with the AP name as the location, the response to the query will be the services that were learnt on that AP.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  * configure terminal
  * **Example:**
    
    Device# configure terminal
| Enters global configuration mode. |
| **Step 2**
  * mdns-sd service-policy *service-policy-name*
  * **Example:**
    
    Device(config)# mdns-sd service-policy mdns-policy1
| Configures the service policy. |
| **Step 3**
  * location ap-name
  * **Example:**
    
    Device(config-mdns-ser-pol)# location ap-name
| Configures location-based filtering using an AP name. |
Configuring mDNS Location-Based Filtering Using AP Location

When a service policy is configured with location as the AP-location, the response to the query will be the services that were learnt on all the APs using the same AP "location" name (not to be confused with "site-tag").

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures the service policy.</td>
</tr>
<tr>
<td><code>mdns-sd service-policy service-policy-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# mdns-sd service-policy mdns-policy1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures location-based filtering using the AP location.</td>
</tr>
<tr>
<td><code>location ap-location</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-mdns-ser-pol)# location ap-location</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-mdns-ser-pol)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
</tbody>
</table>

Configuring mDNS Location-Based Filtering Using Regular Expression

- When a service policy is configured with the location as a regular expression that matches the corresponding AP name, the response to the query will be the services that were learnt on a group of APs based on the AP name.
- When a service policy is configured with the location as a regular expression that matches the corresponding AP location, the response to the query will be the services that were learnt on a group of APs based on the AP location.
## Configuring an mDNS AP

In most of the deployments, the services may be available in VLANs that the APs can hear in the wired side (allowed in the switchport where the AP is directly connected: its own VLAN, or even more VLANs if switchport is a trunk).

The following procedure shows how to configure mDNS AP:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> mdns-sd service-policy <em>service-policy-name</em></td>
<td>Configures the service policy.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# mdns-sd service-policy mdns-policy1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> location regex {ap-location <em>regular-expression</em></td>
<td>Configures location-based filtering using regular expression.</td>
</tr>
<tr>
<td></td>
<td>ap-name <em>regular-expression</em>}</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-mdns-ser-pol)# location regex ap-location dns_location</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-mdns-ser-pol)# location regex ap-name dns_name</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-mdns-ser-pol)# end</td>
<td></td>
</tr>
</tbody>
</table>
### Enabling mDNS Gateway on the RLAN Interface

By configuring the mDNS gateway mode on the RLAN interface, you can configure the mDNS service policy for a specific RLAN.

#### Procedure

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures a remote LAN profile.</td>
</tr>
<tr>
<td><code>ap remote-lan profile-name</code></td>
<td></td>
</tr>
<tr>
<td><code>remote-lan-profile-name rlan-id</code></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# ap remote-lan profile-name rlan_test_1 1</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note** You can create a maximum of 128 RLANs. Also, you cannot use the `rlan-id` of an existing RLAN while creating another RLAN.
### Enabling mDNS Gateway on the RLAN Interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>mdns-sd gateway</td>
<td>Enables mDNS configuration on an RLAN interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-remote-lan)# mdns-sd gateway</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>no shutdown</td>
<td>Restarts the RLAN profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-remote-lan)# no shutdown</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>exit</td>
<td>Exits remote LAN configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-remote-lan)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>ap remote-lan-policy policy-name <em>profile name</em></td>
<td>Configures the RLAN policy profile and enters wireless policy configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ap remote-lan-policy policy-name rlan_named_pp1</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>shutdown</td>
<td>Restarts the RLAN policy profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-remote-lan-policy)# shutdown</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>mdns-sd service-policy <em>service-policy-name</em></td>
<td>Enables an mDNS service policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-remote-lan-policy)# mdns-sd service-policy mdnsTV6</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td>central switching</td>
<td>Configures the RLAN for central switching.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-remote-lan-policy)# central switching</td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>central dhcp</td>
<td>Configures the central DHCP for centrally switched clients.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-remote-lan-policy)# central dhcp</td>
<td></td>
</tr>
<tr>
<td>Step 11</td>
<td>vlan <em>vlan-name</em></td>
<td>Assigns the profile policy to a VLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-remote-lan-policy)# vlan 141</td>
<td></td>
</tr>
<tr>
<td>Step 12</td>
<td>no shutdown</td>
<td>Restarts the RLAN profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Device(config-remote-lan-policy)# no shutdown</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>wireless tag policy <em>policy-tag-name</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# wireless tag policy rlan_pt_1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configures a policy tag.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>remote-lan <em>remote-lan-profile-name</em> policy <em>rlan-policy-profile-name</em> port-<em>id</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-policy-tag)# remote-lan rlan_test_1 policy rlan_named_pp1 port-id 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-policy-tag)# remote-lan rlan_test_1 policy rlan_named_pp1 port-id 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-policy-tag)# remote-lan rlan_test_1 policy rlan_named_pp1 port-id 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-policy-tag)# remote-lan rlan_test_1 policy rlan_named_pp1 port-id 4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maps the RLAN policy profile to the RLAN profile.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <em>remote-lan-profile-name</em>: Name of the RLAN profile.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <em>rlan-policy-profile-name</em>: Name of the policy profile.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <em>port-id</em>: LAN port number on the access point. Range is from 1 to 4.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td>exit</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-policy-tag)# exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Returns to global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td>ap <em>mac-address</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device (config)# ap 0042.5AB6.0EF0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configures the AP and enters the AP tag configuration mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>Use the Ethernet MAC address.</td>
</tr>
<tr>
<td><strong>Step 17</strong></td>
<td>policy-tag <em>policy-tag-name</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device (config-ap-tag)# policy-tag rlan_pt_1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maps a policy tag to the AP.</td>
<td></td>
</tr>
</tbody>
</table>

### Enabling mDNS Gateway on Guest LAN Interface

By configuring the mDNS gateway mode on a Guest LAN interface, you can configure the mDNS service policy for a specific Guest LAN interface.
## Associating mDNS Service Policy with Wireless Profile Policy

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>guest-lan profile-name guest_lan_profile_name num wired-vlan wired_vlan_num</code></td>
<td>Configures guest LAN profile with a wired VLAN.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Configures the wired VLAN only for the Guest Foreign controller.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# guest-lan profile-name open 1 wired-vlan 666</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>guest-lan profile-name guest_lan_profile_name num</code></td>
<td>Configures the guest LAN profile without a VLAN for the Guest Anchor controller.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# guest-lan profile-name open 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>mdns-sd gateway</code></td>
<td>Configures the mDNS gateway for a Guest LAN.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You need to enable mDNS gateway globally for the Guest LAN to work.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-guest-lan)# mdns-sd gateway</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-guest-lan)# end</td>
<td>Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
</tbody>
</table>
### Procedure

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

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>wireless profile policy <strong>profile-policy</strong></td>
<td>Configures wireless profile policy.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# wireless profile policy default-policy-profile</td>
<td>Here, <strong>profile-policy</strong> refers to the name of the WLAN policy profile.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mdns-sd service-policy <strong>custom-mdns-service-policy</strong></td>
<td>Associates an mDNS service policy with the wireless profile policy.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-wireless-policy)# mdns-sd service-policy custom-mdns-service-policy</td>
<td>The default mDNS service policy name is <strong>default-mdns-service-policy</strong>.</td>
</tr>
</tbody>
</table>
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 60: Default Name and mDNS Service Type

<table>
<thead>
<tr>
<th>Default Name</th>
<th>mDNS Service Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airplay</td>
<td>_airplay._tcp.local</td>
</tr>
<tr>
<td>AirTunes</td>
<td>_raop._tcp.local</td>
</tr>
<tr>
<td>HomeSharing</td>
<td>_home-sharing._tcp.local</td>
</tr>
<tr>
<td>Printer-LPD</td>
<td>_printer._tcp.local</td>
</tr>
<tr>
<td>Printer-IPP</td>
<td>_ipp._tcp.local</td>
</tr>
<tr>
<td>Printer-IPPS</td>
<td>_ipps._tcp.local</td>
</tr>
<tr>
<td>Printer-socket</td>
<td>_pdl-datastream._tcp.local</td>
</tr>
<tr>
<td>Googlecast</td>
<td>_googlecast._tcp.local</td>
</tr>
<tr>
<td>TimedSignal2</td>
<td>_applmbdx2._tcp.local</td>
</tr>
</tbody>
</table>
### Enabling or Disabling mDNS Gateway for WLAN

Bridging is the default behaviour. This means that the mDNS packets are always bridged.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wlan profile-name wlan-id ssid-name</td>
<td>Specifies the WLAN name and ID.</td>
</tr>
<tr>
<td>Example: Device(config)# wlan test 24 ssid1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>Global configuration must be in place for mDNS gateway to work.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>mdns-sd {gateway</td>
<td>drop}</td>
</tr>
<tr>
<td>Example: Device(config-wlan)# mdns-sd gateway</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 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.

### Configuring mDNS Gateway on Guest Anchor (Guest LAN)

**Procedure**

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures the guest LAN profile with a wired VLAN.</td>
</tr>
<tr>
<td>guest-lan profile-name guest-lan-profile-name guest-lan-id</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# guest-lan profile-name g-lanpro 2</td>
</tr>
</tbody>
</table>
### Configuring mDNS Gateway on Guest Foreign (Guest LAN)

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>guest-lan profile-name guest-lan-profile-name guest-lan-id wired-vlan vlan-id</td>
<td>Configures guest LAN profile with a wired VLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# guest-lan profile-name g-lanpro 2 wired-vlan 230</td>
<td><strong>Note</strong> Configure the wired VLAN only for the Guest Foreign controller.</td>
</tr>
<tr>
<td>Step 3</td>
<td>mdns-sd gateway</td>
<td>Enables mDNS gateway on the guest LAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-guest-lan)# mdns-sd gateway</td>
<td></td>
</tr>
</tbody>
</table>

#### 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

<table>
<thead>
<tr>
<th>RECORD-NAME</th>
<th>TTL</th>
<th>WLAN</th>
<th>CLIENT-MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>_airplay._tcp.local</td>
<td>4500</td>
<td>30</td>
<td>07c5.a4f2.dc01</td>
</tr>
<tr>
<td>CUST1._airplay._tcp.local</td>
<td>4500</td>
<td>30</td>
<td>04c5.a4f2.dc01</td>
</tr>
<tr>
<td>_ipp._tcp.local</td>
<td>4500</td>
<td>15</td>
<td>04c5.a4f2.dc01</td>
</tr>
</tbody>
</table>
To verify the mDNS cache from wired service provider, use the following command:

```
Device# show mdns-sd cache wired
```

### PTR Records

<table>
<thead>
<tr>
<th>RECORD-NAME</th>
<th>TTL</th>
<th>VLAN</th>
<th>CLIENT-MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>_airplay._tcp.local</td>
<td>4500</td>
<td>16</td>
<td>0866.98ec.97af</td>
</tr>
<tr>
<td>wiredapple._airplay._tcp.local</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>_raop._tcp.local</td>
<td>4500</td>
<td>16</td>
<td>0866.98ec.97af</td>
</tr>
<tr>
<td>086698EC97AF@wiredapple._raop._tcp.local</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### SRV Records

<table>
<thead>
<tr>
<th>RECORD-NAME</th>
<th>TTL</th>
<th>VLAN</th>
<th>CLIENT-MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>wiredapple._airplay._tcp.local</td>
<td>4500</td>
<td>16</td>
<td>0866.98ec.97af</td>
</tr>
<tr>
<td>wiredapple.local</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>086698EC97AF@wiredapple._raop._tcp.local</td>
<td>4500</td>
<td>16</td>
<td>0866.98ec.97af</td>
</tr>
<tr>
<td>wiredapple.local</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### A/AAAA Records

<table>
<thead>
<tr>
<th>RECORD-NAME</th>
<th>TTL</th>
<th>VLAN</th>
<th>CLIENT-MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>wiredapple.local</td>
<td>4500</td>
<td>16</td>
<td>0866.98ec.97af</td>
</tr>
</tbody>
</table>

### TXT Records

<table>
<thead>
<tr>
<th>RECORD-NAME</th>
<th>TTL</th>
<th>VLAN</th>
<th>CLIENT-MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>wiredapple._airplay._tcp.local</td>
<td>4500</td>
<td>16</td>
<td>0866.98ec.97af</td>
</tr>
<tr>
<td>(343)'acl=0'deviceid=08:66:98:EC:97:AF'features=086698EC97AF@wiredapple._raop._tcp.local</td>
<td>4500</td>
<td>16</td>
<td>0866.98ec.97af</td>
</tr>
<tr>
<td>(193)'cn=0,1,2,3'da-true'et=0,3,5*ft=0x5A7FFFFF7</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To verify the mdns-sd type PTR, use the following command:

```
Device# show mdns-sd cache type {PTR | SRV | A-AAA | TXT}
```

### Record-Name

<table>
<thead>
<tr>
<th>RECORD-NAME</th>
<th>TTL</th>
<th>VLAN</th>
<th>CLIENT-MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>_custom1._tcp.local</td>
<td>4500</td>
<td>2</td>
<td>c869.cda8.77d6</td>
</tr>
<tr>
<td>service_t1._custom1._tcp.local</td>
<td>4500</td>
<td>2</td>
<td>c869.cda8.77d6</td>
</tr>
<tr>
<td>_ipp._tcp.local</td>
<td>4500</td>
<td>2</td>
<td>c869.cda8.77d6</td>
</tr>
</tbody>
</table>

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> | glan-id <glan-id> | mdns-ap <mac-address> | rlan-id <rlan-id> | wlan-id <wlan-id> | wired}\n```

### Record-Name

<table>
<thead>
<tr>
<th>RECORD-NAME</th>
<th>TTL</th>
<th>VLAN</th>
<th>CLIENT-MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>_ipp._tcp.local</td>
<td>4500</td>
<td>2</td>
<td>c869.cda8.77d6</td>
</tr>
</tbody>
</table>
### SRV Records

<table>
<thead>
<tr>
<th>RECORD-NAME</th>
<th>TTL</th>
<th>WLAN</th>
<th>CLIENT-MAC</th>
<th>RR-Record-Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>service-4._ipp._tcp.local</td>
<td>4500</td>
<td>2</td>
<td>c869.cda8.77d6</td>
<td>0 0 1212</td>
</tr>
<tr>
<td>mDNS-Client1s-275.local</td>
<td>4500</td>
<td>2</td>
<td>c869.cda8.77d6</td>
<td>0 0 987</td>
</tr>
<tr>
<td>service_t1._custom1._tcp.local</td>
<td>4500</td>
<td>2</td>
<td>c869.cda8.77d6</td>
<td>0 0 197</td>
</tr>
<tr>
<td>mDNS-Client1s-275.local</td>
<td>4500</td>
<td>2</td>
<td>c869.cda8.77d6</td>
<td>120.1.1.33</td>
</tr>
</tbody>
</table>

### A/AAAA Records

<table>
<thead>
<tr>
<th>RECORD-NAME</th>
<th>TTL</th>
<th>WLAN</th>
<th>CLIENT-MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>mDNS-Client1s-275.local</td>
<td>4500</td>
<td>2</td>
<td>c869.cda8.77d6</td>
</tr>
</tbody>
</table>

### TXT Records

<table>
<thead>
<tr>
<th>RECORD-NAME</th>
<th>TTL</th>
<th>WLAN</th>
<th>CLIENT-MAC</th>
<th>RR-Record-Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>service-4._ipp._tcp.local</td>
<td>4500</td>
<td>2</td>
<td>c869.cda8.77d6</td>
<td>'Client1'</td>
</tr>
<tr>
<td>vk11._custom1._tcp.local</td>
<td>4500</td>
<td>2</td>
<td>c869.cda8.77d6</td>
<td>'txtvers=11'</td>
</tr>
<tr>
<td>service_t1._custom1._tcp.local</td>
<td>4500</td>
<td>2</td>
<td>c869.cda8.77d6</td>
<td>'txtvers=12'</td>
</tr>
</tbody>
</table>

To verify the mDNS-SDCache with respect to the RLAN ID, use the following command:

```
Device# show mdns-sd cache rlan-id 1 detail
```

Name: _printer._tcp.local

Type: PTR

TTL: 4500

RLAN: 1

RLAN Name: rlan_test_1

VLAN: 141

Client MAC: 00e.e688.3942

AP Ethernet MAC: 0042.5ab6.0ef0

Remaining-Time: 4485

Site-Tag: default-site-tag

mDNS Service Policy: mdnsTV6
Overriding mDNS Service Policy: NO
UPN-Status: Disabled
Rdata: printer._printer._tcp.local

Name: lab-47-187.local
Type: A/AAAA
TTL: 4500
RLAN: 1
RLAN Name: rlan_test_1
VLAN: 141
Client MAC: 000e.c688.3942
AP Ethernet MAC: 0042.5ab6.0ef0
Remaining-Time: 4485
Site-Tag: default-site-tag
mDNS Service Policy: mdnsTV6
Overriding mDNS Service Policy: NO
UPN-Status: Disabled
Rdata: 10.15.141.124

Name: printer._printer._tcp.local
Type: TXT
TTL: 4500
RLAN: 1
RLAN Name: rlan_test_1
VLAN: 141
Client MAC: 000e.c688.3942
AP Ethernet MAC: 0042.5ab6.0ef0
Remaining-Time: 4485
Site-Tag: default-site-tag
mDNS Service Policy: mdnsTV6
Overriding mDNS Service Policy: NO
UPN-Status: Disabled
To verify the mDNS cache with respect to mDNS-AP, use the following command:

```
Device# show mdns-sd cache mdns-ap 706b.b97d.b060 detail
```

**Name: _printer._tcp.local**

- **Type:** PTR
- **TTL:** 4500
- **VLAN:** 145
- **Client MAC:** 0050.b626.5bfa
- **mDNS AP Radio MAC:** 706b.b97d.b060
- **mDNS AP Ethernet MAC:** 706b.b97c.5208
- **Remaining-Time:** 4480
- **mDNS Service Policy:** mdnsTV

**Rdata:** printer._printer._tcp.local

**Name: Client-46-153.local**

- **Type:** A/AAAA
- **TTL:** 4500
- **VLAN:** 145
- **Client MAC:** 0050.b626.5bfa
- **mDNS AP Radio MAC:** 706b.b97d.b060
- **mDNS AP Ethernet MAC:** 706b.b97c.5208
- **Remaining-Time:** 4480
- **mDNS Service Policy:** mdnsTV

**Rdata:** 10.15.145.103

**Name: printer._printer._tcp.local**

- **Type:** TXT
- **TTL:** 4500
- **VLAN:** 145
- **Client MAC:** 0050.b626.5bfa
- **mDNS AP Radio MAC:** 706b.b97d.b060
- **mDNS AP Ethernet MAC:** 706b.b97c.5208
Verifying mDNS Gateway Configurations

Remaining-Time: 4480

mDNS Service Policy: mdnsTV

Rdata: [1]''

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 cache statistics, use the following command:

Device# show mdns-sd cache statistics
mDNS Cache Stats

Total number of Services: 4191

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
   - 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: 32134
     - 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: 232
     - 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

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 master 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: apple-rdp
Service Names: _afpovertcp._tcp.local
  _net-assistant._tcp.local

Service Definition: web-server
Service Names: _http._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: workstation
Service Names: _workstation._tcp.local

Service Definition: printer-ipps
Service Names: _ipps._tcp.local

Service Definition: apple-homekit
Service Names: _hap._tcp.local
  _homekit._ipp.local
Service Definition: apple-keynote
Service Names: _keynotecontrol._tcp.local
    _keynotepair._tcp.local

Service Definition: amazon-fire-tv
Service Names: _amzn-wplay._tcp.local

Service Definition: apple-airprint
Service Names: _ipp._tcp.local
    _universal._sub._ipp._tcp.local

Service Definition: printer-socket
Service Names: _pdl-datastream._tcp.local

Service Definition: apple-continuity
Service Names: _companion-link._tcp.local

Service Definition: apple-file-share
Service Names: _afpovertcp._tcp.local

Service Definition: apple-timecapsule
Service Names: _adisk._tcp.local
    _afpovertcp._tcp.local

Service Definition: google-chromecast
Service Names: _googlecast._tcp.local

Service Definition: apple-itunes-music
Service Names: _daap._tcp.local

Service Definition: apple-itunes-photo
Service Names: _dpap._tcp.local

Service Definition: apple-remote-login
Service Names: _sftp-ssh._tcp.local
    _ssh._tcp.local

Service Definition: apple-screen-share
Service Names: _rfb._tcp.local

Service Definition: apple-remote-events
Service Names: _eppc._tcp.local

Service Definition: phillips-hue-lights
Service Names: _hap._tcp.local

Service Definition: apple-itunes-library
Service Names: _atc._tcp.local

Service Definition: multifunction-printer
Service Names: _fax-ipp._tcp.local
    _ipp._tcp.local
    _scanner._tcp.local

Service Definition: apple-timecapsule-mgmt
Service Names: _airport._tcp.local

Service Definition: apple-windows-fileshare
Service Names: _smb._tcp.local

Service Definition: itune-wireless-devicesharing2
Service Names: _apple-mobdev2._tcp.local

To verify the mDNS-SD service statistics on the controller, use the following command:
Device# `show mdns-sd service statistics`

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Service Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>_atc._tcp.local</td>
<td>137</td>
</tr>
<tr>
<td>_hap._tcp.local</td>
<td>149</td>
</tr>
<tr>
<td>_ipp._tcp.local</td>
<td>149</td>
</tr>
<tr>
<td>_rfb._tcp.local</td>
<td>141</td>
</tr>
<tr>
<td>_smb._tcp.local</td>
<td>133</td>
</tr>
<tr>
<td>_ssh._tcp.local</td>
<td>142</td>
</tr>
<tr>
<td>_daap._tcp.local</td>
<td>149</td>
</tr>
<tr>
<td>_dpap._tcp.local</td>
<td>149</td>
</tr>
<tr>
<td>_eppc._tcp.local</td>
<td>138</td>
</tr>
<tr>
<td>_adisk._tcp.local</td>
<td>149</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Ethernet MAC</th>
<th>Number of Vlans</th>
<th>Vlan Identifiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP3600-1</td>
<td>7069.5ab8.33d0</td>
<td>1</td>
<td>300</td>
</tr>
</tbody>
</table>

**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 platform software trace message wncd <0-7> chassis active R0
   ```