Aruba Instant 8.7.0.x User Guide



a Hewlett Packard Enterprise company

User Guide

Copyright Information

© Copyright 2023 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Contents ... 3

Revision History ... 9

About this Guide ... 10
- Intended Audience ... 10
- Related Documents ... 10
- Conventions ... 10
- Contacting Support ... 11

About Aruba Instant ... 12
- Instant Overview ... 12
- What is New in the Release ... 15

Setting up an Instant AP ... 19
- Setting up Instant Network ... 19
  - Connecting to a Provisioning Wi-Fi Network ... 21
  - Instant AP Cluster ... 21
  - Disabling the Provisioning Wi-Fi Network ... 21
  - Disabling Activate Communication with Instant AP for Provisioning ... 22
  - Prerequisites for Obtaining the Cloud Activation Key ... 23
  - Viewing the Cloud Activation Key Using the Old WebUI ... 23
  - Viewing the Cloud Activation Key Using the New WebUI ... 24
- Logging in to the Instant UI ... 24
- Accessing the Instant CLI ... 25
- Instant AP Degraded State ... 28

Automatic Retrieval of Configuration ... 29
- Managed Mode Operations ... 29
- Prerequisites ... 29
- Configuring Managed Mode Parameters ... 29
- Verifying the Configuration ... 31

Instant New User Interface ... 32
- Introduction ... 32
- Login Screen ... 32
- Main Window ... 33
- InstantOld User Interface ... 42
  - Tunneling ... 48
  - Routing ... 48
  - IDS ... 48
  - Wired ... 48
  - Services ... 48
  - DHCP Server ... 49
  - Support ... 49
  - Info ... 50

RF Dashboard ... 52
RF Trends ... 53
Usage Trends ... 54
Mobility Trail ... 57

Initial Configuration Tasks ... 64
Configuring System Parameters (Old WebUI) ... 64
Configuring System Parameters (New WebUI) ... 73
Changing Password ... 76

Customizing Instant AP Settings ... 78
Discovery Logic ... 78
Modifying the Instant AP Host Name ... 84
Configuring Zone Settings on an Instant AP ... 84
Disabling AP Factory Reset ... 87
AP USB Management ... 87
Specifying a Method for Obtaining IP Address ... 92
Configuring External Antenna ... 93
Configuring Radio Profiles for an Instant AP ... 94
Enabling Flexible Radio ... 96
Enabling Low Power Mode ... 97
Dual 5 GHz Radio Mode ... 97
Split 5 GHz Radio for 550 Series Access Points ... 98
Air Slice ... 100
Support for Input-Filter on BLE Devices ... 102
Configuring Uplink VLAN for an Instant AP ... 103
Changing the Instant AP Installation Mode ... 103
Changing USB Port Status ... 104
Master Election and Virtual Controller ... 105
Adding an Instant AP to the Network ... 107
Removing an Instant AP from the Network ... 107
Support for BLE Asset Tracking ... 107
IoT Endpoints ... 108
Zigbee-Based IoT ... 109
Zigbee Sockets ... 112
Zigbee Service Profile ... 112
Aruba Sensor Values ... 112
Reporting Sensor Values ... 113
HanVit Sensors ... 114
SoluM ESL Gateway ... 114
Hanshow ESL Gateway ... 115
ZF Openmatics Support for ZF BLE Tag Communication ... 115
IoT Data Filter ... 117
Wiliot Sensors ... 118
Southbound API ... 119
Intelligent Power and Temperature Monitoring ... 119
Transmit Power Calculation Support on 200 Series and 300 Series Access Points ... 122
Hardware Offloading for Increased Transmission Performance ... 122

VLAN Configuration ... 124
VLAN Pooling ... 124
Uplink VLAN Monitoring and Detection on Upstream Devices ... 124
Multiple Management Interface ... 124

IPv6 Support ... 126
IPv6 Notation ... 126

Enabling IPv6 Support for Instant AP Configuration 126
Firewall Support for IPv6 128
GRE Backup Tunnel 128
Debugging Commands 129

Wireless Network Profiles 130
Configuring Wireless Network Profiles 130
Points to Remember 145
MPSK Cache 146
Fast Roaming for Wireless Clients 148
Configuring Modulation Rates on a WLAN SSID 153
Multi-User-MIMO 153
Management Frame Protection 154
High Efficiency WLAN (HEW) 154
Multi Band Operation (MBO) 155
Disabling Short Preamble for Wireless Client 156
Disabling a WLAN SSID Profile 156
Editing a WLAN SSID Profile 157
Deleting a WLAN SSID Profile 157
Enhancements to WLAN SSID Configuration 157
Wireless Client Bridge 159

Wired Profiles 161
Configuring a Wired Profile 161
In the Old WebUI 165
In the New WebUI 166
In the CLI 167
Assigning a Profile to Ethernet Ports 170
Enabling 802.3az Energy Efficient Ethernet Standard 170
Editing a Wired Profile 171
Deleting a Wired Profile 171
LACP 172
Understanding Hierarchical Deployment 173
Loop Protection 174

Captive Portal for Guest Access 176
Understanding Captive Portal 176
Configuring a WLAN SSID for Guest Access 177
Configuring Wired Profile for Guest Access 183
IGMP 186
Configuring Internal Captive Portal for Guest Network 186
Configuring External Captive Portal for a Guest Network 189
Configuring External Captive Portal Authentication Using ClearPass Guest 194
Configuring Facebook Login 196
Configuring Guest Logon Role and Access Rules for Guest Users 198
Configuring Captive Portal Roles for an SSID 200
Configuring Walled Garden Access 202
Disabling Captive Portal Authentication 203
Configuring Facebook Express Wi-Fi 203

Authentication and User Management 207
Overview of Instant AP Users 207
Supported Authentication Methods 212
Supported EAP Authentication Frameworks 224
Supported Authentication Servers 225

Configuring Authentication Servers ... 231
Supported Encryption Types ... 242
Authentication Survivability ... 243
WPA3 Security ... 246
802.1X Supplicant Support ... 250
Blacklisting Clients ... 251
Authentication Certificates ... 254

Roles and Policies ... 259
Firewall Policies ... 259
Content Filtering ... 273
Configuring User Roles ... 277
Configuring Derivation Rules ... 282
Downloadable User Roles ... 293

DHCP Configuration ... 294
Configuring DHCP Scopes ... 294
In the Old WebUI ... 298
In the New WebUI ... 298
In the CLI ... 298
Configuring the Default DHCP Scope for Client IP Assignment ... 309

Configuring Time-Based Services ... 312
Time Range Profiles ... 312
Configuring a Time Range Profile ... 313
Applying a Time Range Profile to a WLAN SSID ... 314
Verifying the Configuration ... 315
Applying a Time Range Profile to a Role ... 316

VPN Configuration ... 317
Understanding VPN Features ... 317
Configuring a Tunnel from an Instant AP to a Mobility Controller ... 319
Configuring Routing Profiles ... 328
Dynamic DNS Registration ... 329

IAP-VPN Deployment ... 332
Understanding IAP-VPN Architecture ... 332
Configuring Instant AP and Controller for IAP-VPN Operations ... 336
IAP-VPN Deployment Scenarios ... 346

Adaptive Radio Management ... 369
ARM Overview ... 369
Configuring ARM Features on an Instant AP ... 370
Configuring Radio Settings ... 377

DPI and Application Visibility ... 382
DPI ... 382
Enabling Application Visibility ... 382
Application Visibility ... 383
Enabling URL Visibility ... 383
Configuring ACL Rules for Application and Application Categories ... 384
Configuring Web Policy Enforcement Service ... 387

Voice and Video ... 391
WMM Traffic Management ... 391
Media Classification for Voice and Video Calls ... 394

WebRTC Prioritization ... 396
Enabling Enhanced Voice Call Tracking ... 396
Wi-Fi Calling ... 397
Unified Communications Manager ... 397

Services ... 399
Configuring AirGroup ... 399
Configuring an Instant AP for RTLS Support ... 408
Configuring an Instant AP for ALE Support ... 410
Clarity Live ... 411
Deny Intra-VLAN Traffic ... 413
Integrating an Instant AP with Palo Alto Networks Firewall ... 414
Integrating an Instant AP with an XML API Interface ... 415
SES-imagotag ESL System ... 418
CALEA Integration and Lawful Intercept Compliance ... 419
BLE IoT for Data Communication ... 424

SDN ... 430
Functionalities of SDN ... 430
OpenFlow for WLAN ... 430
Clickstream Analysis ... 432
Wildcard ACL Support ... 432

Cluster Security ... 434
Cluster Security Using DTLS ... 434
Locked Mode Slave Instant AP ... 434
Enabling Cluster Security ... 435
ZTP with Cluster Security ... 435
Low Assurance Devices ... 436
Cluster Security Debugging Logs ... 437
Verifying the Configuration ... 438

Instant AP Management and Monitoring ... 439
Managing an Instant AP from AirWave ... 439
Managing Instant AP from Aruba Central ... 449
WebSocket Connection ... 452
Support for REST API ... 453

Uplink Configuration ... 454
Uplink Interfaces ... 454
Ethernet Uplink ... 454
Cellular Uplink ... 457
Wi-Fi Uplink ... 459
Uplink Preferences and Switching ... 462

Intrusion Detection ... 469
Detecting and Classifying Rogue APs ... 469
OS Fingerprinting ... 469
Configuring WIP and Detection Levels ... 470
Configuring IDS ... 474

Mesh Instant AP Configuration ... 476
Mesh Network Overview ... 476
Setting up Instant Mesh Network ... 478
Configuring Wired Bridging on Ethernet 0 for Mesh Point ... 479
Mesh Cluster Function ... 479
Radio Selection for Mesh Links ... 481

Fast Roaming with Mesh Access Points ... 481

Mobility and Client Management ... 483
Layer-3 Mobility Overview ... 483
Configuring Layer-3 Mobility ... 484

Spectrum Monitor ... 486
Understanding Spectrum Data ... 486
In the New WebUI ... 490
Configuring Spectrum Monitors and Hybrid Instant APs ... 493

Instant AP Maintenance ... 497
Generating Default Certificates ... 497
Backing up and Restoring Instant AP Configuration Data ... 498
Converting an Instant AP to a Remote AP and Campus AP ... 499
Resetting a Remote AP or Campus AP to an Instant AP ... 503
Rebooting the Instant AP ... 503
DRT Upgrade ... 504

Monitoring Devices and Logs ... 506
Configuring SNMP ... 506
Configuring Syslog Servers ... 509
Configuring TFTP Dump Server ... 511
Running Debug Commands ... 511
Uplink Bandwidth Monitoring ... 515
WAN Link Health Monitoring ... 516

Hotspot Profiles ... 519
Understanding Hotspot Profiles ... 519
Configuring Hotspot Profiles ... 521
Downloading Icon Files to Instant AP ... 528
Configuring OSU Provider Profile Parameters ... 528
Sample Configuration ... 538

Mobility Access Switch Integration ... 542
Mobility Access Switch Overview ... 542
Configuring Instant APs for Mobility Access Switch Integration ... 543

ClearPass Guest Setup ... 544
Configuring ClearPass Guest ... 544
Verifying ClearPass Guest Setup ... 548
Troubleshooting ... 548

Glossary of Terms ... 550

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 09	Added the note in the **802.1X Supplicant Support** chapter.
Revision 08	Added a note on GRE tunnel configuration in a cluster setups.
Revision 07	The following updates were added: ■ Updated the maximum no of user roles to 64 in the Roles and Policies chapter. ■ Corrected the **show app-monitoring list** syntax in the Air Slice topic. ■ Added **Mesh Network with Mixed Indoor and Outdoor APs** topic in the Mesh Network chapter.
Revision 06	Removed all instances of Certification Enrollment Using EST.
Revision 05	**Configuring Facebook Express Wi-Fi** topic was added.
Revision 04	Made minor edits to the Understanding Hierarchical Deployment section.
Revision 03	■ Added a note on platforms that do not support bandwidth share percentage configuration for WMM traffic management in the Voice and Video chapter. ■ Removed the **tpm** parameter from the AP1X configuration setting.
Revision 02	Removed references to Fremont Sensors.
Revision 01	Initial release.

Chapter 1
About this Guide

This User Guide describes the features supported by Aruba Instant and provides detailed instructions for setting up and configuring the Instant network.

Intended Audience

This guide is intended for administrators who configure and use Instant APs.

Related Documents

In addition to this document, the Instant AP product documentation includes the following:

- Aruba Instant Access Point Installation Guides
- Aruba Instant CLI Reference Guide
- Aruba Instant Quick Start Guide
- Aruba Instant Release Notes
- Aruba Instant REST API Guide

Conventions

The following conventions are used throughout this manual to emphasize important concepts:

Table 2: *Typographical Conventions*

Style Type	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: ■ Sample screen output ■ System prompts ■ Filenames, software devices, and specific commands when mentioned in the text.
`Commands`	In the command examples, this style depicts the keywords that must be typed exactly as shown.
<Arguments>	In the command examples, italicized text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: `# send <text message>` In this example, you would type “send” at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.

Table 2: *Typographical Conventions*

Style Type	Description
`[Optional]`	Command examples enclosed in square brackets are optional. Do not type the square brackets.
`{Item A | Item B}`	In the command examples, items within curly brackets and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the curly brackets or bars.

The following informational icons are used throughout this guide:



Indicates helpful suggestions, pertinent information, and important things to remember.



Indicates a risk of damage to your hardware or loss of data.



Indicates a risk of personal injury or death.

Contacting Support

Table 3: *Contact Information*

Main Site	arubanetworks.com
Support Site	https://asp.arubanetworks.com/
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	lms.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

About Aruba Instant

This chapter provides the following information:

- Instant Overview on page 12
- What is New in the Release on page 15

Instant Overview

Instant virtualizes Aruba Mobility Controller capabilities on 802.1 capable access points creating a feature-rich enterprise-grade WLAN that combines affordability and configuration simplicity.

Instant is a simple, easy to deploy turnkey WLAN solution consisting of one or more Instant Access Points. An Ethernet port with routable connectivity to the Internet or a self-enclosed network is used for deploying an Instant Wireless Network. An Instant AP can be installed at a single site or deployed across multiple geographically dispersed locations. Designed specifically for easy deployment and proactive management of networks, Instant is ideal for small customers or remote locations without requiring any on-site IT administrator.

An Instant AP cluster consists of slave Instant APs and a master Instant AP in the same VLAN, as they communicate with broadcast messages. A virtual controller is a combination of the whole cluster, as the slave Instant APs and Master Instant AP coordinate to provide a controllerless Instant solution. In an Instant deployment scenario, the first Instant AP that comes up becomes the master Instant AP. All other Instant APs joining the cluster after that Instant AP, become the slave Instant APs.

In an Instant deployment scenario, only the first Instant AP or the master Instant AP needs to be configured. The other Instant APs download configurations from the first Instant AP that is configured. The Instant solution constantly monitors the network to determine the Instant AP that must function as a master Instant AP at a given time. The master Instant AP may change as necessary from one Instant AP to another without impacting network performance.

Each Instant AP model has a minimum required software version. When a new Instant AP is added into an existing cluster, it can join the cluster only if the existing cluster is running at least the minimum required version of that Instant AP. If the existing cluster is running a version prior to the minimum required version of the new Instant AP, the new Instant AP will not come up and may reboot with the reason **Image sync fail**. To recover from this condition, upgrade the existing cluster to at least the minimum required version of the new Instant AP first, and add the new Instant AP. For more information about supported Instant AP platforms, refer to the *Aruba Instant Release Notes*.



Aruba recommends that networks with more than 128 Instant APs be designed as multiple, smaller virtual controller networks with Layer-3 mobility enabled between these networks.

Aruba Instant APs are available in the following variants:

- US (United States)
- JP (Japan)
- IL (Israel)

- EG (Egypt)
- RW (Rest of the World)

The following table provides the variants supported for each Instant AP platform:

Table 4: *Supported Instant AP Variants*

Instant AP Model (Reg Domain)	Instant AP-###-US (US only)	Instant AP-###-JP (Japan only)	Instant AP-###-IL (Israel only)	Instant AP-###-EG (Egypt only)	Instant AP-###-RW (Rest of the World except US/JP/EG /IL)
570EX Series	Yes	Yes	Yes	Yes	Yes
570 Series	Yes	Yes	Yes	Yes	Yes
AP-518	Yes	Yes	Yes	Yes	Yes
AP-505H	Yes	Yes	Yes	Yes	Yes
500 Series	Yes	Yes	Yes	Yes	Yes
550 Series	Yes	Yes	Yes	Yes	Yes
530 Series	Yes	Yes	Yes	Yes	Yes
510 Series	Yes	Yes	Yes	Yes	Yes
303 Series	Yes	Yes	Yes	Yes	Yes
318 Series	Yes	Yes	Yes	Yes	Yes
370 Series	Yes	Yes	Yes	Yes	Yes
340 Series	Yes	Yes	Yes	Yes	Yes
203H Series	Yes	Yes	Yes	Yes	Yes
360 Series	Yes	Yes	Yes	Yes	Yes
330 Series	Yes	Yes	Yes	Yes	Yes
320 Series	Yes	Yes	Yes	Yes	Yes
310 Series	Yes	Yes	Yes	Yes	Yes
AP-303H	Yes	Yes	Yes	Yes	Yes
207 Series	Yes	Yes	Yes	Yes	Yes
300 Series	Yes	Yes	Yes	Yes	Yes
203R Series	Yes	Yes	Yes	Yes	Yes

For information on regulatory domains and the list of countries supported by the Instant AP-###-RW type, see the **Specifying Country Code** section in Logging in to the Instant UI on page 24.

Instant WebUI

The Instant WebUI provides a standard web-based interface that allows you to configure and monitor a Wi-Fi network. Instant is accessible through a standard web browser from a remote management console or workstation and can be launched using the following browsers:

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Mozilla Firefox 48 or later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 8.0 or later on MacOS
- Google Chrome 67 or later on Windows 7, Windows 8, Windows 10, and macOS

If the Instant UI is launched through an unsupported browser, a warning message is displayed along with a list of recommended browsers. However, the users are allowed to log in using the **Continue login** link on the **Login** page.



To view the Instant UI, ensure that JavaScript is enabled on the web browser.

The Instant UI logs out automatically if the window is inactive for 15 minutes.

Instant CLI

The Instant CLI is a text-based interface that is accessible through an SSH session.

SSH access requires that you configure an IP address and a default gateway on the Instant AP and connect the Instant AP to your network. This is typically performed when the Instant network on an Instant AP is set up.

What is New in the Release

This section lists the new features, enhancements, or hardware platforms introduced in Aruba Instant 8.7.0.0.

New Features and Hardware Platforms

Table 5: *New Features in Instant 8.7.0.0*

Feature	Description
Air Slice	Aruba Air Slice, based on IEEE 802.11ax standard, is similar to 5G network slicing architecture which allows network administrators to build end-to-end virtual networks tailored for specific application requirements.
AP USB Management	Instant supports a new infrastructure to manage any USB device that is plugged to an AP. The infrastructure allows describing a USB device through either CLI configuration or by using predefined descriptors, USB device management through USB ACLs, supports plugin for USB devices, and sending notification to other processes.
ARM Settings in Radio Profiles	ARM settings can be configured for individual radios in their respective radio profiles. This feature allows you to maximize network efficiency in dense RF environments by customizing ARM settings for individual radios.
Automatic Update of CA Certificate Bundle	The Instant AP automatically checks for CA certificate bundle updates and installs the new version when it is available on Activate.
Configuring IoT	Instant supports a new payload content called Exposure Notification.
Configuring Multiple Mesh Cluster Profiles	A new configuration command is introduced to allow users to create multiple mesh cluster profiles on an Instant AP and assign a priority to each profile.
Disabling AP Factory Reset	A new configuration command is introduced to disable the hard reset to factory default when the AP is operational.
Enabling Low Power Mode on an Instant AP	A new CLI command is introduced to allow you to enable or disable low power mode settings on an Instant AP.
Enhancements to Control Ageout of Valid APs and Interfering APs	Two new CLI parameters, **valid-ap-max-unseen-timeout** and **ap-max-unseen-timeout**, are introduced in **ids** command to control the ageout duration of valid and interfering APs. These parameters enable you to effectively control the RF environment.
Enhancement to the Instant AP Hostname	The number of ASCII characters allowed in the Instant AP hostname is increased to 128 characters.
Fast BSS Transition Support for WPA3	Instant supports Fast BSS Transition for WPA3 in both tunnel forwarding and decrypt-tunnel modes.
Installing Third Party Certificates for Instant AP Applications	A new certificate installation method is introduced that enables installation and use of third party certificates for Instant AP applications. This feature is currently supported only in locally managed Instant networks.

Table 5: *New Features in Instant 8.7.0.0*

Feature	Description
Intelligent Thermal Management	Intelligent Thermal Management dynamically adapts operations of the AP to reduce the internal temperature if it exceeds the maximum threshold. This feature is supported in 570 Series, 570EX Series, and AP-518 access points.
IoT Data Filter	The data filter in the Iot transport profile reduces the traffic in the telemetry interfaces. The data filter is a string of numbers that map to the IoT API protobuf fields. Following is the mapping of the data filters and the protobuf fields:
IoT Endpoint Update	When the meridian asset tracking endpoint is configured and the firmware is upgraded to Instant 8.7.0.0, the CA certificate should be uploaded in order to connect to the meridian server.
IoT Southbound API	Instant now supports an IoT Southbound API that allows interaction with IoT devices and does not require any knowledge of the device by Aruba infrastructure.
Local Multiple PSK Operating Mode	Local MPSK operating mode allows you to define up to 24 pre-shared keys per SSID on the gateway or the Instant AP without actually requiring an external policy engine like ClearPass Policy Manager.
Mesh Link Radio Selection	A new CLI command is introduced to configure the 5 GHz radio used for mesh links in 340 Series and 550 Series access points.
Support for New Diffie-Hellman Groups in Enhanced Open Security	Aruba Instant supports Diffie-Hellman Groups 20 and 21.
Support for Wiliot Sensor	Aruba Instant supports Wiliot sensors that provide battery-free BLE tags.
Unified Communications Manager	UCM is the new service module introduced to manage voice and video call traffic in the AP.
Zigbee Service Profile	Instant allows you to configure a zigbee service profile and also set it on the Instant AP.
Zigbee Sockets	ZigBee Socket Device (ZSD) may be configured and applied as a filter in IoT transport. With ZSD, specify the source endpoint, destination endpoint, destination profile ID, or destination cluster ID and the packets between the ZigBee devices and server are transmitted through the Aruba Telemetry Websocket.

Table 6: *New Hardware Platforms in Instant 8.7.0.0*

Hardware	Description
570 Series Access Points	The Aruba 570 Series access points (AP-574, AP-575 and AP-577) are high performance, multi-radio, outdoor access points that can be deployed in either controller-based (ArubaOS) or controller-less (Aruba Instant) network environments. These APs deliver high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with MIMO radios (2x2 in 2.4 GHz, 4x4 in 5 GHz), while also supporting 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services. Additional features include: ▪ IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE

Table 6: *New Hardware Platforms in Instant 8.7.0.0*

Hardware	Description
	802.11ac, and IEEE 802.11ax operation as a wireless access point. ■ IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax spectrum monitor. ■ Mesh mode. ■ Two Ethernet ports, ENET0 and ENET1, capable of data rates up to 2.5 Gbps and 1 Gbps respectively. ■ Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards on both Ethernet ports. ■ Thermal management. For complete technical details and installation instructions, see *Aruba 570 Series Access Points Installation Guide.*
570EX Series Access Points	The Aruba 570EX Series access points (AP-575EX and AP-577EX) are high performance, multi-radio access points suitable for harsh and hazardous outdoor locations. They can be deployed in either controller-based (ArubaOS) or controller-less (Aruba Instant) network environments. These APs deliver high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with MIMO radios (2x2 in 2.4 GHz, 4x4 in 5 GHz), while also supporting 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services. Additional features include: ■ IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax operation as a wireless access point. ■ IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax spectrum monitor. ■ Mesh mode. ■ Two Ethernet ports, ENET0 and ENET1, capable of data rates up to 2.5 Gbps and 1 Gbps respectively. ■ Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards on both Ethernet ports. ■ Thermal management. For complete technical details and installation instructions, see *Aruba 570EX Series Access Points Installation Guide.*
AP-505H Access Point	The Aruba AP-505H access points are entry-level, dual-radio wireless AP that can be deployed in either controller-based (ArubaOS) or controller-less (Aruba Instant) network environments. These APs delivers high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with 2x2 MU-MIMO radios, while also supporting 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services. Additional features include: ■ IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax operation as a wireless access point. ■ IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax spectrum monitor. ■ Mesh mode. ■ Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE

Table 6: *New Hardware Platforms in Instant 8.7.0.0*

Hardware	Description
	standards. ■ One uplink Ethernet port capable of data rates up to 2.5 Gbps. ■ Four downlink Ethernet ports capable of data rates up to 1 Gbps, including two 802.3at PoE PSE ports for supplying power to downlink devices. ■ Integrated BLE and Zigbee radios. ■ Flexible USB host interface with 5W power sourcing capability. For complete technical details and installation instructions, see *Aruba AP-505H Access Point Installation Guide*.
AP-518 Access Point	The Aruba AP-518 access points are high performance, multi-radio, outdoor access point that can be deployed in either controller-based (ArubaOS) or controller-less (Aruba Instant) network environments. These APs deliver high performance concurrent 2.4 GHz and 5 GHz 802.11ax Wi-Fi (Wi-Fi 6) functionality with MIMO radios (2x2 in 2.4 GHz, 4x4 in 5 GHz), while also supporting 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless services. Additional features include: ■ IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax operation as a wireless access point. ■ IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, and IEEE 802.11ax spectrum monitor. ■ Mesh mode. ■ Two Ethernet ports, ENET0 and ENET1, capable of data rates up to 2.5 Gbps and 1 Gbps respectively. ■ Compatible with IEEE 802.3bt, IEEE 802.3at, and IEEE 802.3af PoE standards on both Ethernet ports. ■ Thermal management. For complete technical details and installation instructions, see*ArubaAP-518 Access Point Installation Guide.*

Deprecated Hardware Platforms

The following Instant AP platforms are no longer supported from Aruba Instant 8.7.0.0 onwards:

- 210 Series — IAP-214 and IAP-215
- 220 Series — IAP-224, IAP-225, and IAP-228
- 270 Series — IAP-274, IAP-275, and IAP-277
- RAP-155 and RAP-155P

This chapter describes the following procedures:

- Setting up Instant Network on page 19
- Provisioning an Instant AP on page 20
- Logging in to the Instant UI on page 24
- Accessing the Instant CLI on page 25
- Instant AP Degraded State on page 28

Setting up Instant Network

Before installing an Instant AP:

- Ensure that you have an Ethernet cable of the required length to connect an Instant AP to the home router.
- Ensure that you have one of the following power sources:
  - IEEE 802.3af/at-compliant PoE source. The PoE source can be any power source equipment switch or a midspan power source equipment device.
  - Instant AP power adapter kit.

To set up the Instant network, perform the following procedures :

1. Connecting an Instant AP on page 19
2. Assigning an IP address to the Instant AP on page 19

Connecting an Instant AP

Based on the type of the power source used, perform one of the following steps to connect an Instant AP to the power source:

- PoE switch—Connect the Ethernet 0 port of the Instant AP to the appropriate port on the PoE switch.
- PoE midspan—Connect the Ethernet 0 port of the Instant AP to the appropriate port on the PoE midspan.
- AC to DC power adapter—Connect the 12V DC power jack socket to the AC to DC power adapter.

Assigning an IP address to the Instant AP

The Instant AP needs an IP address for network connectivity. When you connect an Instant AP to a network, it receives an IP address from a DHCP server.

To obtain an IP address for an Instant AP:

1. Ensure that the DHCP service is enabled on the network.
2. Connect the Ethernet 0 port of Instant AP to a switch or router using an Ethernet cable.

3. Connect the Instant AP to a power source. The Instant AP receives an IP address provided by the switch or router.



If there is no DHCP service on the network, the Instant AP can be assigned a static IP address. If a static IP is not assigned, the Instant AP obtains an IP automatically within the 169.254 subnet.

Assigning a Static IP

To assign a static IP to an Instant AP:

1. Connect a terminal, PC, or workstation running a terminal emulation program to the **Console** port on the Instant AP.
2. Turn on the Instant AP. An autoboot countdown prompt that allows you to interrupt the normal startup process and access **apboot** is displayed.
3. Press **Enter** key before the timer expires. The Instant AP goes into the **apboot** mode.
4. In the **apboot** mode, execute the following commands to assign a static IP to the Instant AP.

```
Hit <Enter> to stop autoboot:  0
apboot>
apboot> setenv ipaddr 192.0.2.0
apboot> setenv netmask 255.255.255.0
apboot> setenv gatewayip 192.0.2.2
apboot> save
Saving Environment to Flash...
Un-Protected 1 sectors
.done
Erased 1 sectors
Writing
```

5. Use the **`printenv`** command to view the configuration.

```
apboot> printenv
```

Provisioning an Instant AP

This section provides the following information:

- ZTP and NTP Server and Synchronization
- Provisioning IAPs though Aruba Central
- Provisioning Instant APs through AirWave

ZTP of Instant APs

ZTP eliminates the traditional method of deploying and maintaining devices and allows you to provision new devices in your network automatically, without manual intervention. Following are the ZTP methods for Instant.

Aruba Activate is a cloud-based service designed to enable more efficient deployment and maintenance of Instant APs. ArubaActivate is hosted in the cloud and is available at https://activate.arubanetworks.com. You can register for a free account by using the serial number and MAC address of the device you currently own. For more information on how to setup your device and provision using Aruba Activate, refer to the *Aruba Activate User Guide*.

NTP Server and Instant AP Synchronization

In order for ZTP to be successful, the timezone of the Instant AP must be in synchronization with the NTP server.



To facilitate ZTP using the AMP, Central, or Activate, you must configure the firewall and wired infrastructure to either allow the NTP traffic to pool.ntp.org, or provide alternative NTP servers under DHCP options. For more information on configuring an NTP server, see NTP Server.

In a scenario where the NTP server is unreachable, the connection between the Instant AP and Activate will fall back to the unsecured status. The NTP client process running in the back end will continuously attempt to reconnect to the NTP server until a secure connection is established. The NTP client process receives a response from the NTP server on successfully establishing a connection and notifies the CLI process which runs a series of checks to ensure the NTP server is reachable.

The Instant APs boot with factory default configuration and try to provision automatically. If the automatic provisioning is successful, the Instant SSID will not be available. If AirWave and Activate are not reachable and the automatic provisioning fails, the Instant SSID becomes available and the users can connect to a provisioning network by using the Instant SSID.

To connect to a provisioning Wi-Fi network:

1. Ensure that the client is not connected to any wired network.
2. Connect a wireless-enabled client to a provisioning Wi-Fi network: for example, Instant.
3. If the Windows operating system is used:
   a. Click the wireless network connection icon in the system tray. The **Wireless Network Connection** window is displayed.
   b. Click the Instant network and then click **Connect**.
4. If the Mac operating system is used:
   a. Click the **AirPort** icon. A list of available Wi-Fi networks is displayed.
   b. Click the **instant** network.



The Instant SSIDs are broadcast in 2.4 GHz only.

The provisioning SSID for all APs running Instant 6.5.2.0 onwards, including legacy Instant APs is **SetMeUp-xx:xx:xx.**

Instant APs in the same VLAN automatically find each other and form a single functioning network managed by a virtual controller.



Moving anInstant AP from one cluster to another requires a factory reset of the Instant AP.

The provisioning network is enabled by default. Instant provides the option to disable the provisioning network through the console port. Use this option only when you do not want the default SSID Instant to be broadcast in your network.

To disable the provisioning network:

1. Connect a terminal, PC, or workstation running a terminal emulation program to the **Console** port on the Instant AP.
2. Configure the terminal or terminal emulation program to use the following communication settings:

   Table 7: *Terminal Communication Settings*

Baud Rate	Data Bits	Parity	Stop Bits	Flow Control
9600	8	None	1	None

3. Turn on the Instant AP. An autoboot countdown prompt that allows you to interrupt the normal startup process and access apboot is displayed.
4. Click **Enter**key before the timer expires. The Instant AP goes into the apboot mode through console.
5. In the apboot mode, execute the following commands to disable the provisioning network:

```
apboot> factory_reset

apboot> setenv disable_prov_ssid 1

apboot> saveenv

apboot> reset
```

Some customers do not use Activate either because of their security policy or because it is a new site and they do not have internet connectivity when the Instant AP is initially brought up. These customers prefer to disable all communications between the Instant AP and Activate during initial provisioning.

Under these circumstances, Aruba Instant provides 3 methods to disable Activate provisioning. You may choose either of the following methods to disable Activate provisioning during the initial setup:

- Use the configuration command to disable provisioning by Activate using the Instant CLI.

```
(Instant AP)(config)# activate-disable
```

- Configure a DHCP profile with a DHCP option <type> **43** and the <value> **activate-disable=True**. The DHCP option 43 will broadcast the provisioning information to the Instant AP from the DHCP server instead of Activate.

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP profile <profile-name>)# option 43 activate-disable=True
```

- Configure a DHCP profile with a DHCP option <type> **60** and the <value> **ArubaInstantAP**.

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP profile <profile-name>)# option 60 ArubaInstantAP
```

Provisioning Instant APs through Central

The Aruba Central Central UI provides a standard web-based interface that allows you to configure and monitor multiple Aruba Instant networks from anywhere with a connection to the Internet. Aruba Central supports all the Instant APs running Instant 6.2.1.0-3.3.0.0 or later versions.

Using Central, individual users can manage their own wireless network. This UI is accessible through a standard web browser and can be launched using various browsers.

Central supports automatic ZTP and manual provisioning. There are three different methods of manual provisioning.

- By providing the Activate credentials of the customer.
- By providing cloud activation key and MAC address of the Instant AP.
- By providing the serial number and MAC address of the Instant AP.

For provisioning Instant APs through Central, the Instant APs must obtain the cloud activation key.

To ensure that the Instant APs obtain the cloud activation key from the Aruba Activate server, perform the following checks:

- The serial number or the MAC address of the Instant AP is registered in the Activate database.
- The Instant AP is operational and is able to connect to the Internet.
- Instant AP has received a DNS server address through DHCP or static configuration.
- Instant AP is able to configure time zone using an NTP server.
- The required firewall ports are open. Most of the communication between devices on the remote site and the Central server in the cloud is carried out through HTTPS (TCP 443). However, you may need to configure the following ports:
  - TCP port 443 for configuration and management of devices.
  - TCP port 80 for image upgrade.
  - UDP port 123 for NTP server to configure timezone when factory default Instant AP comes up.
  - TCP port 2083 for RADIUS authentication for guest management. If 2083 port is blocked, the HTTPS protocol is used.

If a cloud activation key is not obtained, perform the following checks:

- If the Instant AP IP address is assigned from the DHCP server, ensure that the DNS server is configured.
- If the Instant AP is assigned a static IP address, manually configure the DNS server IP address. For more information, see Specifying a Method for Obtaining IP Address.

If Instant AP has already obtained the activation key, complete the following steps:

1. Connect to the Instant SSID and type http://instant.arubanetworks.com in the web browser.
2. Log in to the website by using the default username **admin** and the default password which is the Serial Number of the Instant AP.
3. In the Instant AP WebUI, navigate to **Maintenance > About** and copy the cloud activation key.
4. To view the MAC address of the master Instant AP, click the device name under the **Access Points** tab of the main window. The MAC address will be displayed in the **Info** section.

If Instant AP has already obtained the activation key, complete the following steps:

1. Connect to the Instant SSID and type http://instant.arubanetworks.com in the web browser.
2. Log in to the website by using the default username **admin** and the default password which is the Serial Number of the Instant AP.
3. In the Instant AP WebUI, navigate to **Maintenance** > **About**. You can view the cloud activation key in the **Cloud Activation Key** field.
4. To view the MAC address of the master Instant AP, navigate to **Dashboard** > **Overview** and select the device from the **Dashboard** > **Access Points**. The MAC address will be displayed under **Overview** > **Info**. Alternatively, go to **Dashboard** > **Access Points** and select the device from the list of **Access Points**. The MAC address will be displayed under **Overview** > **Info**.

You can also check the cloud activation key of an Instant AP by running the **show about** and **show activate status** commands. For more information on these commands, refer to the *Aruba Instant CLI Reference Guide*.



If the Instant AP is deployed in the cluster mode, the slave Instant APs do not obtain the activation key. You must use the cloud activation key and MAC address of the master Instant AP for provisioning through Central.

Provisioning Instant APs through AirWave

AirWave is a powerful platform and easy-to-use network operations system that manages Aruba wireless, wired, and remote access networks, as well as wired and wireless infrastructures from a wide range of third-party manufacturers. With its easy-to-use interface, AirWave provides real-time monitoring, proactive alerts, historical reporting, as well as fast and efficient troubleshooting. It also offers tools that manage RF coverage, strengthen wireless security, and demonstrate regulatory compliance.

For information on provisioning Instant APs through AirWave, refer to the *AirWave Deployment Guide*.

Logging in to the Instant UI

Launch a web browser and enter http://instant.arubanetworks.com. In the login screen, enter the following credentials:

- Username—admin
- Password—Enter the Serial Number of the Instant AP

When you use a provisioning Wi-Fi network to connect to the Internet, all browser requests are directed to the Instant UI. For example, if you enter www.example.com in the address bar, you are directed to the Instant UI. You can change the default login credentials after the first login.



If an Instant AP does not obtain an IP address, it assigns itself 169.x.x.x as the IP address. In this case, DNS requests from clients on a provisioning SSID will not receive a response because of lack of network connectivity. Hence, automatic redirection to the Instant UI instant.arubanetworks.com will fail. In such a case, you must manually open instant.arubanetworks.com on your browser to access the Instant WebUI.

Regulatory Domains

The IEEE 802.11, 802.11b, 802.11g, or 802.11n Wi-Fi networks operate in the 2.4 GHz spectrum and IEEE 802.11a or 802.11n operate in the 5 GHz spectrum. The spectrum is divided into channels. The 2.4 GHz spectrum is divided into 14 overlapping, staggered 20 MHz wireless carrier channels. These channels are spaced 5 MHz apart. The 5 GHz spectrum is divided into more channels. The channels that can be used in a particular country vary based on the regulations of that country.

The initial Wi-Fi setup requires you to specify the country code for the country in which the Instant AP operates. This configuration sets the regulatory domain for the radio frequencies that the Instant APs use. Within the regulated transmission spectrum, a HT 802.11ac, 802.11a, 802.11b, 802.11g, or 802.11n radio setting can be configured. The available 20 MHz, 40 MHz, or 80 MHz channels are dependent on the specified country code.

You cannot change a country code for Instant APs in regulatory domains such as Japan and Israel. However, for Instant AP-US and Instant AP-RW variants, you can select from the list of supported regulatory domains. If the supported country code is not in the list, contact your Aruba Support team to know if the required country code is supported and obtain the software that supports the required country code.



Improper country code assignments can disrupt wireless transmissions. Most countries impose penalties and sanctions on operators of wireless networks with devices set to improper country codes.

To view the country code information, run the **show country-codes** command.

Specifying Country Code

The **Country Code** window is displayed for the Instant AP-US and Instant AP-RW variants when you login to the Instant AP UI for the first time. The **Please Specify the Country Code** drop-down list displays only the supported country codes. If the Instant AP cluster consists of multiple Instant AP platforms, the country codes supported by the master Instant AP is displayed for all other Instant APs in the cluster. Select a country code from the list and click **OK**. The Instant AP operates in the selected country code domain.



Country code once set, cannot be changed in the Instant UI. It can be changed only by using the **virtual-controller-country** command in the Instant CLI.

Slave Instant APs obtain country code configuration settings from the master Instant AP.

You can also view the list of supported country codes for the Instant AP-US and Instant AP-RW variants by using the **show country-codes** command.

Accessing the Instant CLI

Instant supports the use of CLI for scripting purposes. When you make configuration changes on a master Instant AP in the CLI, all associated Instant APs in the cluster inherit these changes and subsequently update their configurations. By default, you can access the CLI from the serial port or from an SSH session. You must explicitly enable Telnet access on the Instant AP to access the CLI through a Telnet session.

For information on enabling SSH and Telnet access to the Instant AP CLI, see Terminal access on page 70.

Connecting to a CLI Session

On connecting to a CLI session, the system displays its host name followed by the login prompt. Use the administrator credentials to start a CLI session. For example:

```
Username: admin
```

If the login is successful, the privileged command mode is enabled and a command prompt is displayed. For example:

```
(Instant AP)#
```

The privileged EXEC mode provides access to **show**, **clear**, **ping**, **traceroute**, and **commit** commands. The configuration commands are available in the config mode. To move from Privileged EXEC mode to the Configuration mode, enter the following command at the command prompt:

```
(Instant AP)# configure terminal
```

The configure terminal command allows you to enter the basic configuration mode and the command prompt is displayed as follows:

```
(Instant AP)(config)#
```

The Instant CLI allows CLI scripting in several other subcommand modes to allow the users to configure individual interfaces, SSIDs, access rules, and security settings.

You can use the question mark (?) to view the commands available in a privileged EXEC mode, configuration mode, or subcommand mode.



Although automatic completion is supported for some commands such as **configure terminal**, the complete **exit** and **end** commands must be entered at command prompt.

Applying Configuration Changes

Each command processed by the virtual controller is applied on all the slaves in a cluster. The changes configured in a CLI session are saved in the CLI context. The CLI does not support the configuration data exceeding the 4K buffer size in a CLI session. Therefore, it is recommended that you configure fewer changes at a time and apply the changes at regular intervals.

To apply and save the configuration changes at regular intervals, execute the following command in the privileged EXEC mode:

```
(Instant AP)# commit apply
```

To apply the configuration changes to the cluster without saving the configuration, execute the following command in the privileged EXEC mode:

```
(Instant AP)# commit apply no-save
```

To view the changes that are yet to be applied, execute the following command in the privileged EXEC mode:

```
(Instant AP)# show uncommitted-config
```

To revert to the earlier configuration, execute the following command in the privileged EXEC mode.

```
(Instant AP)# commit revert
```

Example:

To apply and view the configuration changes:

```
(Instant AP)(config)# rf dot11a-radio-profile
```

```
(Instant AP)# show uncommitted-config
```

Using Sequence-Sensitive Commands

The Instant CLI does not support positioning or precedence of sequence-sensitive commands. Therefore, it is recommended that you remove the existing configuration before adding or modifying the configuration details for sequence-sensitive commands. You can either delete an existing profile or remove a specific configuration by using the **no** commands.

The following table lists the sequence-sensitive commands and the corresponding **no** commands to remove the configuration:

Table 8: *Sequence-Sensitive Commands*

Sequence-Sensitive Command	Corresponding no command
`rule <dest> <mask> <match> <protocol> <start-port> <end-port> {permit | deny | src-nat | dst-nat {<IP-address> <port> | <port>}} [<option1....option9>]`	`no rule <dest> <mask> <match> <protocol> <start-port> <end-port> {permit | deny | src-nat | dst-nat}`
`mgmt-auth-server <auth-profile-name>`	`no mgmt-auth-server <auth-profile-name>`
`set-role <attribute>{{equals| not-equals | starts-with | ends-with | contains} <operator> <role> | value-of}`	`no set-role <attribute>{{equals | not-equals | starts-with | ends-with | contains} <operator>| value-of}` `no set-role`
`set-vlan <attribute>{{equals | not-equals | starts-with | ends-with | contains} <operator> <VLAN-ID> | value-of}`	`no set-vlan <attribute>{{equals | not-equals | starts-with | ends-with | contains} <operator> | value-of}` `no set-vlan`
`auth-server <name>`	`no auth-server <name>`

Banner and Loginsession Configuration

Starting from Instant 6.5.0.0-4.3.0.0, the Banner and Loginsession Configuration feature is introduced in the Instant AP. The text banner can be displayed at the login prompt when users are on a management (Telnet or SSH) session of the CLI, and the management session can remain active even when there is no user activity involved.

The **banner** command defines a text banner to be displayed at the login prompt of a CLI. Instant supports up to 16 lines text, and each line accepts a maximum of 255 characters including spaces.

To configure a banner:

```
(Instant AP)(config)# banner motd <motd_text>
```

To display the banner:

```
(Instant AP)# show banner
```

The **loginsession** command configures the management session (Telnet or SSH) to remain active without any user activity.

To define a timeout interval:

```
(Instant AP) (config) #loginsession timeout <val>
```

<val> can be any number of minutes from 5 to 60, or any number of seconds from 1 to 3600. You can also specify a timeout value of 0 to disable CLI session timeouts. The users must re-login to the Instant AP after the session times out. The session does not time out when the value is set to 0.

Instant AP Degraded State

The following conditions may cause an Instant AP to prevent users from logging in to the WebUI and CLI. In most cases, the Instant AP will display the error message **Warning: CLI Module is running in a degraded state. Some commands will not function**

1. When the Instant AP cannot be a master Instant AP because it has no IP address, and does not have an uplink connection.
2. When the Instant AP is unable to join the cluster because of a missing country code, image, or incorrect regulatory hardware.
3. When the Instant AP has been denied permission to the existing cluster based on the allowed AP whitelist or the auto-join configuration present in the cluster.
4. In a mixed class network, when the slave Instant APs join the master Instant AP with a different software version, causing the image sync from the cloud or AirWave to fail.

Additionally, the following console messages indicate other error conditions:

- **4-0 Authentication server failure**: Incorrect username or password.
- **5-0 Authentication server timeout** - no response from RADIUS server.
- **7-0**: Indicates PAPI errors within the Instant AP. The Instant AP log messages provide details on the error condition. Consult Aruba Technical Support for further assistance.
- **8-0**: Indicates an authentication failure or an incomplete synchronization of a swarm configuration.

An example of one of the above mentioned console messages is **Internal error 7-0, please contact support**.

Chapter 4
Automatic Retrieval of Configuration

This chapter provides the following information:

- Managed Mode Operations on page 29
- Prerequisites on page 29
- Configuring Managed Mode Parameters on page 29
- Verifying the Configuration on page 31

Managed Mode Operations

Instant APs support managed mode operations to retrieve the configuration file from a server through the FTP or FTPS, and automatically update the Instant AP configuration.

The server details for retrieving configuration files are stored in the basic configuration of the Instant APs. The basic configuration of an Instant AP includes settings specific to an Instant AP, for example, host name, static IP, and radio configuration settings. When an Instant AP boots up, it performs a GET operation to retrieve the configuration (.cfg) file from the associated server using the specified download method.

After the initial configuration is applied to the Instant APs, the configuration can be changed at any point. You can configure a polling mechanism to fetch the latest configuration by using an FTP or FTPS client periodically. If the remote configuration is different from the one running on the Instant AP and if a difference in the configuration file is detected by the Instant AP, the new configuration is applied. At any given time, Instant APs can fetch only one configuration file, which may include the configuration details specific to an Instant AP. For configuring polling mechanism and downloading configuration files, the users are required to provide credentials (username and password). However, if automatic mode is enabled, the user credentials required to fetch the configuration file are automatically generated. To enable automatic configuration of the Instant APs, configure the managed mode command parameters.

Prerequisites

Perform the following checks before configuring the managed mode command parameters:

- Ensure that the Instant AP is running Instant 6.2.1.0-3.4 or later versions.
- When the Instant APs are in the managed mode, ensure that the Instant APs are not managed by AirWave.

Configuring Managed Mode Parameters

To enable the automatic configuration, perform the steps described in the following table:

Table 9: *Managed Mode Commands*

Steps	Command
1. Start a CLI session to configure the managed-mode profile for automatic configuration.	`(Instant AP)(config)# managed-mode-profile`

2. Enable automatic configuration
Or
Specify the user credentials.
	`(Instant AP)(managed-mode-profile)#  automatic`
	Or
	`(Instant AP)(managed-mode-profile)# username <username>`
	`(Instant AP)(managed-mode-profile)# password <password>`
	
	NOTE: If the automatic mode is enabled, the user credentials are automatically generated based on Instant AP MAC address.

3. Specify the configuration file.	`(Instant AP)(managed-mode-profile)# config-filename  <file_name>` `Filename`—Indicates filename in the alphanumeric format. Ensure that configuration file name does not exceed 40 characters.
4. Specify the configuration file download method.	`(Instant AP)(managed-mode-profile)# download-method <ftp|ftps>` You can use either FTP or FTPS for downloading configuration files.
5. Specify the name of the server or the IP address of the server from which the configuration file must be downloaded.	`(Instant AP)(managed-mode-profile)# server <server_name>`
6. Configure the day and time at which the Instant APs can poll the configuration files	`(Instuant AP) (managed-mode-profile)#  sync-time day <dd> hour <hh> min <mm> window <window>` Based on the expected frequency of configuration changes and maintenance window, you can set the configuration synchronization timeline. ■ `day <dd>`—Indicates day, for example to configure Sunday as the day, specify 01. To configure the synchronization period as everyday, specifiy 00. ■ `hour <hh>`—Indicates hour within the range of 0–23. ■ `min <mm>`—Indicates minutes within the range of 0–59.

Table 9: *Managed Mode Commands*

Steps	Command
from the server.	■ `window <hh>`—Defines a window for synchronization of the configuration file. The default value is 3 hours.
7. Configure the time interval in minutes between two retries, after which Instant APs can retry downloading the configuration file.	`(Instant AP)(managed-mode-profile)# retry-poll-period <seconds>` **NOTE:** Specify the retry interval in seconds within the range of 5–60 seconds. The default retry interval is 5 seconds.
8. Apply the configuration changes.	`(Instant AP)(managed-mode-profile)# end` `(Instant AP)# commit apply`

If you want to apply the configuration immediately and do not want to wait until next configuration retrieval attempt, execute the following command:

```
(Instant AP)# managed-mode-sync-server
```

Example

To configure managed mode profile:

```
(Instant AP)(config)# managed-mode-profile
```

Verifying the Configuration

To verify if the automatic configuration functions, perform the following checks:

1. Verify the status of configuration by running the following commands at the command prompt:

```
(Instant AP)# show managed-mode config
(Instant AP)# show managed-mode status
```

2. Verify the status of download by running the following command at the command prompt:

```
(Instant AP)# show managed-mode logs
```

If the configuration settings retrieved in the configuration file are incomplete, Instant APs reboot with the earlier configuration.

This chapter describes the following sections:

- Introduction on page 32
- Login Screen on page 32
- Main Window on page 33

Introduction

The old Instant WebUI is not fully aligned with the other products of Aruba. For an enhanced user experience, Instant 8.4.0.0. introduces the new WebUI.

The key features of the new WebUI are that is has a modern look and feel with a responsive layout that is mobile and/or tablet friendly and it has an improvised search capability.

You can toggle between the old and new WebUI as and when required.

- If you are on the old WebUI and want to switch to the new WebUI, click the **Switch to new UI** link on the Instant main window.
- If you are on the new WebUI and want switch to the old WebUI, expand the User menu at the top right corner of the Instant main window and click the **Switch to old UI** link.

Login Screen

The Instant login page allows you to perform the following tasks:

- View Instant Network Connectivity summary
- View the WebUI in a specific language
- Log in to the new WebUI

Viewing Connectivity Summary

The login page also displays the connectivity status to the Instant network. The users can view a summary that indicates the status of the Internet availability, uplink, cellular modem and signal strength, VPN, and AirWave configuration details before logging in to the WebUI.

Language

The **Language** drop-down list contains the available languages and allows users to select their preferred language before logging in to the WebUI. A default language is selected based on the language preferences in the client desktop operating system or browser. If Instant cannot detect the language, then **English** is used as the default language.

You can also select the required language option from the **Languages** drop-down list located on the Instant main window.

Logging into the New WebUI

To log in to the WebUI, enter the following credentials:

- Username—admin
- Password—Enter the Serial Number of the Instant AP.



If the Instant AP is currently operating in FIPS mode, the login credentials are Username: **admin** Password: **admindefault**.

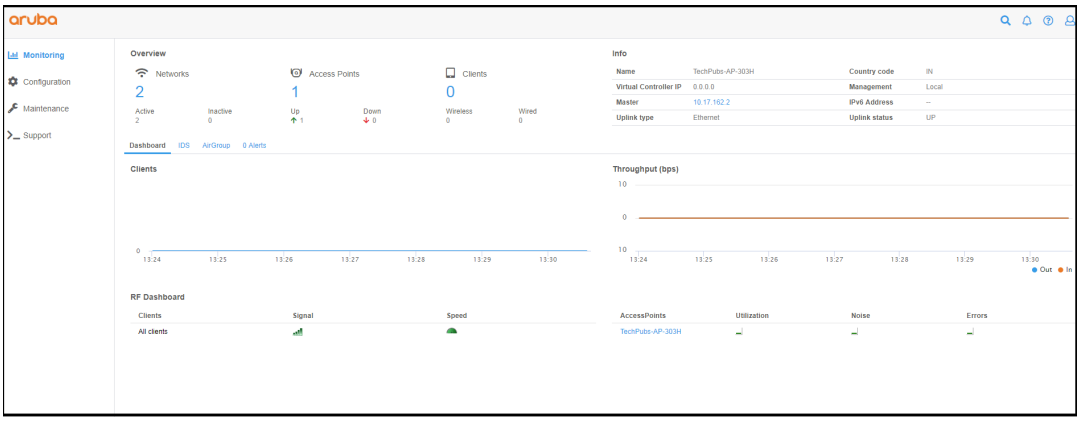
The new WebUI main window is displayed.

When you log in to an Instant AP with the factory default settings, a popup box displays an option to sign up for the Aruba cloud solution and enable Instant AP management through Central. To sign up for a free 90-day trial of Central, click here.

Main Window

After you log in to Instant, the new WebUI main window is displayed.

Figure 1 *Instant New WebUI Main Window*



The horizontal pane of the main window is divided based on the following icons:

- **Aruba logo**—The Aruba logo.
- **Search**—Administrators can search for an Instant AP, client, or a network in the Search text box. When you type a search text, the search function suggests matching keywords and allows you to automatically complete the search text entry.
- **Notifications**—The Notifications link displays notifications about new updates with regard to the WebUI.
- **Help**—The Help link allows you to view a short description or definition of the selected terms in the WebUI windows or the dialog boxes.

To activate the context-sensitive help:

1. Click the Help link available above the Search bar on the Instant main window.
2. Click any text or term displayed in green italics to view its description or definition.
3. To disable the help mode, click the Help link.
4. **User menu**—Drop-down menu that displays your username, user settings, link to documentation, option to switch to the old WebUI, and an option to logout of the Instant AP.

The vertical pane of the main window consists of the following tabs:

- Monitoring
- Configuration
- Maintenance
- Support

Monitoring

The **Monitoring** tab displays the Monitoring pane for the Instant network. Click the **Monitoring** tab to compress or expand the Monitoring pane.

The Monitoring pane consists of the following sections:

- Overview
- Networks
- Access Points
- Clients

Overview

This section displays the following sections:

- **Overview**—This section displays the number of configured networks, access points, and clients
- **Info**—This section displays information about the access point name, country code, virtual controller IP address, management, master Instant AP IP address, IPv6 address, uplink type, and uplink status.
- **Clients**—The Clients graph displays the number of clients that were associated with the virtual controller in the last 15 minutes.
- **Throughput**—The Throughput Graph shows the throughput of the selected client for the last 15 minutes.
  - **Out**—Throughput for the outgoing traffic is displayed in blue.
  - **In**—Throughput for the incoming traffic is displayed in orange. To see an enlarged view, click the graph. To see the exact throughput at a particular time, move the cursor over the graph line.
- **RF Dashboard**—This section displays the Instant APs that exceed the utilization, noise, or error threshold. It also shows the clients with low speed or signal strength in the network and the RF information for the Instant AP to which the client is connected.

The Instant AP names are displayed as links. When an Instant AP is clicked, the Instant AP configuration information is displayed on the Instant main window.

The following table describes the parameters available on the RF Dashboard pane:

Table 10: *RF Dashboard Parameters*

Parameter	Description
Signal	Displays the signal strength of the client. Signal strength is measured in dB. Depending on the signal strength of the client, the color of the lines on the Signal icon changes in the following order: ■ Green—Signal strength is more than 20 dB. ■ Orange—Signal strength is between 15 dB and 20 dB. ■ Red—Signal strength is less than 15 dB.
Speed	Displays the data transfer speed of the client. Depending on the data transfer speed of the client, the color of the Speed icon changes in the following order:

Table 10: *RF Dashboard Parameters*

Parameter	Description
	■ Green—Data transfer speed is more than 50% of the maximum speed supported by the client. ■ Orange—Data transfer speed is between 25% and 50% of the maximum speed supported by the client. ■ Red—Data transfer speed is less than 25% of the maximum speed supported by the client.
Utilization	Displays the radio utilization rate of the Instant APs. Depending on the percentage of utilization, the color of the lines on the Utilization icon changes in the following order: ■ Green—Utilization is less than 50%. ■ Orange—Utilization is between 50% and 75%. ■ Red—Utilization is more than 75%.
Noise	Displays the noise floor details for the Instant APs. Noise is measured in decibel per meter. Depending on the noise floor, the color of the lines on the Noise icon changes in the following order: ■ Green—Noise floor is more than -87 dBm. ■ Orange—Noise floor is between -80 dBm and -87 dBm. ■ Red—Noise floor is less than -80 dBm.
Errors	Displays the errors for the Instant APs. Depending on the errors, color of the lines on the Errors icon changes in the following order: ■ Green—Errors are less than 5000 frames per second. ■ Orange—Errors are between 5000 and 10,000 frames per second. ■ Red—Errors are more than 10000 frames per second.

Networks

This section displays a list of Wi-Fi networks that are configured in the Instant network. The network names are displayed as links. The expanded view displays the following information about each WLAN SSID:

- **Name**—Name of the network.
- **Clients**—Number of clients that are connected to the network.
- **Type**—Type of network such as Employee, Guest, or Voice.
- **Band**—Band in which the network is broadcast: 2.4 GHz band, 5 GHz band, or both.
- **Authentication Method**—Authentication method required to connect to the network.
- **Key Management**—Authentication key type.
- **IP Assignment**—Source of IP address for the client.
- **Zone**—Instant AP zone configured on the SSID.
- **Active**—Status of the network.

Access Points

If the Auto-Join Mode feature is enabled, a list of enabled and active Instant APs in the Instant network is displayed on the **Access Points** section. The Instant AP names are displayed as links.

The **Access Points** section displays the following information about each Instant AP:

- **Name**—Name of the Instant AP. If the Instant AP functions as a master Instant AP in the network, the asterisk sign "*" is displayed next to the Instant AP.
- **IP Address**—IP address of the Instant AP.
- **Mode**—Mode of theInstant AP.
  - **Access**—In this mode, the Instant AP serves clients and scans the home channel for spectrum analysis while monitoring channels for rogue Instant APs in the background.
  - **Monitor**—In this mode, the Instant AP acts as a dedicated AM, scanning all channels for rogue Instant APs and clients.
- **Spectrum**—When enabled, the Instant AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference from neighboring Instant APs or non-Wi-Fi devices such as microwaves and cordless phones. When Spectrum is enabled, the Instant AP does not provide access services to clients.
- **Clients**—Number of clients that are currently associated to the Instant AP.
- **Type**—Model number of the Instant AP.
- **Mesh Role**—Role of the Instant AP as a mesh portal or mesh point.
- **Zone**—Instant AP zone.
- **Serial number**—Serial number of the device.

Clients

This section displays a list of clients that are connected to the Instant network. The client names are displayed as links. The client view displays the following information about each client:

- **Name**—User name of the client or guest users if available.
- **IP Address**—IP address of the client.
- **MAC address**—MAC address of the client.
- **OS**—Operating system that runs on the client.
- **ESSID**—ESSID to which the client is connected.
- **Access Point**—Instant AP to which the client is connected.
- **Channel**—The client operating channel.
- **Type**—Type of the Wi-Fi client.
- **Role**—Role assigned to the client.
- **IPv6 Address**—IPv6 address assigned to the client.
- **Signal**—Current signal strength of the client, as detected by the Instant AP.
- **Speed (Mbps)**—Current speed at which data is transmitted. When the client is associated with an Instant AP, it constantly negotiates the speed of data transfer. A value of 0 means that the Instant AP has not heard from the client for some time.

Configuration

The following configurations allow you to configure various features for the Instant network:

- Networks
- Access Points
- System
- RF
- Security
- IDS

- Routing
- Tunneling
- Services
- DHCP Server

Networks

The **Networks** section displays the following tabs:

- **Name**—Displays the name of a WLAN or a wired network profile.
- **Type**—Shows whether the configured network profile is a WLAN or a wired profile.
- **Clients**—Shows the number of clients associated with the network profile.

You can add, edit, or delete a network profile by clicking the corresponding icons.

Access Points

The **Access Points** section displays the following tabs:

- **Name**—Name of the Instant AP. If the Instant AP functions as a master Instant AP in the network, the asterisk sign "*" is displayed next to the Instant AP.
- **IP Address**—IP address of the Instant AP.
- **Mode**—Mode of theInstant AP.
  - **Access**—In this mode, the Instant AP serves clients and scans the home channel for spectrum analysis while monitoring channels for rogue Instant APs in the background.
  - **Monitor**—In this mode, the Instant AP acts as a dedicated AM, scanning all channels for rogue Instant APs and clients.
- **Spectrum**—When enabled, the Instant AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference from neighboring Instant APs or non-Wi-Fi devices such as microwaves and cordless phones. When Spectrum is enabled, the Instant AP does not provide access services to clients.
- **Clients**—Number of clients that are currently associated to the Instant AP.
- **Type**—Model number of the Instant AP.
- **Mesh Role**—Role of the Instant AP as a mesh portal or mesh point.
- **Zone**—Instant AP zone.
- **Serial number**—Serial number of the device.

To edit a network profile, select the access point.

System

This **System** section displays the following tabs:



Use the **Show/Hide Advanced** option of the **System** window to view or hide the advanced options.

The **System** section displays the following tabs:

- **General**—Allows you to configure, view, or edit the Name, IP address, NTP Server, and other Instant AP settings for the virtual controller.
- **Admin**—Allows you to configure administrator credentials for access to the virtual controller management UI. You can also configure AirWave in this tab. For more information on management

interface and AirWave configuration, see Overview of Instant AP Users on page 207 and Managing an Instant AP from AirWave on page 439, respectively.

- **Uplink**—Allows you to view or configure uplink settings. See Uplink Configuration on page 454 for more information.
- **L3 Mobility**—Allows you to view or configure the Layer-3 mobility settings. See Configuring Layer-3 Mobility on page 484 for more information.
- **Monitoring**—Allows you to view or configure the following details:
  - **Syslog**—Allows you to view or configure Syslog server details for sending syslog messages to the external servers. See Configuring Syslog Servers on page 509 for more information.
  - **TFTP Dump**—Allows you to view or configure a TFTP dump server for core dump files. See Configuring TFTP Dump Server on page 511 for more information.
  - **SNMP**—Allows you to view or configure SNMP agent settings. See Configuring SNMP on page 506 for more information.
- **WISPr**—Allows you to view or configure the WISPr settings. See WISPr Authentication on page 221 for more information.
- **Proxy**—Allows you to configure HTTP proxy on anInstant AP. Refer to the *ArubaInstant Release Notes* for more information.
- **Time Based Services**—Allows you to configure a time profile which can be assigned to the SSID configured on the Instant AP. See Configuring Time-Based Services on page 312

RF

The **RF** section displays a window for configuring ARM and Radio features.

- **ARM**—Allows you to view or configure channel and power settings for all the Instant APs in the network. For information on ARM configuration, see ARM Overview on page 369.
- **Radio**—Allows you to view or configure radio settings for 2.4 GHz and the 5 GHz radio profiles. For information on Radio, see Configuring Radio Settings on page 377.

Security

The **Security** section displays a window with the following tabs:

- **Authentication Servers**—Use this tab to configure an external RADIUS server for a wireless network. For more information, see Configuring an External Server for Authentication on page 231.
- **Users**—Use this tab to populate the system's internal authentication server with users. This list is used by networks for which per-user authorization is specified using the internal authentication server of the virtual controller. For more information on users, see Overview of Instant AP Users on page 207.
- **Roles** —Use this tab to view the roles defined for all the Networks. The Access Rules part allows you to configure permissions for each role. For more information, see Configuring User Roles on page 277 and Configuring ACL Rules for Network Services on page 260.
- **Blacklisting**—Use this tab to blacklist clients. For more information, see Blacklisting Clients on page 251.
- **Firewall Settings**—Use this tab to enable or disable ALG supporting address and port translation for various protocols and to configure protection against wired attacks. For more information, see Configuring ALG Protocols on page 267 and Configuring Firewall Settings for Protection from ARP Attacks on page 267

- **Inbound Firewall**—Use this tab to enhance the inbound firewall by allowing the configuration of inbound firewall rules, management subnets, and restricted corporate access through an uplink switch. For more information, see Managing Inbound Traffic on page 269.
- **External Captive Portal**—Use this tab to configure external captive portal profiles. For more information, see Configuring External Captive Portal for a Guest Network on page 189.
- **Custom Blocked Page URL**—Use this tab to create a list of URLs that can be blocked using an ACL rule. For more information, see Creating Custom Error Page for Web Access Blocked by AppRF Policies on page 276.

IDS

The **IDS** section displays a list of foreign Instant APs and foreign clients that are detected in the network. It consists of the following sections:

- **Detection**—Lists the threats for the Instant AP to detect.
  - **Infrastructure**—Specifies the policy for detecting wireless attacks on access points.
  - **Cients**—Specifies the policy for detecting wireless attacks on clients.
- **Protection**—Lists the threats for the Instant AP to protect.
  - **Infrastructure**—Specifies the policy for protecting clients from wireless attacks.
  - **Cients**—Prevents unauthorized stations from connecting to your Instant network.

For more information on the intrusion detection feature, see Intrusion Detection on page 469.

Routing

The **Routing** section displays the following list of parameters:

- **Destination**— Lists the destination network that is reachable through the VPN tunnel.
- **Netmask**—Lists the subnet mask to the destination.
- **Gateway**—Lists the gateway to which the traffic must be routed.
- **Metric**—Lists a metric value for the datapath route.

Tunneling

The **Tunneling** section displays the following list of parameters:

- **Controller** —Allows you to configure VPN protocols for remote access. See Understanding VPN Features on page 317 for more information.
- **Enterprise Domains**—Allows you to view or configure the DNS domain names that are valid in the enterprise network. See Configuring Enterprise Domains on page 274 for more information.

Services

The **Services** window consists of the following tabs:

- **AirGroup**—Allows you to configure the AirGroup and AirGroup services. For more information, see Configuring AirGroup on page 399.
- **RTLS**—Allows you to integrate AMP or third-party RTLS such as Aeroscout RTLS with Instant. For more information, see Configuring an Instant AP for RTLS Support on page 408.
- The RTLS tab also allows you to integrate Instant AP with the ALE. For more information about configuring anInstant AP for ALE integration, see Configuring an Instant AP for ALE Support on page 410.

- **CALEA**—Allows you configure support for CALEA server integration, thereby ensuring compliance with Lawful Intercept and CALEA specifications. For more information, see CALEA Integration and Lawful Intercept Compliance on page 419.
- **Network Integration**—Allows you to configure an Instant AP for integration with Palo Alto Networks Firewall and XML API server. For more information on Instant AP integration with PAN, see Integrating an Instant AP with Palo Alto Networks Firewall on page 414and Integrating an Instant AP with an XML API Interface on page 415.
- **Dynamic DNS**—Allows you to configure dynamic DNS on Distributed L3 clients. For more information on Dynamic DNS, see Dynamic DNS Registration on page 329.
- **Clarity**—Allows you to configure Clarity Live for generating inline monitoring statistics. For more information, see Clarity Live on page 411.
- **Openflow**—Allows you to configure OpenFlow services on the Instant AP. For more information, see SDN on page 430.
- **IoT**—Allows you to configure IoT endpoints on the Instant AP. For more information, see BLE IoT for Data Communication on page 424.

DHCP Server

The **DHCP Servers** window allows you to configure various DHCP modes. For more information, see DHCP Configuration on page 294.

Maintenance

The **Maintenance** tab displays a window that allows you to maintain the Wi-Fi network. The **Maintenance** tab consists of the following sections:

- **About**—Displays the name of the product, build time, Instant AP model name, the Instant version, website address of Aruba Networks , copyright information, and the cloud activation key.
- **Firmware**—Displays the current firmware version and provides various options to upgrade to a new firmware version. For more information, refer to the *ArubaInstant Release Notes*.
- **Configuration**—Displays the following details:
  - **Current Configuration**—Displays the current configuration details.
  - **Clear Configuration**—Allows you to clear the current configuration details of the network. Select the **Remove all configurations including per-AP settings and certificates** checkbox to remove the per-AP settings and certificates as well.



The **Remove all configurations including per-AP settings and certificates** option is applicable only to clear configurations. It is not applicable to backup and restore configurations.

  - **Backup Configuration**—Allows you to back up local configuration details. The backed up configuration data is saved in the file named **instant.cfg**.
  - **Restore Configuration**—Allows you to restore the backed up configuration. After restoring the configuration, the Instant AP must be rebooted for the changes to take effect.
- **Certificates**—Displays information about the certificates installed on the Instant AP. You can also upload new certificates to the Instant AP database. For more information, see Authentication Certificates on page 254.
- **Reboot**—Displays the Instant APs in the network and provides an option to reboot the required Instant AP or all Instant APs. For more information, refer to the *Aruba Instant Release Notes*.

- **Convert**—Provides an option to convert an Instant AP to a Mobility Controller managed Remote AP or Campus AP, or to the default virtual controller mode. For more information, see Converting an Instant AP to a Remote AP and Campus AP on page 499.
- **DRT**—Displays the DRT version running in an Instant AP. The DRT window contains the following sections:
  - **Manual**—Displays the current DRT version of the Instant AP. You can manually upgrade the DRT version by uploading a DRT file or by entering the URL.
  - **Reset**—Resets the DRT version.
  - **Automatic**—Enables an automatic DRT version upgrade.

Support

The **Support** tab consists of the following details:

- **Command**—Allows you to select a support command for execution.
- **Target**—Displays a list of Instant APs in the network.
- **Run**—Allows you to execute the selected command for a specific Instant AP or all Instant APs and view logs.
- **Auto Run**—Allows you to configure a schedule for automatic execution of a support command for a specific Instant AP or all Instant APs.
- **Filter**—Allows you to filter the contents of a command output.
- **Clear**—Clears the command output that is displayed after a command is executed.
- **Save**—Allows you to save the support command logs as an HTML or text file.

For more information on support commands, see Running Debug Commands on page 511.

InstantOld User Interface

This chapter describes the following WebUI elements:

- Login Screen on page 42
- Main Window on page 42

Login Screen

The Instant login page allows you to perform the following tasks:

- View Instant Network Connectivity summary
- View the WebUI in a specific language
- Log in to the WebUI

Viewing Connectivity Summary

The login page also displays the connectivity status to the Instant network. The users can view a summary that indicates the status of the Internet availability, uplink, cellular modem and signal strength, VPN, and AirWave configuration details before logging in to the WebUI.

Language

The **Language** drop-down list contains the available languages and allows users to select their preferred language before logging in to the WebUI. A default language is selected based on the language preferences in the client desktop operating system or browser. If Instant cannot detect the language, then **English** is used as the default language.

You can also select the required language option from the **Languages** drop-down list located on the Instant main window.

Logging into the WebUI

To log in to the WebUI, enter the following credentials:

- Username—admin
- Password—Enter the Serial Number of the Instant AP.

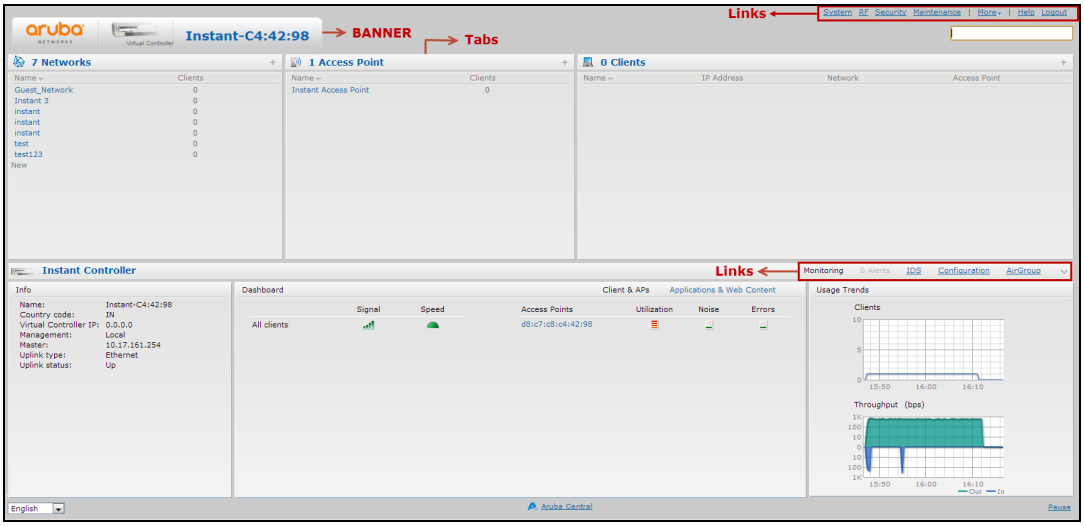
The WebUI main window is displayed.

When you log in to an Instant AP with the factory default settings, a popup box displays an option to sign up for the Aruba cloud solution and enable Instant AP management through Central. To sign up for a free 90-day trial of Central, click here.

Main Window

After you log in to Instant, the WebUI main window is displayed.

Figure 2 *Instant Main Window*



The main window consists of the following elements:

- Banner
- Search Text Box
- Tabs
- Links
- Views

Banner

The banner is a horizontal grey rectangle that appears on the Instant main window. It displays the company name, logo, and the virtual controller name.

Search Text Box

Administrators can search for an Instant AP, client, or a network in the **Search** text box. When you type a search text, the search function suggests matching keywords and allows you to automatically complete the search text entry.

Tabs

The Instant main window consists of the following tabs:

- Network Tab—Provides information about the network profiles configured in the Instant network.
- Access Points Tab—Provides information about the Instant APs configured in the Instant network.
- Clients Tab—Provides information about the clients in the Instant network.

Each tab appears in a compressed view by default. The number of networks, Instant APs, or clients in the network precedes the coresponding tab names. The individual tabs can be expanded or collapsed by clicking the tabs. The list items in each tab can be sorted by clicking the triangle icon next to the heading labels.

Network Tab

This tab displays a list of Wi-Fi networks that are configured in the Instant network. The network names are displayed as links. The expanded view displays the following information about each WLAN SSID:

- **Name**—Name of the network.
- **Clients**—Number of clients that are connected to the network.
- **Type**—Type of network such as Employee, Guest, or Voice.
- **Band**—Band in which the network is broadcast: 2.4 GHz band, 5 GHz band, or both.
- **Authentication Method**—Authentication method required to connect to the network.
- **Key Management**—Authentication key type.
- **IP Assignment**—Source of IP address for the client.
- **Zone**—Instant AP zone configured on the SSID.

To add a wireless network profile, click the **New** link on the **Network** tab. To edit, click the **edit** link that is displayed on clicking the network name in the **Network** tab. To delete a network, click the **x** link.

For more information on the procedure to add or modify a wireless network, see Wireless Network Profiles on page 130.

Access Points Tab

If the Auto-Join Mode feature is enabled, a list of enabled and active Instant APs in the Instant network is displayed on the **Access Points** tab. The Instant AP names are displayed as links. If the Auto Join Mode feature is disabled, the **New** link is displayed. Click this link to add a new Instant AP to the network. If an Instant AP is configured and not active, its MAC Address is displayed in red.

The expanded view of the **Access Points** tab displays the following information about each Instant AP:

- **Name**—Name of the Instant AP. If the Instant AP functions as a master Instant AP in the network, the asterisk sign "*****" is displayed next to the Instant AP.
- **IP Address**—IP address of the Instant AP.
- **Mode**—Mode of the Instant AP.
- **Access**—In this mode, the Instant AP serves clients and scans the home channel for spectrum analysis while monitoring channels for rogue Instant APs in the background.
- **Monitor**—In this mode, the Instant AP acts as a dedicated AM, scanning all channels for rogue Instant APs and clients.
- **Spectrum**—When enabled, the Instant AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference from neighboring Instant APs or non-Wi-Fi devices such as microwaves and cordless phones. When Spectrum is enabled, the Instant AP does not provide access services to clients.
- **Clients**—Number of clients that are currently associated to the Instant AP.
- **Type**—Model number of the Instant AP.
- **Mesh Role**—Role of the Instant AP as a mesh portal or mesh point.
- **Zone**—Instant AP zone.
- **Serial number**—Serial number of the device.
- **Channel**—Channel on which the Instant AP is currently broadcast.
- **Power (dB)**—Maximum transmission EIRP of the radio.
- **Utilization (%)**—Percentage of time that the channel is utilized.
- **Noise (dBm)**—Noise floor of the channel.

An **edit** link is displayed on clicking the Instant AP name. For details on editing Instant AP settings, see Customizing Instant AP Settings on page 78.

Clients Tab

This tab displays a list of clients that are connected to the Instant network. The client names are displayed as links. The expanded view displays the following information about each client:

- **Name**—Username of the client or guest users if available.
- **IP Address**—IP address of the client.
- **MAC Address**—MAC address of the client.
- **OS**—Operating system that runs on the client.
- **ESSID**—ESSID to which the client is connected.
- **Access Point**—Instant AP to which the client is connected.
- **Channel**—The client operating channel.
- **Type**—Type of the Wi-Fi client.
- **Role**—Role assigned to the client.
- **IPv6 Address**—IPv6 address assigned to the client.
- **Signal**—Current signal strength of the client, as detected by the Instant AP.
- **Speed (Mbps)**—Current speed at which data is transmitted. When the client is associated with an Instant AP, it constantly negotiates the speed of data transfer. A value of 0 means that the Instant AP has not heard from the client for some time.

Links

The following links allow you to configure various features for the Instant network:

- New Version Available
- System
- RF
- Security
- Maintenance
- Tunneling
- Help
- Logout
- Info
- Client Match
- AppRF
- Spectrum
- Alerts
- IDS
- This AirGroup link provides an overall view of your AirGroup configuration. Click each parameter to view or edit the settings.
- Configuration
- AirWave Setup
- Pause/Resume

Each of these links is explained in the subsequent sections.

New Version Available

This link is displayed on the Instant main window only if a new image version is available on the image server and AirWave is not configured. For more information on the **New version available** link and its functions, refer to the *Aruba Instant Release Notes*.

System

This link displays the **System** window. The **System** window consists of the following tabs:



Use the **Show/Hide Advanced** option of the **System** window to view or hide the advanced options.

- **General**—Allows you to configure, view, or edit the Name, IP address, NTP Server, and other Instant AP settings for the virtual controller.
- **Admin**—Allows you to configure administrator credentials for access to the virtual controller management UI. You can also configure AirWave in this tab. For more information on management interface and AirWave configuration, see Overview of Instant AP Users on page 207 and Managing an Instant AP from AirWave on page 439, respectively.
- **Uplink**—Allows you to view or configure uplink settings. See Uplink Configuration on page 454 for more information.
- **L3 Mobility**—Allows you to view or configure the Layer-3 mobility settings. See Configuring Layer-3 Mobility on page 484 for more information.
- **Enterprise Domains**—Allows you to view or configure the DNS domain names that are valid in the enterprise network. See Configuring Enterprise Domains on page 274 for more information.
- **Monitoring**—Allows you to view or configure the following details:
  - **Syslog**—Allows you to view or configure Syslog server details for sending syslog messages to the external servers. See Configuring Syslog Servers on page 509 for more information.
  - **TFTP Dump**—Allows you to view or configure a TFTP dump server for core dump files. See Configuring TFTP Dump Server on page 511 for more information.
  - **SNMP**—Allows you to view or configure SNMP agent settings. See Configuring SNMP on page 506 for more information.
- **WISPr**—Allows you to view or configure the WISPr settings. See WISPr Authentication on page 221 for more information.
- **Proxy**—Allows you to configure HTTP proxy on an Instant AP. Refer to the *Aruba Instant Release Notes* for more information.
- **Time Based Services**—Allows you to configure a time profile which can be assigned to the SSID configured on the Instant AP. See Configuring Time-Based Services on page 312

RF

The **RF** link displays a window for configuring ARM and Radio features.

- **ARM**—Allows you to view or configure channel and power settings for all the Instant APs in the network. For information on ARM configuration, see ARM Overview on page 369.
- **Radio**—Allows you to view or configure radio settings for 2.4 GHz and the 5 GHz radio profiles. For information on Radio, see Configuring Radio Settings on page 377.

Security

The **Security** link displays a window with the following tabs:

- **Authentication Servers**—Use this tab to configure an external RADIUS server for a wireless network. For more information, see Configuring an External Server for Authentication on page 231.
- **Users for Internal Server**—Use this tab to populate the system's internal authentication server with users. This list is used by networks for which per-user authorization is specified using the internal

authentication server of the virtual controller. For more information on users, see Overview of Instant AP Users on page 207.

- **Roles** —Use this tab to view the roles defined for all the Networks. The Access Rules part allows you to configure permissions for each role. For more information, see Configuring User Roles on page 277 and Configuring ACL Rules for Network Services on page 260.
- **Blacklisting**—Use this tab to blacklist clients. For more information, see Blacklisting Clients on page 251.
- **Firewall Settings**—Use this tab to enable or disable ALG supporting address and port translation for various protocols and to configure protection against wired attacks. For more information, see Configuring ALG Protocols on page 267 and Configuring Firewall Settings for Protection from ARP Attacks on page 267
- **Inbound Firewall**—Use this tab to enhance the inbound firewall by allowing the configuration of inbound firewall rules, management subnets, and restricted corporate access through an uplink switch. For more information, see Managing Inbound Traffic on page 269.
- **Walled Garden**—Use this tab to allow or prevent access to a selected list of websites. For more information, see Configuring Walled Garden Access on page 202.
- **External Captive Portal**—Use this tab to configure external captive portal profiles. For more information, see Configuring External Captive Portal for a Guest Network on page 189.
- **Custom Blocked Page URL**—Use this tab to create a list of URLs that can be blocked using an ACL rule. For more information, see Creating Custom Error Page for Web Access Blocked by AppRF Policies on page 276.

Maintenance

The **Maintenance** link displays a window that allows you to maintain the Wi-Fi network. The **Maintenance** window consists of the following tabs:

- **About**—Displays the name of the product, build time, Instant AP model name, the Instant version, website address of Aruba Networks , and copyright information.
- **Configuration**—Displays the following details:
  - **Current Configuration**—Displays the current configuration details.
  - **Clear Configuration**—Allows you to clear the current configuration details of the network. Select the **Remove all configurations including per-AP settings and certificates** checkbox to remove the per-AP settings and certificates as well.

    The **Remove all configurations including per-AP settings and certificates** option is applicable only to clear configurations. It is not applicable to backup and restore configurations.

  - **Backup Configuration**—Allows you to back up local configuration details. The backed up configuration data is saved in the file named **instant.cfg**.
  - **Restore Configuration**—Allows you to restore the backed up configuration. After restoring the configuration, the Instant AP must be rebooted for the changes to take effect.
- **Certificates**—Displays information about the certificates installed on the Instant AP. You can also upload new certificates to the Instant AP database. For more information, see Authentication Certificates on page 254.
- **Firmware**—Displays the current firmware version and provides various options to upgrade to a new firmware version. For more information, refer to the *Aruba Instant Release Notes*.
- **Reboot**—Displays the Instant APs in the network and provides an option to reboot the required Instant AP or all Instant APs. For more information, refer to the *Aruba Instant Release Notes*.

- **Convert**—Provides an option to convert an Instant AP to an Mobility Controller managed Remote AP or Campus AP, or to the default virtual controller mode. For more information, see Converting an Instant AP to a Remote AP and Campus AP on page 499.
- **DRT**—Displays the DRT version running in an Instant AP. The DRT window contains the following sections:
  - **Manual**—Displays the current DRT version of the Instant AP. You can manually upgrade the DRT version by uploading a DRT file or by entering the URL.
  - **Reset**—Resets the DRT version.
  - **Automatic**—Enables an automatic DRT version upgrade.

More

The **More** link allows you to select the following options:

- Tunneling
- Routing
- IDS
- Wired
- Services
- DHCP Server
- Support

The **Tunneling** window displays the following list of parameters:

- **Controller** —Allows you to configure VPN protocols for remote access. See Understanding VPN Features on page 317 for more information.
- **Enterprise Domains**—Allows you to view or configure the DNS domain names that are valid in the enterprise network. See Configuring Enterprise Domains on page 274 for more information.

The **Routing** window displays the following list of parameters:

- **Destination**— Lists the destination network that is reachable through the VPN tunnel.
- **Netmask**—Lists the subnet mask to the destination.
- **Gateway**—Lists the gateway to which the traffic must be routed.
- **Metric**—Lists a metric value for the datapath route.

The **IDS** window allows you to configure wireless intrusion detection and protection levels.

For more information on wireless intrusion detection and protection, see Detecting and Classifying Rogue APs on page 469.

The **Wired** window allows you to configure a wired network profile. See Wired Profiles on page 161 for more information.

The **Services** window allows you to configure services such as AirGroup and RTLS. The Services window consists of the following tabs:

- **AirGroup**—Allows you to configure the AirGroup and AirGroup services. For more information, see Configuring AirGroup on page 399.
- **RTLS**—Allows you to integrate AMP or third-party RTLS such as Aeroscout RTLS with Instant. For more information, see Configuring an Instant AP for RTLS Support on page 408.
- The RTLS tab also allows you to integrate Instant AP with the ALE. For more information about configuring an Instant AP for ALE integration, see Configuring an Instant AP for ALE Support on page 410.
- **CALEA**—Allows you configure support for CALEA server integration, thereby ensuring compliance with Lawful Intercept and CALEA specifications. For more information, see CALEA Integration and Lawful Intercept Compliance on page 419.
- **Network Integration**—Allows you to configure an Instant AP for integration with Palo Alto Networks Firewall and XML API server. For more information on Instant AP integration with PAN, see Integrating an Instant AP with Palo Alto Networks Firewall on page 414and Integrating an Instant AP with an XML API Interface on page 415.
- **Dynamic DNS**—Allows you to configure dynamic DNS on Distributed L3 clients. For more information on Dynamic DNS, see Dynamic DNS Registration on page 329.
- **Clarity**—Allows you to configure Clarity Live for generating inline monitoring statistics. For more information, see Clarity Live on page 411.
- **Openflow**—Allows you to configure OpenFlow services on the Instant AP. For more information, see SDN on page 430.
- **IoT**—Allows you to configure IoT endpoints on the Instant AP. For more information, see BLE IoT for Data Communication on page 424.

The **DHCP Servers** window allows you to configure various DHCP modes. For more information, see DHCP Configuration on page 294.

The **Support** link consists of the following details:

- **Command**—Allows you to select a support command for execution.
- **Target**—Displays a list of Instant APs in the network.
- **Run**—Allows you to execute the selected command for a specific Instant AP or all Instant APs and view logs.
- **Auto Run**—Allows you to configure a schedule for automatic execution of a support command for a specific Instant AP or all Instant APs.
- **Filter**—Allows you to filter the contents of a command output.
- **Clear**—Clears the command output that is displayed after a command is executed.
- **Save**—Allows you to save the support command logs as an HTML or text file.

For more information on support commands, see Running Debug Commands on page 511.

Help

The **Help** link allows you to view a short description or definition of the selected terms in the UI windows or the dialog boxes.

To activate the context-sensitive help:

1. Click the **Help** link available above the Search bar on the Instant main window.
2. Click any text or term displayed in green italics to view its description or definition.
3. To disable the help mode, click **Done**.

Logout

The **Logout** link allows you to log out of the Instant UI.

Monitoring

The **Monitoring** link displays the Monitoring pane for the Instant network. Use the down arrow located to the right side of these links to compress or expand the Monitoring pane.

The Monitoring pane consists of the following sections:

- Info
- RF Dashboard
- RF Trends
- Usage Trends
- Mobility Trail

The **Info** section displays the configuration information of the virtual controller by default. On selecting the **Network View** tab, the monitoring pane displays configuration information of the selected network. Similarly, in the **Access Point** or the **Client** view, this section displays the configuration information of the selected Instant AP or the client.

Table 11: *Contents of the Info Section in the Instant Main Window*

Name	Description
Info section in the **Virtual Controller** view	The **Info** section in the **Virtual Controller** view displays the following information: ■ **Name**—Displays the virtual controller name. ■ **Country Code**—Displays the Country in which the virtual controller is operating. ■ **Virtual Controller IP address**—Displays the IP address of the virtual controller. ■ **VC DNS**—Displays the DNS IP address configured for the virtual controller. ■ **Management**—Indicates if the Instant AP is managed locally or through AirWave or Central. ■ **Master**—Displays the IP address of the Instant AP acting as virtual controller. ■ **MAS integration**—Displays the status of the Mobility Access Switch integration feature. ■ **Uplink type**—Displays the type of uplink configured on the Instant AP, for example, Ethernet or 3G. ■ **Uplink status**—Indicates the uplink status. ■ **Blacklisted clients**—Displays the number of blacklisted clients. ■ **Internal RADIUS Users**—Displays the number of internal RADIUS users.

Table 11: *Contents of the Info Section in the Instant Main Window*

Name	Description
	▪ **Internal Guest Users**—Displays the number of internal guest users. ▪ **Internal User Open Slots**—Displays the available slots for user configuration as supported by the Instant AP model.
Info section in the **Network** view	The **Info** section in the **Network** view displays the following information: ▪ **Name**—Displays the name of the network. ▪ **Status**—Displays the status of the network. ▪ **Type**—Displays the type of network, for example, Employee, Guest, or Voice. ▪ **VLAN**—Displays VLAN details. ▪ **IP Assignment**—Indicates if the Instant AP clients are assigned IP address from the network that the virtual controller is connected to, or from an internal autogenerated IP scope from the virtual controller. ▪ **Access**—Indicates the level of access control configured for the network. ▪ **WMM DSCP**—Displays WMM DSCP mapping details. ▪ **Security level**—Indicates the type of user authentication and data encryption configured for the network. The **info** section for WLAN SSIDs also indicates status of captive portal and CALEA ACLs and provides a link to upload certificates for the internal server. For more information, see Authentication Certificates on page 254.
Info section in the **Access Point** view	The **Info** section in the **Access Point** view displays the following information: ▪ **Name**—Displays the name of the selected Instant AP. ▪ **IP Address**—Displays the IP address of the Instant AP. ▪ **Mode**—Displays the mode in which the Instant AP is configured to operate. ▪ **Spectrum**—Displays the status of the spectrum monitor. ▪ **Clients**—Number of clients associated with the Instant AP. ▪ **Type**—Displays the model number of the Instant AP. ▪ **Zone**—Displays Instant AP zone details. ▪ **CPU Utilization**—Displays the CPU utilization in percentage. ▪ **Memory Free**—Displays the memory availability of the Instant AP in MB. ▪ **Serial number**—Displays the serial number of the Instant AP. ▪ **MAC**—Displays the MAC address. ▪ **From Port**—Displays the port from where the slave Instant AP is learned in hierarchy mode.
Info section in the **Client** view	The **Info** section in the **Client** view displays the following information: ▪ **Name**—Displays the name of the client. ▪ **IP Address**—Displays the IP address of the client. ▪ **MAC Address**—Displays MAC address of the client. ▪ **OS**—Displays the operating system that is running on the client. ▪ **ESSID**—Indicates the network to which the client is connected. ▪ **Access Point**—Indicates the Instant AP to which the client is connected.

Table 11: *Contents of the Info Section in the Instant Main Window*

Name	Description
	■ **Channel**—Indicates the channel that is currently used by the client. ■ **Type**—Displays the channel type on which the client is broadcasting. ■ **Role**—Displays the role assigned to the client.

The **RF Dashboard** section lists the Instant APs that exceed the utilization, noise, or error threshold. It also shows the clients with low speed or signal strength in the network and the RF information for the Instant AP to which the client is connected.

The Instant AP names are displayed as links. When an Instant AP is clicked, the Instant AP configuration information is displayed in the Info section and the RF Dashboard section is displayed on the Instant main window.

The following table describes the icons available on the RF Dashboard pane:

Table 12: *RF Dashboard Icons*

Icon number	Name	Description
1	Signal	Displays the signal strength of the client. Signal strength is measured in dB. Depending on the signal strength of the client, the color of the lines on the Signal icon changes in the following order: ■ Green—Signal strength is more than 20 dB. ■ Orange—Signal strength is between 15 dB and 20 dB. ■ Red—Signal strength is less than 15 dB. To view the signal graph for a client, click the signal icon next to the client in the **Signal** column.
2	Speed	Displays the data transfer speed of the client. Depending on the data transfer speed of the client, the color of the Speed icon changes in the following order: ■ Green—Data transfer speed is more than 50% of the maximum speed supported by the client. ■ Orange—Data transfer speed is between 25% and 50% of the maximum speed supported by the client. ■ Red—Data transfer speed is less than 25% of the maximum speed supported by the client. To view the data transfer speed graph of a client, click the speed icon corresponding to the client name in the **Speed** column.
3	Utilization	Displays the radio utilization rate of the Instant APs. Depending on the percentage of utilization, the color of the lines on the Utilization icon changes in the following order: ■ Green—Utilization is less than 50%. ■ Orange—Utilization is between 50% and 75%. ■ Red—Utilization is more than 75%. To view the utilization graph of an Instant AP, click the Utilization icon next to the Instant AP in the **Utilization** column.

Table 12: *RF Dashboard Icons*

Icon number	Name	Description
4	Noise	Displays the noise floor details for the Instant APs. Noise is measured in decibel per meter. Depending on the noise floor, the color of the lines on the Noise icon changes in the following order: ■ Green—Noise floor is more than -87 dBm. ■ Orange—Noise floor is between -80 dBm and -87 dBm. ■ Red—Noise floor is less than -80 dBm. To view the noise floor graph of an Instant AP, click the Noise icon next to the Instant AP in the **Noise** column.
5	Errors	Displays the errors for the Instant APs. Depending on the errors, color of the lines on the Errors icon changes in the following order: ■ Green—Errors are less than 5000 frames per second. ■ Orange—Errors are between 5000 and 10,000 frames per second. ■ Red—Errors are more than 10000 frames per second. To view the errors graph of an Instant AP, click the Errors icon next to the Instant AP in the **Errors** column.

The **RF Trends** section displays the graphs for the selected Instant AP and the client. To view the details on the graphs, click the graphs and hover the mouse on a data point.

The following table describes the RF trends graphs available in the Client view:

Table 13: *Client View—RF Trends Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Signal	The Signal graph shows the signal strength of the client for the last 15 minutes. It is measured in dB. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average signal statistics of the client for the last 15 minutes. To see the exact signal strength at a particular time, move the cursor over the graph line.	To monitor the signal strength of the selected client for the last 15 minutes: 1. Log in to the Instant UI. The virtual controller view is displayed. This is the default view. 2. On the **Clients** tab, click the IP address of the client for which you want to monitor the signal strength. 3. Study the Signal graph in the RF Trends pane. For example, the graph shows that signal strength for the client is 54.0 dB at 12:23 hours.
Frames	The Frames graph shows the In and Out frame rate per second of the client for the last 15 minutes. It also shows data for the Retry In and Retry Out frames. ■ Outgoing frames—Outgoing frame traffic is displayed in green. It is shown above the median line.	To monitor the In and Out frame rate per second and retry frames for the In and Out traffic, for the last 15 minutes: 1. Log in to the Instant UI. The virtual controller view is displayed. This is the default view. 2. On the **Clients** tab, click the IP address of the client for which you want to monitor the

Table 13: *Client View—RF Trends Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
	▪ Incoming frames—Incoming frame traffic is displayed in blue. It is shown below the median line. ▪ Retry Out—Retries for the outgoing frames are displayed above the median line in black . ▪ Retry In—Retries for the incoming frames are displayed below the median line in red. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In, Out, Retries In, and Retries Out frames. To see the exact frames at a particular time, move the cursor over the graph line.	frames. 3. Study the Frames graph in the RF Trends pane. For example, the graph shows 4.0 frames per second for the client at 12:27 hours.
Speed	The Speed graph shows the data transfer speed for the client. Data transfer is measured in Mbps. To see an enlarged view, click the graph. The enlarged view shows Last, Minimum, Maximum, and Average statistics of the client for the last 15 minutes. To see the exact speed at a particular time, move the cursor over the graph line.	To monitor the speed for the client for the last 15 minutes: 1. Log in to the Instant UI. The virtual controller view is displayed. This is the default view. 2. On the **Clients** tab, click the IP address of the client for which you want to monitor the speed. 3. Study the Speed graph in the RF Trends pane. For example, the graph shows that the data transfer speed at 12:26 hours is 240 Mbps.
Throughput	The Throughput Graph shows the throughput of the selected client for the last 15 minutes. ▪ Outgoing traffic—Throughput for the outgoing traffic is displayed in green. It is shown above the median line. ▪ Incoming traffic—Throughput for the incoming traffic is displayed in blue. It is shown below the median line. To see an enlarged view, click the graph. The enlarged view shows Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the client for the last 15 minutes. To see the exact throughput at a particular time, move the cursor over the graph line.	To monitor the errors for the client for the last 15 minutes: 1. Log in to the Instant UI. The virtual controller view is displayed. This is the default view. 2. In the **Clients** tab, click the IP address of the client for which you want to monitor the throughput. 3. Study the Throughput graph in the RF Trends pane. For example, the graph shows 1.0 Kbps outgoing traffic throughput for the client at 12:30 hours.

The **Usage Trends** section displays the following graphs:

- **Clients**—In the default view, the Clients graph displays the number of clients that were associated with the virtual controller in the last 15 minutes. In Network view or the Access Point view, the graph displays the number of clients that were associated with the selected network or Instant AP in the last 15 minutes.
- **Throughput**—In the default view, the Throughput graph displays the incoming and outgoing throughput traffic for the virtual controller in the last 15 minutes. In the Network view or the Access Point view, the graph displays the incoming and outgoing throughput traffic for the selected network or Instant AP in the last 15 minutes.

The following table describes the graphs displayed in the Network view:

Table 14: *Network View–Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Clients	The Clients graph shows the number of clients associated with the network for the last 15 minutes. To see an enlarged view, click the graph. ▪ The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the virtual controller for the last 15 minutes. ▪ To see the exact number of clients in the Instant network at a particular time, move the cursor over the graph line.	To check the number of clients associated with the network for the last 15 minutes: 1. Log in to the Instant UI. The virtual controller view is displayed. This is the default view. 2. On the **Network** tab, click the network for which you want to check the client association. 3. Study the Clients graph in the **Usage Trends** pane. For example, the graph shows that one client is associated with the selected network at 12:00 hours.
Throughput	The Throughput graph shows the throughput of the selected network for the last 15 minutes. ▪ Outgoing traffic—Throughput for the outgoing traffic is displayed in green. Outgoing traffic is shown above the median line. ▪ Incoming traffic—Throughput for the incoming traffic is displayed in blue. Incoming traffic is shown below the median line. To see an enlarged view, click the graph. ▪ The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the network for the last 15 minutes. To see the exact throughput of the selected network at a particular time, move the cursor over the graph line.	To check the throughput of the selected network for the last 15 minutes, 1. Log in to the Instant UI. The virtual controller view is displayed. This is the default view. 2. On the **Network** tab, click the network for which you want to check the client association. 3. Study the Throughput graph in the **Usage Trends** pane. For example, the graph shows 22.0 Kbps incoming traffic throughput for the selected network at 12:03 hours.

The following table describes the graphs displayed in the Access Point view:

Table 15: *Access Point View—Usage Trends and Monitoring Procedures*

Graph Name	Instant AP Description	Monitoring Procedure
Neighboring Instant APs	The Neighboring Instant APs graph shows the number of Instant APs detected by the selected Instant AP: ■ Valid Instant APs: An Instant AP that is part of the enterprise providing WLAN service. ■ Interfering Instant APs: An Instant AP that is seen in the RF environment but is not connected to the network. ■ Rogue Instant APs: An unauthorized Instant AP that is plugged into the wired side of the network. To see the number of different types of neighboring Instant APs for the last 15 minutes, move the cursor over the respective graph lines.	To check the neighboring Instant APs detected by the Instant AP for the last 15 minutes: 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Access Points** tab, click the Instant AP for which you want to monitor the client association. 3. Study the Neighboring Instant APs graph in the **Overview** section. For example, the graph shows that 148 interfering Instant APs are detected by the Instant AP at 12:04 hours.
CPU Utilization	The CPU Utilization graph displays the utilization of CPU for the selected Instant AP. To see the CPU utilization of the Instant AP, move the cursor over the graph line.	To check the CPU utilization of the Instant AP for the last 15 minutes: 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Access Points** tab, click the Instant AP for which you want to monitor the client association. 3. Study the CPU Utilization graph in the **Overview** pane. For example, the graph shows that the CPU utilization of the Instant AP is 30% at 12:09 hours.
Neighboring Clients	The Neighboring Clients graph shows the number of clients not connected to the selected Instant AP, but heard by it. ■ Any client that successfully authenticates with a valid Instant AP and passes encrypted traffic is classified as a valid client. ■ Interfering: A client associated to any Instant AP and is not valid is classified as an interfering client. To see the number of different types of neighboring clients for the last 15 minutes, move the cursor over the respective graph lines.	To check the neighboring clients detected by the Instant AP for the last 15 minutes, 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Access Points** tab, click the Instant AP for which you want to monitor the client association. 3. Study the Neighboring Clients graph in the **Overview** pane. For example, the graph shows that 20 interfering clients were detected by the Instant AP at 12:15 hours.
Memory free (MB)	The Memory free graph displays the memory availability of the Instant AP in MB.	To check the free memory of the Instant AP for the last 15 minutes:

Table 15: *Access Point View—Usage Trends and Monitoring Procedures*

Graph Name	Instant AP Description	Monitoring Procedure
	To see the free memory of the Instant AP, move the cursor over the graph line.	1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Access Points** tab, click the Instant AP for which you want to monitor the client association. 3. Study the Memory free graph in the **Overview** pane. For example, the graph shows that the free memory of the Instant AP is 64 MB at 12:13 hours.
Clients	The Clients graph shows the number of clients associated with the selected Instant AP for the last 15 minutes. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the Instant AP for the last 15 minutes. To see the exact number of clients associated with the selected Instant AP at a particular time, move the cursor over the graph line.	To check the number of clients associated with the Instant AP for the last 15 minutes: 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Access Points** tab, click the Instant AP for which you want to monitor the client association. 3. Study the Clients graph. For example, the graph shows that six clients are associated with the Instant AP at 12:11 hours.
Throughput	The Throughput graph shows the throughput for the selected Instant AP for the last 15 minutes. ▪ Outgoing traffic—Throughput for the outgoing traffic is displayed in green. It is shown above the median line. ▪ Incoming traffic—Throughput for the incoming traffic is displayed in blue. It is shown below the median line. To see an enlarged view, click the graph. ▪ The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the Instant AP for the last 15 minutes. To see the exact throughput of the selected Instant AP at a particular time, move the cursor over the graph line.	To check the throughput of the selected Instant AP for the last 15 minutes: 1. Log in to the Instant UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Access Points** tab, click the Instant AP for which you want to monitor the throughput. 3. Study the Throughput graph. For example, the graph shows 44.03 Kbps incoming traffic throughput at 12:08 hours.

The **Mobility Trail** section displays the following mobility trail information for the selected client:

- **Association Time**—The time at which the selected client was associated with a particular Instant AP. The Instant UI shows the client and Instant AP association over the last 15 minutes.
- **Access Point**—The Instant AP name with which the client was associated.

NOTE

Mobility information about the client is reset each time it roams from one Instant AP to another.

Client Match

If Client Match is enabled, the **Client Match** link provides a graphical representation of radio map view of an Instant AP and the client distribution on an Instant AP radio.

On clicking an access point in the **Access Points** tab and the **Client Match** link, a stations map view is displayed and a graph is drawn with real-time data points for the Instant APradio. If the Instant AP supports dual-band, you can toggle between 2.4 GHz and 5 GHz links in the Client Match graph area to view the data. When you hover the mouse on the graph, details such as RSSI, Client Match status, and the client distribution on channels are displayed.

On clicking a client in the **Clients** tab and the **Client Match** link, a graph is drawn with real-time data points for an Instant AP radio map. When you hover the mouse on the graph, details such as RSSI, channel utilization details, and client count on each channel are displayed.

AppRF

The **AppRF** link displays the application traffic summary for Instant APs and client devices. The **AppRF** link in the activity panel is displayed only if **AppRF visibility** is enabled in the **System** window. For more information on application visibility and AppRF charts, see Application Visibility on page 383.

Spectrum

The spectrum link (in **Access Point** view) displays the spectrum data that is collected by a hybrid Instant AP or by an Instant AP that has enabled spectrum monitor. The spectrum data is not reported to the virtual controller.

The spectrum link displays the following:

- **Device list**—The device list display consists of a device summary table and channel information for active non Wi-Fi devices currently seen by a spectrum monitor or a hybrid Instant AP radio.
- **Channel Utilization and Monitoring**—This chart provides an overview of channel quality across the spectrum. It shows channel utilization information such as channel quality, availability, and utilization metrics as seen by a spectrum monitor for the 2.4 GHz and 5 GHz radio bands. The first bar for each channel represents the percentage of airtime used by non-Wi-Fi interference and Wi-Fi devices. The second bar indicates the channel quality. A higher percentage value indicates better quality.
- **Channel Details**—When you move your mouse over a channel, the channel details or the summary of the 2.4 GHz and 5 GHz channels as detected by a spectrum monitor are displayed. You can view the aggregate data for each channel seen by the spectrum monitor radio, including the maximum Instant AP power, interference, and the SNIR. Spectrum monitors display spectrum analysis data seen on all channels in the selected band, and hybrid Instant APs display data from the single channel that they are monitoring.

For more information on spectrum monitoring, see Spectrum Monitor on page 486.

Alerts

Alerts are generated when a user encounters problems while accessing or connecting to a network. The alerts that are generated can be categorized as follows:

- 802.11-related association and authentication failure alerts
- 802.1X-related mode and key mismatch, server, and client time-out failure alerts
- IP-address-related failures—Static IP address or DHCP-related alerts.

The **Alerts** link displays the following types of alerts:

- Client Alerts
- Active Faults
- Fault History

Table 16: *Types of Alerts*

Type of Alert	Description	Information Displayed
Client Alerts	The alert type, **Client Alerts**, occur when clients are connected to the Instant network.	The alert type, **Client Alert** displays the following information: ■ **Timestamp**—Displays the time at which the client alert was recorded. ■ **MAC address**—Displays the MAC address of the client that caused the alert. ■ **Description**—Provides a short description of the alert. ■ **Access Points**—Displays the IP address of the Instant AP to which the client is connected. ■ **Details**—Provides complete details of the alert.
Active Faults	The **Active Faults** alerts occur in the event of a system fault.	The **Active Faults** alerts consists of the following information: ■ **Time**—Displays the system time when an event occurs. ■ **Number**—Indicates the number of sequence. ■ **Description**—Displays the event details.
Fault History	The **Fault History** alerts display the historic system faults.	The **Fault History** alert displays the following information: ■ **Time**—Displays the system time when an event occurs. ■ **Number**—Indicates the number of sequence. ■ **Cleared by**—Displays the module which cleared this fault. ■ **Description**—Displays the event details.

The following table displays a list of alerts that are generated in the Instant AP network:

Table 17: *Alerts List*

Description Code	Description	Details	Corrective Actions
100101	Internal error	The Instant AP has encountered an internal error for this client.	Contact the Aruba customer support team.
100102	Unknown SSID in association request	The Instant AP cannot allow this client to associate because the association request received contains an unknown SSID.	Identify the client and check its Wi-Fi driver and manager software.

Table 17: *Alerts List*

Description Code	Description	Details	Corrective Actions
100103	Mismatched authentication or encryption setting	The Instant AP cannot allow this client to associate because its authentication or encryption settings do not match AP's configuration.	Ascertain the correct authentication or encryption settings and try to associate again.
100104	Unsupported 802.11 rate	The Instant AP cannot allow this client to associate because it does not support the 802.11 rate requested by this client.	Check the configuration on the Instant AP to see if the desired rate can be supported; if not, consider replacing the Instant AP with another model that can support the rate.
100105	Maximum capacity reached on Instant AP	The Instant AP has reached maximum capacity and cannot accommodate any more clients.	Consider expanding capacity by installing additional Instant APs or balance load by relocating Instant APs.
100206	Invalid MAC Address	The Instant AP cannot authenticate this client because its MAC address is not valid.	This condition may be indicative of a misbehaving client. Try to locate the client device and check its hardware and software.
100307	Client blocked due to repeated authentication failures	The Instant AP is temporarily blocking the 802.1X authentication request from this client because the credentials provided have been rejected by the RADIUS server too many times.	Identify the client and check its 802.1X credentials.
100308	RADIUS server connection failure	The Instant AP cannot authenticate this client using 802.1X because the RADIUS server did not respond to the authentication request. If the Instant AP is using the internal RADIUS server, it is recommend to check the related configuration as well as the installed certificate and passphrase.	If the Instant AP is using the internal RADIUS server, Aruba recommends checking the related configuration as well as the installed certificate and passphrase. If the Instant AP is using an external RADIUS server, check if there are any issues with the RADIUS server and try connecting again.
100309	RADIUS server authentication failure	The Instant AP cannot authenticate this client using 802.1X, because the RADIUS server rejected the authentication credentials (for example, password) provided by the client.	Ascertain the correct authentication credentials and log in again.

Table 17: *Alerts List*

Description Code	Description	Details	Corrective Actions
100410	Integrity check failure in encrypted message	The Instant AP cannot receive data from this client because the integrity check of the received message has failed. Recommend checking the encryption setting on the client and on the Instant AP.	Check the encryption setting on the client and on the Instant AP.
100511	DHCP request timed out	This client did not receive a response to its DHCP request in time. Recommend checking the status of the DHCP server in the network.	Check the status of the DHCP server in the network.
101012	Wrong Client VLAN	VLAN mismatch between the Instant AP and the upstream device. Upstream device can be upstream switch or RADIUS server.	

IDS

The **IDS** link displays a list of foreign Instant APs and foreign clients that are detected in the network. It consists of the following sections:

- **Foreign Access Points Detected**—Lists the Instant APs that are not controlled by the virtual controller. The following information is displayed for each foreign Instant AP:
  - **MAC address**—Displays the MAC address of the foreign Instant AP.
  - **Network**—Displays the name of the network to which the foreign Instant AP is connected.
  - **Classification**—Displays the classification of the foreign Instant AP, for example, Interfering Instant AP or Rogue Instant AP.
  - **Channel**—Displays the channel in which the foreign Instant AP is operating.
  - **Type**—Displays the Wi-Fi type of the foreign Instant AP.
  - **Last seen**—Displays the time when the foreign Instant AP was last detected in the network.
  - **Where**—Provides information about the Instant AP that detected the foreign Instant AP. Click the push pin icon to view the information.
- **Foreign Clients Detected**— Lists the clients that are not controlled by the virtual controller. The following information is displayed for each foreign client:
  - **MAC address**—Displays the MAC address of the foreign client.
  - **Network**—Displays the name of the network to which the foreign client is connected.
  - **Classification**—Displays the classification of the foreign client: Interfering client.
  - **Channel**—Displays the channel in which the foreign client is operating.
  - **Type**—Displays the Wi-Fi type of the foreign client.
  - **Last seen**—Displays the time when the foreign client was last detected in the network.

- **Where**—Provides information about the Instant AP that detected the foreign client. Click the Push Pin icon to view the information.

For more information on the intrusion detection feature, see Intrusion Detection on page 469.

AirGroup

This **AirGroup** link provides an overall view of your AirGroup configuration. Click each parameter to view or edit the settings.

- **MAC**—Displays the MAC address of the AirGroup servers.
- **IP**—Displays the IP address of the AirGroup servers.
- **Host Name**—Displays the machine name or host name of the AirGroup servers.
- **Service**— Displays the type of services such as AirPlay or AirPrint.
- **VLAN**—Displays VLAN details of the AirGroup servers.
- **Wired/Wireless**—Displays if the AirGroup server is connected through a wired or wireless interface.
- **Role**—Displays the user role if the server is connected through 802.1X authentication. If the server is connected through phase-shift keying or open authentication, this parameter is blank.
- **Group**—Displays the group.
- **CPPM**—By clicking this, you get details of the registered rules in ClearPass Policy Manager for this server.
- **MDNS Cache**—By clicking this, you receive MDNS record details of a particular server.

Configuration

The **Configuration** link provides an overall view of your virtual controller, Instant APs, and WLAN SSID configuration.

AirWave Setup

AirWave is a solution for managing rapidly changing wireless networks. When enabled, AirWave allows you to manage the Instant network. For more information on AirWave, see Managing an Instant AP from AirWave on page 439. The AirWave status is displayed below the virtual controller section of the Instant main window. If the AirWave status is **Not Set Up**, click the **Set Up Now** link to configure AirWave. The **System > Admin** window is displayed.

Central

The Instant UI provides a link to launch a support portal for Central. You can use Central's evaluation accounts through this website and get registered for a free account. You must fill in the registration form available on this page. After you complete this process, an activation link will be sent to your registered ID to get started.

Pause/Resume

The **Pause/Resume** link is located on the Instant main window.

The Instant UI is automatically refreshed every 15 seconds by default. Click the **Pause** link to pause the automatic refreshing of the Instant UI after every 15 seconds. When the automatic refreshing is paused, the **Pause** link changes to **Resume**. Click the **Resume** link to resume automatic refreshing.

Automatic refreshing allows you to get the latest information about the network and network elements. You can use the **Pause** link when you want to analyze or monitor the network or a network element, and therefore do not want the UI to refresh.

Views

Depending on the link or tab that is clicked, Instant displays information about the virtual controller, Wi-Fi networks, Instant APs, or the clients in the Info section. The views on the Instant main window are classified as follows:

- **Virtual Controller** view—The virtual controller view is the default view. This view allows you to monitor the Instant network. The following WebUI elements are available in this view:
  - **Tabs**—Networks, Access Points, and Clients. For detailed information on the tabs, see Tabs on page 43.
  - **Links**—Monitoring, Client Alerts, and IDS. The Spectrum link is visible if you have configured the Instant AP as a spectrum monitor. These links allow you to monitor the Instant network. For more information on these links, see Info on page 50, IDS on page 61, Alerts on page 58, and Spectrum Monitor on page 486.
- **Network** view—The Network view provides information that is necessary to monitor a selected wireless network. All Wi-Fi networks in the Instant network are listed in the **Network** tab. Click the name of the network that you want to monitor.
- Instant Access Point view—The Instant Access Point view provides information that is necessary to monitor a selected Instant AP. All Instant APs in the Instant network are listed in the **Access Points** tab. Click the name of the Instant AP that you want to monitor.
- **Client** view—The Client view provides information that is necessary to monitor a selected client. In the Client view, all the clients in the Instant network are listed in the **Clients** tab. Click the IP address of the client that you want to monitor.

For more information on the graphs and the views, see Info on page 50.

This chapter consists of the following sections:

- Configuring System Parameters (Old WebUI) on page 64
- Changing Password on page 76

Configuring System Parameters (Old WebUI)

This section describes how to configure the system parameters of an Instant AP using the old WebUI.

Navigate to **System** > **General**.

Table 18: *System Parameters*

Parameter	Description	CLI Configuration
Name	Name of the Instant AP.	▪ `(Instant AP)# name <name>`
System location	Physical location of the Instant AP.	▪ `(Instant AP)#(config)# syslocation <location-name>`
Virtual Controller IP	This parameter allows you to specify a single static IP address that can be used to manage a multi-Instant APInstant network. This IP address is automatically provisioned on a shadow interface on the Instant AP that takes the role of a virtual controller. When anInstant AP becomes a virtual controller, it sends three ARP messages with the static IP address and its MAC address to update the network ARP cache.	▪ `(Instant AP)(config)# virtual-controller-ip <IP-address>`
Allow IPv6 Management	Select the check box to enable IPv6 configuration	
Virtual Controller IPv6	This parameter is used to configure the IPv6 address.	▪ `(Instant AP)(config)# virtual-controller-ipv6 <ipv6 address>`

Table 18: *System Parameters*

Parameter	Description	CLI Configuration
Uplink switch native VLAN	This parameter notifies the Instant AP about the native-VLAN of the upstream switch to which the Instant AP is connected. The parameter stops the Instant AP from sending out tagged frames to clients connected with the SSID that has the same VLAN as the native VLAN of the upstream switch, to which the Instant AP is connected. By default, the Instant AP considers the uplink switch native VLAN value as 1.	■ `(Instant AP)(config)# enet-vlan <vlan-ID>`
Dynamic Proxy	This parameter allows you to enable or disable the dynamic proxy for RADIUS and TACACS servers. ■ **Dynamic RADIUS Proxy**—When dynamic RADIUS proxy is enabled, the virtual controller network will use the IP address of the virtual controller for communication with external RADIUS servers. Ensure that you set the virtual controller IP address as a NAS client in the RADIUS server if Dynamic RADIUS proxy is enabled. ■ **Dynamic TACACS Proxy**—When enabled, the virtual controller network will use the IP address of the virtual controller for communication with external TACACS servers. The IP address is chosen based on one of the following rules: • If a VPN tunnel exists between the Instant AP and the TACACS server, then the IP address of the tunnel interface will be used.	To enable dynamic RADIUS proxy: ■ `(Instant AP)(config)# dynamic-radius-proxy` To enable TACACS proxy: ■ `(Instant AP)(config)# dynamic-tacacs-proxy`

Table 18: *System Parameters*

Parameter	Description	CLI Configuration
	• If a virtual controller IP address is configured, the the same will be used by the virtual controller network to communicate with the external TACACS server. • If a virtual controller IP is not configured, then the IP address of the bridge interface is used. **NOTE:** When dynamic-tacacs-proxy is enabled on the Instant AP, the TACACS server cannot identify the slave Instant AP that generates the TACACS traffic as the source IP address is changed.	
MAS Integration	Select **Enabled**/**Disabled** from the **MAS integration** drop-down list to enable or disable the LLDP protocol for Mobility Access Switch integration. With this protocol, Instant APs can instruct the Mobility Access Switch to turn off ports where rogue access points are connected, as well as take actions such as increasing PoE priority and automatically configuring VLANs on ports where Instant access points are connected.	■ `(Instant AP)(config)# mas-integration`
NTP Server	This parameter allows you to configure NTP servers for the Instant AP. Up to four NTP servers can be configured for the AP, each one separated by a comma. To facilitate communication between various elements in a network, time synchronization between the elements and across the network is critical. Time synchronization allows you to: ■ Trace and track security gaps, monitor network usage, and troubleshoot network issues.	To configure NTP servers: ■ `(Instant AP)(config)# ntp-server <name>,<name2>,<name3>,<name4>` To remove NTP servers: ■ `(Instant AP)(config)# no ntp-server` To view NTP status: ■ `(Instant AP)# show ntp status` or ■ `(Instant AP)# show running-config | include ntp` To view NTP debug logs: ■ `(Instant AP)# show ntp debug`

Table 18: *System Parameters*

Parameter	Description	CLI Configuration
	■ Validate certificates. ■ Map an event on one network element to a corresponding event on another. ■ Maintain accurate time for billing services and similar tasks. NTP helps obtain the precise time from a server and regulate the local time in each network element. Connectivity to a valid NTP server is required to synchronize the Instant AP clock to set the correct time. If NTP server is not configured in the Instant AP network, an Instant AP reboot may lead to variation in time data. By default, the Instant AP tries to connect to **pool.ntp.org** to synchronize time. The NTP server can also be provisioned through the DHCP option 42. If the NTP server is configured, it takes precedence over the DHCP option 42 provisioned value. The NTP server provisioned through the DHCP option 42 is used if no server is configured. The default server **pool.ntp.org** is used if no NTP server is configured or provisioned through DHCP option 42. **NOTE:** To facilitate ZTP using the AMP, Central, or Activate, you must configure the firewall and wired infrastructure to either allow the NTP traffic to pool.ntp.org, or provide alternative NTP servers under DHCP options.	
Timezone	Timezone in which the Instant AP must operate. You can also enable DST on Instant APs if the time zone you selected supports the DST. When enabled, the DST ensures that the Instant APs reflect the seasonal time changes in the region they serve.	To configure timezone: ■ `(Instant AP)(config)# clock timezone <name> <hour-offset> <minute-offset>` To configure DST: ■ `(Instant AP)(config)# clock summer-time <timezone> recurring` ■ `<start-week> <start-day> <start-month>`

Table 18: *System Parameters*

Parameter	Description	CLI Configuration
		■ `<start-hour> <end-week> <end-day> <end-month> <end-hour>`
Preferred Band	The preferred band for the Instant AP. **NOTE:** Reboot the Instant AP after modifying the radio profile for changes to take effect.	■ `(Instant AP)(config)# rf-band <band>`
AppRF Visibility	Select one of the following options from the **AppRF visibility** drop-down list. ■ **App**—Displays only inbuilt DPI data. ■ **WebCC**—Displays the DPI data hosted on the cloud. ■ **All**—Displays both App and WebCC DPI data. ■ **None**—Does not display any AppRF content.	■ `(Instant AP)(config)# dpi`
URL Visibility	Select **Enabled** or **Disabled** from the **URL visibility** drop-down list.	■ `(Instant AP)(config)# url-visibility`
Cluster security	Select **Enabled** to ensure that the control plane messages between access points are secured. This option is disabled by default. **NOTE:** The Cluster security setting can be enabled only if the default NTP server or a static NTP server is reachable.	■ `(Instant AP)(config)# cluster-security`
Low assurance PKI	Select **Allow** or **Deny** from the drop-down list. You can enable the this parameter only if DTLS is allowed.	■ `(Instant AP)(config)# cluster-security` ■ `(Instant AP)(cluster-security)# allow-low-assurance-devices`

Table 18: *System Parameters*

Parameter	Description	CLI Configuration
Non-DTLS Slaves	When DTLS is supported on low assurance Instant APs, users have an option to prevent non-TPM Instant APs from establishing a DTLS connection with regular Instant APs. A new alert is displayed on the WebUI to warn the users when a DTLS connection with a non-TPM Instant AP is denied. The alert also displays the IP address of the Instant AP. For more security, specific Instant APs are allowed to form a cluster.	■ `(Instant AP)(config)# cluster-security` ■ `(Instant AP)(cluster-security)# dtls`
Virtual Controller network settings	If the virtual controller IP address is in a different subnet than that of the Instant AP, ensure that you select **Custom** from the **Virtual Controller network settings** drop-down list and configure the following details: ■ **Virtual Controller Netmask**—Enter subnet mask details. ■ **Virtual Controller Gateway**—Enter a gateway address. ■ **Virtual Controller DNS**—If the DNS IP address is configured for a master Instant AP, the DNS IP settings are synchronized for all APs in anInstant AP cluster. • If the DNS IP address is configured for anInstant AP as part of the per Instant AP setting (**Edit Access Point > General**), it takes precedence over the virtual controller DNS IP address defined in the **System > General** window. • If the Instant APs are not explicitly assigned a DNS IP address, the DNS IP	■ `(Instant AP)(config)# virtual-controller-dnsip <addr>` ■ `(Instant AP)(config)# virtual-controller-vlan <vcvlan> <vcmask> <vcgw>`

Table 18: *System Parameters*

Parameter	Description	CLI Configuration
	address defined in **System > General** takes precedence. • If the DNS IP address is not defined for Instant APs or virtual controller, the DNS address dynamically assigned from the DHCP server is used. ■ **Virtual Controller VLAN**—Ensure that the VLAN defined for the virtual controller is not the same as the native VLAN of the Instant AP.	
Auto join mode	The Auto-Join feature allows Instant APs to automatically discover the virtual controller and join the network. The Auto-Join feature is enabled by default. If the Auto-Join feature is disabled, a link is displayed in the **Access Points** tab indicating that there are new Instant APs discovered in the network. Click this link if you want to add these Instant APs to the network. When Auto-Join feature is disabled, the inactive Instant APs are displayed in red.	To disable auto-join mode: ■ `(Instant AP)(config)# no allow-new-aps` To enable auto-join mode: ■ `(Instant AP)(config)# allow-new-aps`
Terminal access	When terminal access is enabled, you can access the Instant AP CLI through SSH. The terminal access is enabled by default	■ `(Instant AP)(config)# terminal-access`
Console access	When enabled, you can access the Instant AP through the console port.	■ `(Instant AP)(config)# console`
Telnet server	To start a Telnet session with the Instant AP CLI, enable access to the Telnet server.	■ `(Instant AP)(config)# telnet-server`

Table 18: *System Parameters*

Parameter	Description	CLI Configuration
LED display	LED display status of the Instant AP. To enable or disable LED display for all Instant APs in a cluster, select **Enabled** or **Disabled**, respectively. **NOTE:** The LEDs are always enabled during the Instant AP reboot.	■ `(Instant AP)(config)# led-off`
Extended SSID	**Extended SSID** is enabled by default in the factory default settings of Instant APs. This disables mesh in the factory default settings. Instant APs support up to 14 SSIDs when Extended SSID is disabled and up to 16 SSIDs with Extended SSID enabled. If more than 16 SSIDs are assigned to a zone, you will receive an error message when you disable extended zone.	■ `(Instant AP)(config)# extended-ssid`
Deny inter user bridging	If you have security and traffic management policies defined in upstream devices, you can disable bridging traffic between two clients connected to the same Instant AP on the same VLAN. When inter user bridging is denied, the clients can connect to the Internet but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision. This global parameter overwrites all the options available in an SSID profile. For example, when this parameter is enabled, all the SSIDs deny client-to-client bridging traffic. By default, the **Deny inter user bridging** parameter is disabled.	■ `(Instant AP)(config)# deny-inter-user-bridging` To disable inter-user bridging for the WLAN SSID clients: ■ `(Instant AP)(config)# wlan ssid-profile <ssid-profile>` ■ `(Instant AP)(SSID Profile <ssid-profile>)# deny-inter-user-bridging`

Table 18: *System Parameters*

Parameter	Description	CLI Configuration
Deny local routing	If you have security and traffic management policies defined in upstream devices, you can disable routing traffic between two clients connected to the same Instant AP on different VLANs. When local routing is disabled, the clients can connect to the Internet but cannot communicate with each other, and the routing traffic between the clients is sent to the upstream device to make the forwarding decision. This global parameter overwrites all the options in an SSID profile. For example, when this parameter is enabled, all the SSIDs deny client-to-client local traffic. By default, the **Deny local routing** parameter is disabled.	■ `(Instant AP)(config)# deny-local-routing`
Dynamic CPU Utilization	Instant APs perform various functions such as wired and wireless client connectivity and traffic flows, wireless security, network management, and location tracking. If anInstant AP is overloaded, it prioritizes the platform resources across different functions. Typically, the Instant APs manage resources automatically in real time. However, under special circumstances, if dynamic resource management needs to be enforced or disabled altogether, the dynamic CPU management feature settings can be modified. To configure dynamic CPU management, select any of the following options from **DYNAMIC CPU UTILIZATION**. ■ **Automatic**—When selected, the CPU management is enabled or disabled automatically during runtime. This decision is based on real-time load calculations taking into account all different functions that the CPU needs to perform. This is	■ `(Instant AP)(config)# dynamic-cpu-mgmt`

Table 18: *System Parameters*

Parameter	Description	CLI Configuration
	the default and recommended option. ■ **Always Disabled in all APs**—When selected, this setting disables CPU management on all Instant APs, typically for small networks. This setting protects user experience. ■ **Always Enabled in all APs**—When selected, the client and network management functions are protected. This setting helps in large networks with high client density.	

Configuring System Parameters (New WebUI)

This section describes how to configure the system parameters of an Instant AP using the new WebUI.

Navigate to **Configuration** > **System** > **General**.

Table 19: *System Parameters*

Parameter	Description	CLI Configuration
Name	Name of the Instant AP.	■ `(Instant AP)# name <name>`
System location	Physical location of the Instant AP.	■ `(Instant AP)#(config)# syslocation <location-name>`
Virtual Controller IP	This parameter allows you to specify a single static IP address that can be used to manage a multi-Instant APInstant network. This IP address is automatically provisioned on a shadow interface on the Instant AP that takes the role of a virtual controller. When anInstant AP becomes a virtual controller, it sends three ARP messages with the static IP address and its MAC address to update the network ARP cache.	■ `(Instant AP)(config)# virtual-controller-ip <IP-address>`
Allow IPv6 Management	Click the toggle switch to enable IPv6 configuration	
Virtual Controller IPv6	This parameter is used to configure the IPv6 address.	■ `(Instant AP)(config)# virtual-controller-ipv6 <ipv6 address>`

Table 19: *System Parameters*

Parameter	Description	CLI Configuration
Dynamic RADIUS Proxy	When dynamic RADIUS proxy is enabled, the virtual controller network will use the IP address of the virtual controller for communication with external RADIUS servers. Ensure that you set the virtual controller IP address as a NAS client in the RADIUS server if Dynamic RADIUS proxy is enabled.	■ `(Instant AP)(config)# dynamic-radius-proxy`
Dynamic TACACS Proxy	When enabled, the virtual controller network will use the IP address of the virtual controller for communication with external TACACS servers. The IP address is chosen based on one of the following rules: ■ If a VPN tunnel exists between the Instant AP and the TACACS server, then the IP address of the tunnel interface will be used. ■ If a virtual controller IP address is configured, the the same will be used by the virtual controller network to communicate with the external TACACS server. ■ If a virtual controller IP is not configured, then the IP address of the bridge interface is used. **NOTE:** When dynamic-tacacs-proxy is enabled on the Instant AP, the TACACS server cannot identify the slave Instant AP that generates the TACACS traffic as the source IP address is changed.	■ `(Instant AP)(config)# dynamic-tacacs-proxy`
MAS Integration	Click the toggle switch to enable or disable the LLDP protocol for Mobility Access Switch integration. With this protocol, Instant APs can instruct the Mobility Access Switch to turn off ports where rogue access points are connected, as well as take actions such as increasing PoE priority and automatically configuring VLANs on ports where Instant access points are connected.	■ `(Instant AP)(config)# mas-integration`
NTP Server	This parameter allows you to configure NTP servers for the Instant AP. Up to four NTP servers can be configured for the AP, each one separated by a comma.	To configure NTP servers: ■ `(Instant AP)(config)# ntp-server <name>,<name2>,<name3>,<name4>` To remove NTP servers:

Table 19: *System Parameters*

Parameter	Description	CLI Configuration
	To facilitate communication between various elements in a network, time synchronization between the elements and across the network is critical. Time synchronization allows you to: ■ Trace and track security gaps, monitor network usage, and troubleshoot network issues. ■ Validate certificates. ■ Map an event on one network element to a corresponding event on another. ■ Maintain accurate time for billing services and similar tasks. NTP helps obtain the precise time from a server and regulate the local time in each network element. Connectivity to a valid NTP server is required to synchronize the Instant AP clock to set the correct time. If NTP server is not configured in the Instant AP network, an Instant AP reboot may lead to variation in time data. By default, the Instant AP tries to connect to **pool.ntp.org** to synchronize time. The NTP server can also be provisioned through the DHCP option 42. If the NTP server is configured, it takes precedence over the DHCP option 42 provisioned value. The NTP server provisioned through the DHCP option 42 is used if no server is configured. The default server **pool.ntp.org** is used if no NTP server is configured or provisioned through DHCP option 42. **NOTE:** To facilitate ZTP using the AMP, Central, or Activate, you must configure the firewall and wired infrastructure to either allow the NTP traffic to pool.ntp.org, or provide alternative NTP servers under DHCP options.	■ `(Instant AP)(config)# no ntp-server` To view NTP status: ■ `(Instant AP)# show ntp status` ■ `(Instant AP)# show running-config | include ntp` To view NTP debug logs: ■ `(Instant AP)# show ntp debug`
Timezone	Timezone in which the Instant AP must operate. You can also enable DST on Instant APs if the time zone you selected supports the DST. When enabled, the DST ensures that the Instant APs reflect the seasonal time changes in the region they serve.	To configure timezone: ■ `(Instant AP)(config)# clock timezone <name> <hour-offset> <minute-offset>` To configure DST: ■ `(Instant AP)(config)# clock summer-time <timezone> recurring` ■ `<start-week> <start-day>`

Table 19: *System Parameters*

Parameter	Description	CLI Configuration
		<start-month> ■ <start-hour> <end-week> <end-day> <end-month> <end-hour>
Preferred Band	The preferred band for the Instant AP. **NOTE:** Reboot the Instant AP after modifying the radio profile for changes to take effect.	■ (Instant AP)(config)# rf-band <band>
AppRF Visibility	Select one of the following options from the **AppRF visibility** drop-down list. ■ **App**—Displays only inbuilt DPI data. ■ **WebCC**—Displays the DPI data hosted on the cloud. ■ **All**—Displays both App and WebCC DPI data. ■ **None**—Does not display any AppRF content.	■ (Instant AP)(config)# dpi
URL Visibility	Click the toggle switch to enable URL visibility.	■ (Instant AP)(config)# url-visibility
Cluster security	Select **Enabled** to ensure that the control plane messages between access points are secured. This option is disabled by default. **NOTE:** The Cluster security setting can be enabled only if the default NTP server or a static NTP server is reachable.	■ (Instant AP)(config)# cluster-security

Changing Password

The following procedure describes how to update your password details by using the WebUI.

Table 20: *Steps to Update Password*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **System** > **Admin**. 2. Under **Local**, provide a new password that you would like the admin users to use. 3. Click **Save**.	1. Navigate to **System** > **Admin**. 2. Under **Local**, provide a new password that you would like the admin users to use. 3. Click **OK**.

The following CLI snippet allows you to change the admin username and password:

```
(Instant AP)(config)# mgmt-user <username> [password]
```

Hashing of Management User Password

Starting from Instant 6.5.0.0-4.3.0.0, all the management user passwords can be stored and displayed as hash instead of plain text. Hashed passwords are more secure as they cannot be converted back to plain text format.

Upgrading to the Instant 6.5.0.0-4.3.0.0 version will not automatically enable hashing of management user passwords, as this setting is optional. Users can choose if management passwords need to be stored and displayed as hash, or if the passwords need to remain in encrypted format.

This setting is enabled by default on factory reset Instant APs running Instant 6.5.0.0-4.3.0.0 onwards, and is applicable to all Instant APs in the cluster.

The following procedure describes how to enable hashing of the management user password by using the WebUI.

Table 21: *Hashing of Management Username and Password*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **System** > **Admin**. 2. Click the **show advanced options** link. 3. Select the **Hash Management Password** check box. This will enable the hashing of the management user password.	1. Navigate to **System** > **Admin**. 2. Click the **show advanced options** link. 3. Select the **Hash Management Password** check box. This will enable the hashing of the management user password.



The check box will appear grayed out after this setting is enabled, as this setting cannot be reversed.

Run the following command to enable hashing of a management user password:

```
(Instant AP)(config)# hash-mgmt-password
```

Run the following command to add a management user with read-only privilege:

```
(Instant AP)(config)# hash-mgmt-user john password cleartext password01 usertype read-only
```

Run the following command to remove a management user with read-only privilege:

```
(Instant AP)(config)# no hash-mgmt-user read-only
```

Chapter 8
Customizing Instant AP Settings

This chapter describes the procedures for configuring settings that are specific to an Instant AP in the cluster.

- Discovery Logic on page 78
- Modifying the Instant AP Host Name on page 84
- Configuring Zone Settings on an Instant AP on page 84
- Specifying a Method for Obtaining IP Address on page 92
- Configuring External Antenna on page 93
- Configuring Radio Profiles for an Instant AP on page 94
- Air Slice on page 100
- Enabling Flexible Radio on page 96
- Configuring Uplink VLAN for an Instant AP on page 103
- Changing the Instant AP Installation Mode on page 103
- Changing USB Port Status on page 104
- Master Election and Virtual Controller on page 105
- Adding an Instant AP to the Network on page 107
- Removing an Instant AP from the Network on page 107
- Support for BLE Asset Tracking on page 107
- Intelligent Power and Temperature Monitoring on page 119
- Transmit Power Calculation Support on 200 Series and 300 Series Access Points on page 122
- Hardware Offloading for Increased Transmission Performance on page 122

Discovery Logic

In the previous Instant releases, access points were predefined as either controller-based Campus APs or controller-less Instant APs. Each legacy Instant AP was shipped with an Instant image that enabled the Instant AP to act as its own virtual controller or to join an existing Instant cluster.

Starting with Instant 6.5.2.0, the new access points introduced in this release or following releases can run on both controller-based mode and controller-less mode. Based on the selected mode, the AP runs a corresponding image:

- Controller mode will run ArubaOS image.
- Controller-less mode will run Instant image.

Each access point is shipped with either a limited functionality manufacturing image or an Instant image. An access point with either of the limited functionality manufacturing image or the Instant image will run the full discovery logic. Based on that, it will download the ArubaOS or Instant image and convert to the corresponding mode.

Starting from Instant 6.5.4.5, the Cloud First principle is applied to the AP discovery feature. In this principle, the AP, regardless of whether it is factory reset or configured, retrieves provisioning rules from Activate after it boots up.



The Instant AP acts as a DHCP server for wired clients if both the Ethernet ports of the Instant AP are connected to the uplink switch. This occurs when LACP is not configured on the uplink switch. Therefore it is recommended to not connect both the Ethernet ports of the Instant AP to the uplink switch if LACP is not configured.

Preference Role

Users can predefine the AP mode by configuring the preference role using the WebUI or the CLI.

In the ArubaOS WebUI

To set the AP preference role to controller-less in the WebUI:

1. Navigate to **Maintenance** > **Access Point** > **Convert to instant mode** in the WebUI.
2. Select the AP(s) on which you want to set the preference role to controller-less.
3. Click **Convert to instant mode**.

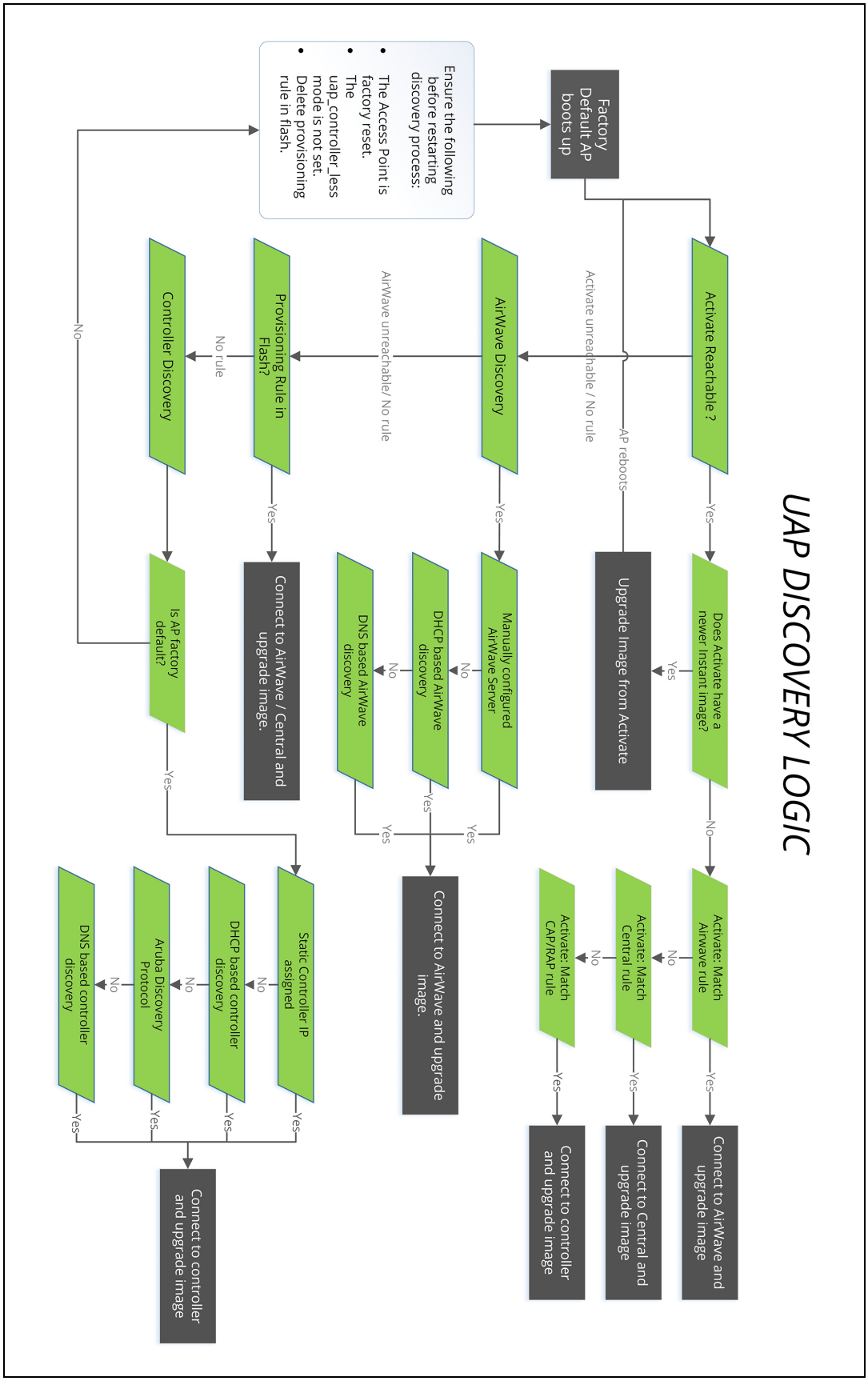
In the CLI

To set the AP preference role to controller-less in the CLI, execute the following commands:

```
(host) #ap redeploy controller-less
all
ap-group
ap-name
ip-addr
ip6-addr
wired-mac
```

Discovery Logic Workflow

Figure 3 *AP Discovery Logic*



The following steps describe the AP discovery logic:

1. When an AP boots up, it connects to Activate to obtain a provisioning rule.
2. If provisioning is already done by AirWave or Central, verify if a provisioning rule exists. If yes, the provisioning rule is saved in the flash memory. Compare the saved provisioning rule with the rule in Activate. If the rule in Activate is new, save the new provisioning rule in flash. For example, if the master and slave Instant APs obtain different AirWave addresses or if the master and slave Instant APs obtain a different AirWave or Central rule, the master Instant AP rule takes higher precedence.



Only the master Instant AP can apply provisioning rules to the Instant AP cluster.

3. If the rule is to perform a mandatory upgrade of the Instant AP, ensure to upgrade the Instant AP to the desired version. The master Instant AP executes the upgrade after a cluster is formed.
4. If the rule is to convert the Instant AP to Campus AP or Remote AP, the conversion takes effect for every Instant AP regardless of whether it is a master or a slave. This requires a manual registration of every master and slave Instant AP with Activate.
5. If there is no rule from Activate or if conversion to Campus AP or Remote AP fails, the master AP conducts local provisioning detection to check the local AirWave configuration.
   - If the AirWave server is configured and is in the configuration file, apply the server details. Otherwise, conduct a DHCP based AirWave or Central detection.
   - If DHCP-based AirWave is not found and the Instant AP is in factory default status, perform a DNS based AirWave discovery.
   - If none of the above methods can detect the AirWave server and if the Instant AP cannot connect to Activate, use the provisioning rule in flash.
6. If the AirWave or Central server is not found, or if the Instant AP is a slave, verify if the following conditions for local controller discovery are met:
   - The Instant AP is factory reset.
   - The **uap_controller_less** mode is not set.
   - There is no provision rule saved in flash.
7. If the controller is found, the Instant AP sends a hello message to the controller and converts to a Campus AP.
8. When a master failover happens, the new masterInstant AP connects to Activate to retrieve the provisioning rule. If the new master successfully obtains the provisioning rule, it applies this rule to the cluster.

Manual Upgrade

APs running in unprovisioned mode broadcast a special provisioning SSID to which users can connect to upgrade the AP manually. Upon connecting, users can access a local provisioning page in the WebUI to upgrade the AP to an ArubaOS or Instant image. For more information on upgrading APs manually, refer to the following scenarios:

- Controller-based AP over Manual Campus AP or Remote AP Conversion in the *ArubaOS User Guide*.
- Controller-less AP over Manual Instant AP Conversion in the *ArubaOS User Guide*.



The provisioning SSID for all APs running Instant 6.5.2.0 onwards, including legacy Instant APs is **SetMeUp-xx:xx:xx**.

Deployment Scenarios

This section describes the controller-less AP deployment and hybrid deployment scenarios:

Controller-less AP Deployments

The following sections describe controller-less AP deployment scenarios.

Controller-less AP in an Instant Network

Users can deploy APs directly into a running Instant network, which consists of an Instant AP cluster and a virtual controller that manages the network. In this scenario, there is an actively running Instant network with a master Instant AP.

The AP is able to successfully discover the Instant Virtual Controller and join the cluster. The manufacturing image image in the AP is upgraded to the Instant image of the virtual controller and the configuration is synchronized from the Virtual Controller to the newly added Instant AP.

For more information on electing a master in an Instant network, see Master Election and Virtual Controller on page 105.

Controller-less AP over Activate, AirWave, or Central

In this scenario, there is no cluster deployed in the subnet but AirWave, Activate, and Central can be reached over the network.



In this deployment scenario, Activate,AirWave, or Central must be accessible to the AP.

APs are upgraded to the Instant image through AirWave, Activate, and Central in the following steps:

1. The AP boots up with the limited functionality manufacturing image or the Instant image and attempts to locate Activate.
2. If the AP locates Activate, it receives pre-configured provisioning rules to connect to AirWave or Central or convert into a Campus AP or Remote AP. If Activate is unreachable, the AP attemps to locate a virtual controller, AirWave, or Central.

   APs that connect to Activate are automatically upgraded from the manufacturing image to the latest Instant or Instant image. Refer to the latest *Aruba Activate User Guide* for more details on configuring provisioning rules.

3. If the AP locates AirWave, it can be upgraded to the Instant image. If an enforced image upgrade rule is configured in AirWave, the AP is upgraded to the Instant image that is configured for the enforced upgrade rule. If no enforced upgrade rule is configured, the AP is upgraded to the latest Instant image in AirWave. After the AP is upgraded, it reboots in controller-less mode. Refer to the latest *AirWave User Guide* for details on AP image upgrade.



All firmware must be uploaded to AirWave before the AP connects and downloads the Instant image. Refer to the latest *AirWave Deployment Guide* for details on firmware upload.

4. If the AP locates Central, it can be upgraded to the Instant image through the **Maintenance > Firmware** page in the Central WebUI. After the AP is upgraded, it reboots in controller-less mode. Refer to the latest *Central User Guide* for more details on AP image upgrade.

   Central synchronizes with Aruba Activate to retrieve the latest Instant image.

5. After the AP is upgraded to controller-less mode, it forms a new Instant AP cluster and converts into the master. Other APs which are not deployed can join the cluster and upgrade to the Instant image.

Controller-less AP over Manual Instant AP Conversion.

If the AP cannot be upgraded into an Instant AP through a virtual controller, Activate, AirWave, or Central, users can connect to a special provisioning SSID broadcasted by the unprovisioned AP to manually convert the AP to an Instant AP through the WebUI. Refer to the *Controller-less AP in an Instant Network* section and the *Controller-less AP over Activate, AirWave, or Central* section in the *ArubaOS User Guide* for details on upgrading an AP to the Instant image using a virtual controller, Activate, AirWave, or Central.

To manually convert an AP to an Instant AP in the WebUI:

1. Log in to your virtual controller.
2. Connect to the following provisioning SSID broadcasted by the unprovisioned AP: **SetMeUp-xx:xx:xx**.
3. Open a web browser and then navigate to the following URL:

   https://setmeup.arubanetworks.com
4. Under **Access Point Setup**, select **Image File** or **Image URL** to upload the Instant image.

- If you selected **Image File**, click **Browse** to locate and select an Instant image file from your local file explorer.
- If you selected **Image URL**, enter the web address of the Instant image under **URL**.

5. Click **Save**.

After the AP is upgraded, it reboots in the controller-less mode.

Behavior of Default Provisioning SSID

Starting with Instant 8.5.0.0, The AP will stop broadcast of default SetMeUp SSID when it discovers the controller IP through Activate, DHCP server or DNS server.

The AP in its factory default state scans for the controller IP every 1 second. During the scan if the AP discovers the controller IP, it disables the default SetMeUp SSID. The SetMeUp SSID is disabled as the AP attempts to connect to the controller and remains disabled even if it is unable to connect to the controller. The default SetMeUp SSID will be disabled if the Instant AP receives any of the following:

- DHCP option 43/60
- DHCPv6 option 52
- DHCP option 43/60 (IPv4) and DHCP 52 (IPv6) for dual stack environment
- Activate provisioning rule to convert IAP-to-CAP (IPv4)

To re-enable the default SetMeUp SSID, remove the controller IP from Activate, DHCP server and DNS server. When the AP scans for the controller IP again, it does not discover the IP and the default SetMeUp SSID starts broadcasting.

AP Deployments in Hybrid Controller-Instant Networks

Users can deploy APs into hybrid networks, which contain both controller-based and controller-less APs. APs in hybrid networks are upgraded to the ArubaOS or Instant image using the same methods as APs in pure controller or Instant networks. However, the following items must be in place before deploying APs in a hybrid network:

- Controller-based APs and controller-less APs must run on different subnets (for example, a controller-based AP subnet and a separate controller-less AP subnet).
- Different discovery methods should be used for controller-based APs and controller-less APs, as the controller discovery process and Instant AirWave discovery process share the same DHCP or DNS discovery methods. For example, controller-based APs can use a DHCP server to discover a controller, while controller-less APs can use a DNS server on AirWave.
- If the same discovery method must be used for both controller-based APs and controller-less APs, it is recommended that you use DHCP-based discovery. DHCP servers can respond to DHCP requests based on the AP's subnet and vendor ID. DNS servers do not have a subnet limit and this can cause the APs that share a DNS server to be upgraded on the wrong AP subnet.

Modifying the Instant AP Host Name

You can change the host name of an Instant AP through the WebUI or the CLI.

Table 22: *Steps to change the host name of an Instant AP*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Access Points**. 2. Select the Instant AP to rename and click **Edit**. 3. Expand **General** and enter the new name in the **Name** field. You can specify a name of up to 128 ASCII characters. 4. Click **Save**.	1. In the **Access Points** tab, select the Instant AP you want to rename. 2. Click the **edit** link. 3. Under **General** tab, enter a new name in **Name** field. You can specify a name of up to 128 ASCII characters. 4. Click **OK**.

Run the following command to change the host name of an Instant AP:

```
(Instant AP)# hostname <system_name>
```



As a best practice, It is recommended to configure the hostname by using only **a**-**z**, **A**-**Z**, **0**-**9**, '.', '-', ':', '_' , but not special characters such as "**#$%**".

Configuring Zone Settings on an Instant AP

Starting from Instant 8.3.0.0, Instant APs can be assigned RF zones and SSID zones to enhance the wireless network environment. RF zones enable the creation of custom RF environments for Instant APs and SSID zones enable the creation of Wi-Fi zones to service multiple sets of clients in different zones of the wireless environment. RF zones and SSID zones are independent of each other and are configured separately.

RF zones

RF zones enable the creation of RF environments for individual APs. RF zones are configured using radio profiles. Radio profiles allow the creation of additional radio profiles which can be associated to one or more APs using their zone name. Each radio profile has a zone parameter which can be configured except for the default radio profile and each AP can be assigned a single RF zone. Instant supports up to 10 radio profiles each for both 2.4 GHz radio and 5 GHz radio in an Instant cluster. A single RF zone can

be configured on multiple APs and all APs should be configured to a RF zone. If no RF zone is assigned to an AP, the default radio profile will be used.



Two radio profiles can have the same zone name given that the profiles are in different bands, i.e, A 2.4 GHz radio profile and a 5 GHz radio profile can have the same zone name. Using the same zone name for a 2.4 GHz profile and a 5 GHz profile brings the two radio profiles under one RF zone, which can then be applied to the AP using the zone name. This enables you to apply radio profiles to both the radios of the AP. However, two radio profiles in the same band cannot have the same zone name.

Configuring RF Zones for Instant AP

RF zones are created by configuring radio profiles with a zone name and then attaching them to the Instant AP using the same zone name. Only one RF zone can be applied to an AP and if no specific zone is assigned to an AP then the default radio profile will be used. The radio profile assigned to the AP will use the following priority: assigned RF zone > default radio profile > ARM profile.

The following procedure configures an RF zone using the WebUI:

Table 23: *Steps to Configure an RF Zone*

New WebUI	Old WebUI
1. Configure a radio profile and specify a name for the zone in the **zone** field. For configuring radio profile, see Configuring Radio Settings. To configure an RF zone with profiles for both 2.4 GHz and 5 GHz radio use the same zone name in the two radio profiles. 2. Attach the configured radio profile to the Instant AP using the zone name. Use the following procedure to configure an RF zone to an Instant AP: 3. Navigate to the **Configuration** > **Access Points** page. 4. Select the Instant AP from the **Access Points** list and click **Edit**. 5. Expand **General** and specify the Instant AP zone in the **RF zone** field. 6. Click **Save**.	1. Configure a radio profile and specify a name for the zone in the **zone** field. For configuring radio profile, see Configuring Radio Settings. To configure an RF zone with profiles for both 2.4 GHz and 5 GHz radio use the same zone name in the two radio profiles. 2. Attach the configured radio profile to the Instant AP using the zone name. Use the following procedure to configure an RF zone to an Instant AP: 3. Navigate to the **Access Points** tab. Select the Instant AP to configure, and then click **edit**. 4. In the **Edit Access Point** > **General** tab, specify the Instant AP zone name in the **RF Zone** field. 5. Click Save.

Run the following commands to configure an RF zone:

1. Configure radio settings using **rf dot11a-radio-profile** and **rf dot11g-radio-profile** commands for 5 GHz and 2.4 GHz radio respectively and specify a name for the zone using the **zone <zone name>** parameter. To configure an RF zone with profiles for both 2.4 GHz and 5 GHz radio use the same zone name in the two radio profiles. The following is the syntax to configure zone name for 2.4 GHz and 5 GHz radio profile.

To configure zone name in a 2.4 GHz radio profile:

```
InstantAP (config) # rf dot11g-radio-profile <profile name>
InstantAP (RF dot11g Radio Profile "<profile name>") # zone <zone name>
```

To configure zone name in a 5 GHz radio profile:

```
InstantAP (config) # rf dot11a-radio-profile <profile name>
InstantAP (RF dot11a Radio Profile "<profile name>") # zone <zone name>
```

2. Attach the specific RF zone and the associated radio profile to the AP using the **rf-zone <zone name>** command. This is a per-ap setting and should configured on the respective AP. The following is the syntax to attach a radio profile to the AP:

```
rf-zone <zone name>
```

To view the radio profile used by the AP, use the **show radio profile** command. The active profile is listed in the **Zone** column.

SSID Zones

SSID zones enables the creation of Wi-Fi zones with different SSIDs to service different sets of clients. SSID zones are created using WLAN SSID profile. Traditionally only one zone can be configured to an Instant AP but starting from Instant 8.3.0.0, Instant APs can be assigned multiple SSID zones to serve different set of clients in different zones of the Wi-Fi environment. In the previous releases, commas were a part of the zone name. Commas configured in ArubaInstant 6.5.4.x or prior versions will be used as delimiters when Instant APs are upgraded to ArubaInstant 8.3.0.x or later.



You can configure up to six SSID zones per AP, and up to 32 SSID zones per ssid-profile. However, it is strongly recommended not to configure multiple zones in per-AP and per-SSID profiles at the same time.

Configuring SSID zones for Instant AP

SSID zones are created by configuring WLAN SSID profiles with a zone and attaching them to the AP using the zone name. A maximum of 6 SSID zones can be assigned to an AP and if no specific zone is assigned, the AP will broadcast only the SSIDs configured on the AP or the Instant cluster. SSID zones can be configured using the WebUI, CLI, AirWave or Central.

The following procedure configures an SSID zone using the WebUI:

Table 24: *Steps to Configure an SSID Zone*

New WebUI	Old WebUI
1. Configure a WLAN SSID profile and specify a name for the zone in the **zone** field. For configuring WLAN SSID profiles, see Configuring WLAN Settings for an SSID Profile. 2. Attach the configured WLAN SSID profile to the Instant AP using the zone name. Use the following procedure to configure an SSID zone to an Instant AP: a. Navigate to the **Configuration** > **Access Points** page. b. Select the Instant AP from the **Access Points** list and click **Edit**.	1. Configure a WLAN SSID profile and specify a name for the zone in the **zone** field. For configuring WLAN SSID profiles, see Configuring WLAN Settings for an SSID Profile. 2. Attach the configured WLAN SSID profile to the Instant AP using the zone name. Use the following procedure to configure an SSID zone to an Instant AP: a. Navigate to the **Access Points** tab. Select the Instant AP to configure, and then click **edit**. b. In the **Edit Access Point** > **General** tab, specify the Instant AP zone in the **Zone** field.

New WebUI	Old WebUI
c. Expand **General** and specify the Instant AP zone in the **Zone** field. 3. Click **Save**.	3. Click **OK**.

Run the following command to configure an SSID Zone:

1. Configure WLAN settings for the SSID settings using **wlan ssid-profile** command and specify a name for the zone using the **zone <zone name>** parameter. The following is the syntax to configure zone name for a wlan ssid profile.

To configure zone name in a wlan ssid profile:

```
InstantAP (config) # wlan ssid-profile <profile name>
InstantAP (SSID Profile "<profile name>") # zone <zone name>
```

2. Attach the specific SSID zone and the associated SSID profile to the AP using the **zonename <zone name>** command. A maximum of 6 SSID zones can be assigned to an AP and the different zones are separated using commas. This is a per-ap setting and should configured on the respective AP. The following is the syntax to attach an SSID zone to the AP:

```
zonename <zone1 name, zone2 name>
```

Disabling AP Factory Reset

An AP can be reset to factory default configuration by pressing its reset button for more than 5 seconds while the AP is operational. Aruba Instant allows you to disable AP factory reset while the AP is operational.



The AP factory reset is enabled by default; which means, an AP may be reset to factory default configuration by pressing its reset button for more than 5 seconds while the AP is operational.

The following CLI command disables the AP factory reset feature while the AP is operational:

```
(Instant AP)(Config)# disable-factory-reset
```

The following CLI command enables the AP factory reset feature while the AP is operational:

```
(Instant AP)(Config)# no disable-factory-reset
```

AP USB Management

Aruba Instant supports new infrastructure to manage any USB device that is plugged to an AP. The infrastructure allows describing a USB device through either CLI configuration or by using predefined descriptors. The infrastructure allows USB device management through USB ACLs. The infrastructure also supports plugin for USB devices. A plugin can perform further identification or perform normal logical interaction with the USB device. The infrastructure supports sending notification to other processes. For example: USB device plug-in or unplug notifications are sent to the IoT daemon. The infrastructure also supports sending script-based notifications. The USB ACLs are applied to the USB Management Daemon (UDMD) process and when a USB device is plugged in to an AP, the

USB device walks through all USB ACL rules sequentially. Instant supports USB devices only from Aruba approved vendors. The following vendors are approved:

- Alcatel-L800
- Amberbox-detector
- Amberbox-gateway
- C-motech-CNU-680
- EpiValley-SEC-8089
- Fraklin-u770-u772
- Franklin-U300
- Franklin-U301
- Franklin-U600
- Fujisoft
- Globetrotter-ICON-225
- Globetrotter-ICON-322
- HanShow
- Huawei-3276s-150
- Huawei-D41HW
- Huawei-E1552
- Huawei-E157
- Huawei-E160
- Huawei-E169-E180-E220
- Huawei-E170-E272-E220
- Huawei-E173
- Huawei-E1731-177DT06
- Huawei-E1750
- Huawei-E176-E176G-E1553
- Huawei-E1762
- Huawei-E180
- Huawei-E180-E1692-E1762
- Huawei-E1820e
- Huawei-E220
- Huawei-E261
- Huawei-E3131
- Huawei-E3272s-153
- Huawei-E3276
- Huawei-E3276s-500
- Huawei-E3372
- Huawei-E3372h-153-hilink
- Huawei-E3372h-153-modem
- Huawei-E352s-5
- Huawei-E353
- Huawei-E353-E1750-E367
- Huawei-E367

- Huawei-E3765
- Huawei-E392
- Huawei-e398
- Huawei-E8372
- Huawei-EC150
- Huawei-EC167
- Huawei-HWD12-LTE
- Huawei-K3770
- Huawei-K3772
- Huawei-K4505
- Huawei-K4510
- Huawei-K4605
- Huawei-K5150
- Huawei-K5160
- Huawei-KDDI-DATA07
- Icon-452
- Longcheer-WM72
- Netgear-340u
- Netgear-341u
- Novatel-MC545
- Novatel-MC551L
- Novatel-MiFi-2200
- Novatel-Ovation-U727
- Novatel-U620L
- Novatel-U720
- Novatel-U727
- Novatel-U760-Sprint
- Novatel-U760-Virgin
- NTT-DoCoMo-L-02A
- NTT-DoCoMo-L-02C
- NTT-DoCoMo-L-05A
- NTT-DoCoMo-L-08C
- Pantech-UM150
- Pantech-UM175
- Pantech-UM190
- Pantech-UML290
- Pantech-UML295
- Pantech-UML295-cold
- Qualcomm-SXC-1080
- SES-Imagotag-021
- Sierra-250U
- Sierra-305-308
- Sierra-306-308-503-312U

- Sierra-313u
- Sierra-320U
- Sierra-330U
- Sierra-598
- Sierra-881U
- Sierra-885
- Sierra-Compass-597
- Sierra-Compass-885
- Sierra-Tstick-C597
- SIMTech
- Solu-M-SLG-DM101
- UGM1831
- UMG181
- Utstarcom-UM100C
- ZTE-3565
- ZTE-AC2726
- ZTE-AC2736
- ZTE-AC3781
- ZTE-Fivespot
- ZTE-K4505-z
- ZTE-MF110
- ZTE-MF180-HSDPA
- ZTE-MF190-Egypt
- ZTE-MF190-India
- ZTE-MF190-Thailand
- ZTE-MF591
- ZTE-MF633-MF636
- ZTE-MF637-MF656
- ZTE-MF668
- ZTE-MF683-HSDPA
- ZTE-MF79S
- ZTE-MF820
- ZTE-MF820D
- ZTE-MF823
- ZTE-MF825C
- ZTE-MF831
- ZTE-MF832S
- ZTE-MF832U
- ZTE-MF832U-Zero

USB ACL Profile

Aruba Instant supports definition of up to 16 USB ACL profiles. A USB ACL profile is a vendor-product name with one action (permit, deny, reset). You cannot configure vendor ID in the USB descriptor, but can configure the name and action. When a USB ACL is applied to an AP group, all APs in that AP group

inherit the USB ACL rules. When a USB device is described using a predefined descriptor, they are permitted by default.

When there is no USB ACL configuration but a USB profile is pushed, the UDMD process applies permit-all by default. If there is configured USB ACL, the SAPD or CLI process automatically adds deny-all rule at the end of the pushed rule list. That is, when UDMD does not find the matched USB ACL rule from the configuration, it applies the deny-all rule by default.

The following CLI command creates a USB ACL profile named sample-usb-acl-profile with **rule** to **permit** USB devices from **HanShow**:

```
(Instant AP)(config)# usb acl-profile sample-usb-acl-profile
(Instant AP)(AP USB ACL Profile "sample-usb-acl-profile") #rule HanShow permit
```

The following CLI command creates a USB ACL profile named sample-usb-acl-profile with **rule** to **deny** USB devices from **HanShow**:

```
(Instant AP)(config)# usb acl-profile sample-usb-acl-profile
(Instant AP)(AP USB ACL Profile "sample-usb-acl-profile") #rule HanShow deny
```

The following CLI command creates a USB ACL profile named sample-usb-acl-profile with **no rule** to **permit** USB devices from **HanShow**:

```
(Instant AP)(config)# usb acl-profile sample-usb-acl-profile
(Instant AP)(AP USB ACL Profile "sample-usb-acl-profile") #no rule HanShow permit
```

The following CLI command creates a USB ACL profile named sample-usb-acl-profile with **no rule** to **deny** USB devices from **HanShow**:

```
(Instant AP)(config)# usb acl-profile sample-usb-acl-profile
(Instant AP)(AP USB ACL Profile "sample-usb-acl-profile") #no rule HanShow deny
```

The following CLI command creates an AP USB profile named sample-ap-usb-profile and applies a USB ACL profile named sample-usb-acl-profile to it:

```
(Instant AP)(config)# usb-profile sample-ap-usb-profile
(Instant AP)(AP USB profile "sample-ap-usb-profile") #usb-acl-profile sample-usb-acl-
profile
```

The following CLI command binds an AP USB profile named sample-usb-profile:

```
(Instant AP)(config)# usb-profile-binding sample-usb-profile
```

The following CLI command resets the USB device:

```
(Instant AP)# usb-device-mgmt reset device <device ID>
```

The following CLI command shows the USB profile:

```
(Instant AP)# show usb profile
```

The following CLI command shows the details of a specific USB profile based on its profile name:

```
(Instant AP)# show usb-profile sample-ap-usb-profile
```

The following command shows the USB ACL profile:

```
(Instant AP)# show usb acl-profile
```

The following CLI command shows the details of a specific USB ACL profile based on its profile name:

```
(Instant AP)# show usb-acl-prof sample-ap-usb-acl-profile
```

The following command shows the details of the devices connected to the Instant AP:

```
(Instant AP)# show usb devices
```

The following CLI command shows the list of supported vendor USB products:

```
(Instant AP)# show usb supported vendor-product
```

The following CLI command shows the USB cellular status:

```
(Instant AP)# show usb status
```

Specifying a Method for Obtaining IP Address

You can either specify a static IP address or allow the Instant AP to obtain an IP address from the DHCP server. By default, the Instant APs obtain IP address from the DHCP server. The following procedure configures a static IP address:

Table 25: *Steps to Update Password*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **Access Points** page. Select the Instant AP from the Access Points list and click **Edit**. 2. Under **General**, for the **IP address for Access Point** option, select **Specify statically** and enter values for the following: ▪ **IP address**: Enter a new IP address for the Instant AP. ▪ **Netmask:** Enter the subnet mask of the network. ▪ **Default gateway**: Enter the IP address of the default gateway. ▪ **DNS server**: Enter the IP address of the DNS server in the text box. You can configure up to two DNS servers separated by a comma. If the first DNS server goes down, the second DNS server will take control of resolving the domain name. ▪ **Domain name**: Enter the domain name. 3. Click **Save** and reboot the Instant AP.	1. In the **Access Points** tab, select the Instant AP to modify and click the **edit** link. 2. Under **General**, for the **IP address for Access Point** option, select **Specify statically** and enter values for the following: ▪ **IP address**: Enter a new IP address for the Instant AP. ▪ **Netmask:** Enter the subnet mask of the network. ▪ **Default gateway**: Enter the IP address of the default gateway. ▪ **DNS server**: Enter the IP address of the DNS server in the text box. You can configure up to two DNS servers separated by a comma. If the first DNS server goes down, the second DNS server will take control of resolving the domain name. ▪ **Domain name**: Enter the domain name. 3. Click **OK** and reboot the Instant AP.

Run the following command to configure a static IP address:

```
(Instant AP)# ip-address <IP-address> <subnet-mask> <NextHop-IP> <DNS-IP-address>
<domain-name>
```

When IAP-VPN is not configured or IPsec tunnel to the controller is down, DNS query from the client that is associated to the master Instant AP is taken by DNS proxy function on the master Instant AP. So, if the DNS server address for the the master Instant AP is set (by dnsip or from DHCP server), the DNS query will be sent to the DNS server by the master Instant AP. But if the DNS server address is not set, the DNS query will not be sent by the master Instant AP. However, the DNS query from the client that is associated to the slave Instant AP is not affected to this behavior.

Configuring External Antenna

If your Instant AP has external antenna connectors, you need to configure the transmit power of the system. The configuration must ensure that the system's EIRP is in compliance with the limit specified by the regulatory authority of the country in which the Instant AP is deployed. You can also measure or calculate additional attenuation between the device and the antenna before configuring the antenna gain. To know if your Instant AP device supports external antenna connectors, refer to the *Aruba Instant Installation Guide* that is shipped along with the Instant AP device.

EIRP and Antenna Gain

The following formula can be used to calculate the EIRP-limit-related RF power based on selected antennas (antenna gain) and feeder (Coaxial Cable loss):

EIRP = Tx RF Power (dBm) + GA (dB) - FL (dB)

The following table describes this formula:

Table 26: *Formula Variable Definitions*

Formula Element	Description
EIRP	Limit specific for each country of deployment.
Tx RF Power	RF power measured at RF connector of the unit.
GA	Antenna gain
FL	Feeder loss

Example

For example, the maximum gain that can be configured on an Instant AP with AP-ANT-1F dual-band and omni-directional antenna is as follows:

Table 27: *Maximum Antenna Gains*

Frequency Band	Gain (dBi)
2.4–2.5 GHz	2.0 dBi
4.9–5.875 GHz	5.0 dBi

For information on antenna gain recommended by the manufacturer, see www.arubanetworks.com.

Configuring Antenna Gain

You can configure antenna gain for Instant APs with external connectors by using the WebUI or the CLI.

Table 28: *Steps to Configure Antenna Gain Value*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **Access Points** page. Select the Instant AP and click **Edit**. 2. In the **Edit Access Point** window, select **External Antenna** to configure the antenna gain value. This option is available only for access points that support external antennas. 3. Enter the antenna gain values in dBm for the 2.4 GHz and 5 GHz bands. 4. Click **Save**.	1. From the **Access Points** tab, select the Instant AP to configure, and click **edit**. 2. In the **Edit Access Point** window, select **External Antenna** to configure the antenna gain value. This option is available only for access points that support external antennas. 3. Enter the antenna gain values in dBm for the 2.4 GHz and 5 GHz bands. 4. Click **OK**.

In the CLI

Run the following command to configure an external antenna for 5 GHz frequency:

```
(Instant AP)# a-external-antenna <dBi>
```

Run the following command to configure an external antenna for 2.4 GHz frequency:

```
(Instant AP)# g-external-antenna <dBi>
```

Configuring Radio Profiles for an Instant AP

You can configure a radio profile on an Instant AP either manually or by using the ARM feature.

ARM is enabled on Instant by default. It automatically assigns appropriate channel and power settings for the Instant APs. For more information on ARM, see Adaptive Radio Management on page 369.

Table 29: *Steps to Configure ARM-Assigned Radio Profiles*

New WebUI	Old WebUI
1. Navigate to the **Configuration > Access Points** page. Navigate to the **Configuration > Access Points** page. 2. Expand **Radio**. 3. In the **Mode** drop down list box of the desired band, select **Access**. 4. Select the **Adaptive radio management assigned** radio button. 5. Click **Save**.	1. In the **Access Points** tab, select the Instant AP to modify and click **edit**. 2. Select the **Radio** tab. 3. In the **Mode** drop down list box of the desired band, select **Access**. 4. Select the **Automatic channel and transmit power (ARM)** radio button. 5. Click **OK**.

The following procedure configures a radio profile manually:

Table 30: *Steps to Configure Radio Profiles Manually*

New WebUI	Old WebUI
1. Navigate to the **Configuration > Access Points**	In the **Access Points** tab, select the Instant AP to modify and click **edit**.

New WebUI	Old WebUI
page. 2. Expand **Radio**. 3. Select a desired radio mode for the respective bands from their **Mode** drop-down list box. The following table describes various configuration modes for an Instant AP: ■ **Access**—In **Access** mode, the Instant AP serves clients, while also monitoring for rogue Instant APs in the background. If the **Access** mode is selected, perform the following actions: 1. Select **Administrator assigned** in **2.4 GHz** and **5 GHz** band sections. 2. Select appropriate channel number from the **Channel** drop-down list for both **2.4 GHz** and **5 GHz** band sections. 3. Enter appropriate transmit power value in the **Transmit power** text box in **2.4 GHz** and **5 GHz** band sections. **NOTE:** If the transmit power is set to 0, the Instant AP is assigned the last transmitted power value set by the ARM. ■ **Monitor**—In **Monitor** mode, the Instant AP acts as a dedicated monitor, scanning all channels for rogue Instant APs and clients. You can set one radio on the Monitor mode and the other radio on the access mode, so that the clients can use one radio when the other one is in the Air Monitor mode. ■ **Spectrum Monitor**—In **Spectrum Monitor** mode, the Instant AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring Instant APs or from non-WiFi devices such as microwaves and cordless phones. **NOTE:** In this mode, Instant APs do not provide access services to clients. Click **Save**.	Select the **Radio** tab. Select a desired radio mode for the respective bands from their **Mode** drop-down list box. The following table describes various configuration modes for an Instant AP: ■ **Access**—In **Access** mode, the Instant AP serves clients, while also monitoring for rogue Instant APs in the background. If the **Access** mode is selected, perform the following actions: 1. Select **Administrator assigned** in **2.4 GHz** and **5 GHz** band sections. 2. Select appropriate channel number from the **Channel** drop-down list for both **2.4 GHz** and **5 GHz** band sections. 3. Enter appropriate transmit power value in the **Transmit power** text box in **2.4 GHz** and **5 GHz** band sections. **NOTE:** If the transmit power is set to 0, the Instant AP is assigned the last transmitted power value set by the ARM. ■ **Monitor**—In **Monitor** mode, the Instant AP acts as a dedicated monitor, scanning all channels for rogue Instant APs and clients. You can set one radio on the Monitor mode and the other radio on the access mode, so that the clients can use one radio when the other one is in the Air Monitor mode. ■ **Spectrum Monitor**—In **Spectrum Monitor** mode, the Instant AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring Instant APs or from non-WiFi devices such as microwaves and cordless phones. **NOTE:** In this mode, Instant APs do not provide access services to clients. Click **OK**.



By default, the channel and power for an Instant AP are optimized dynamically using ARM. You can override ARM on the 2.4 GHz and 5 GHz bands and set the channel and power manually if desired.

When radio settings are assigned manually by the administrator, the ARM is disabled.

Run the following commands to configure a radio profile:

```
(Instant AP)# wifi0-mode {<access> | <monitor> | <spectrum>}
(Instant AP)# wifi1-mode {<access> | <monitor> | <spectrum>}
```

If the access mode is configured, run the following commands to configure the channel and transmission power:

```
(Instant AP)# a-channel <channel> <tx-power>
(Instant AP)# g-channel <channel> <tx-power>
```

Configuring Maximum Clients on SSID Radio Profiles

You can set the maximum number of clients in every individual Instant AP for SSID profiles operating on the 2.4 GHz and 5 GHz radios. This is a per-AP and per-Radio configuration. This configuration is not persistent and is lost once the Instant AP is rebooted.

Run the following commands to configure maximum clients for an SSID radio profile in the privileged exec mode:

```
(Instant AP)# a-max-clients <ssid_profile> <max-clients>
(Instant AP)# g-max-clients <ssid_profile> <max-clients>
```

Run the following commands to view the maximum clients allowed for an SSID profile:

```
(Instant AP)# show a-max-clients <ssid_profile>
(Instant AP)# show g-max-clients <ssid_profile>
```



You can also set the maximum clients when configuring SSID profiles using the **Max Clients Threshold** parameter in the WebUI and **max-clients-threshold** parameter in the Instant CLI. For more information, see Configuring WLAN Settings for an SSID Profile on page 131.

If the maximum clients setting is configured multiple times, using either the configuration mode or Privileged EXEC mode, the latest configuration takes precedence.

Enabling Flexible Radio

This feature allows the AP to seamlessly switch between modes where the radio resources are either combined in a single 2x2 radio or separated into two 1x1 radios.

You can configure the flexible radio in the following modes:

- 5 GHz mode: acts as a single radio operating on 5 GHz band
- 2.4 GHz mode: acts as a single radio operating on 2.4 GHz band
- 2.4 GHz and 5 GHz mode: acts as two radio interfaces, one operating on 5 GHz band, and the other on the 2.4 GHz band. By default, the flexible radio is set to this mode.

AP-203H, AP-203R, and AP-203RP access points have one radio each, wherein each radio operates on two bands. When the flexible radio mode is at 2.4 GHz or 5 GHz, the radio operates on one band and the Instant AP broadcasts 16 different SSIDs. However, when the flexible radio mode is at 2.4 GHz and 5 GHz, the radio operates on both the bands and the Instant AP broadcasts only 8 SSIDs for each band, even if more than 8 SSIDs are configured. The SSIDs with an index value from 0 to 7 will be broadcasted. You can configure the **Flexible Radio** parameter using the WebUI or the CLI.

The following procedure configures flexible radio:

Table 31: *Steps to Configure Flexible Radio*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Access Points**. 2. Click the Instant AP to edit. 3. Click the **Flexible Radio** tab. 4. Specify the **Mode** from the drop-down list. 5. Click **Save** and reboot the Instant AP.	1. On the **Access Points** tab, click the Instant AP to modify. 2. Click the **edit** link. 3. Click the **Flexible Radio** tab. 4. Specify the **Mode** from the drop-down list. 5. Click **OK** and reboot the Instant AP.

In the CLI

Run the following command to configure the flexible radio mode:

```
(Instant AP)# flex-radio-mode <mode>
```

Enabling Low Power Mode

The Instant CLI allows you to enable or disable the low power mode feature on an Instant AP. Enabling the low power mode feature results in the USB and POE-PSE capabilities, if applicable, on the AP to be disabled, and the requested POE draw is reduced accordingly. The AP switches back to its normal mode when this option is disabled.

The following CLI command enables the low power mode on the AP:

```
(Instant AP)# ap-poe-power-optimization enable
```

The following CLI command disables the low power mode on the AP:

```
(Instant AP)# ap-poe-power-optimization disable
```

The following CLI command deletes the low power mode configuration on the AP:

```
(Instant AP)# no ap-poe-power-optimization
```

Dual 5 GHz Radio Mode

This feature allows the Instant AP to configure two radio interfaces, both running 5 GHz channel. The Instant APs have two radios, one operating on 2.4 GHz band, and the other on 5 GHz band. AP-344 and AP-345 access points support upgrade of the 2.4 GHz radio interface to a 5 GHz radio interface. In dual mode, both radio interfaces can operate on 5 GHz band. You can configure the **dual-5GHz-mode** parameter using the WebUI or the CLI.

The following procedure describes how to configure a dual 5 GHz radio:

Table 32: *Steps to Update Password*

Old WebUI
1. On the **Access Points** tab, click the Instant AP to modify. 2. Click the **edit** link. 3. Click the **Radio** tab.

Old WebUI

4. Select **Enable** from the **Dual 5G Mode** drop-down list.
5. Click **OK** and reboot the Instant AP.

NOTE

The dual-5 GHz-mode configuration is currently not supported in the new WebUI.

The following command configures the dual-5 GHz-mode:

```
(Instant AP)# dual-5GHz-mode {<enable><disable>}
```

NOTE

The dual-5 GHz-mode command is supported only in AP-344 and AP-345 access points.

Split 5 GHz Radio for 550 Series Access Points

Split 5 GHz radio is an Instant feature that leverages the power of software to provide three radios on supported access points. The split 5 GHz radio feature splits the 8X8 5 GHz radio of the supported access points into two 4X4 5 GHz radios operating on the upper and the lower part of the radio antenna offering three radios available for configuration - radio 0 (5 GHz), radio 1 (2.4 GHz) and radio 2 (5 GHz). Radio 0 operates on the lower band and Radio 2 operates on the upper band of the 5 GHz radio. The three radios of the AP can be deployed in either of the configuration modes- Access, Air Monitor and Spectrum monitor. The default mode of these radios is access.

The **dot11a-secondary-radio-profile** is the configuration profile for radio 2. This profile is active when tri-radio is enabled on the AP. The **dot11a-radio-profile**, profile of radio 0, will be used as default by the dot11a-secondary -radio-profile, radio 2, when split 5 GHz radio is enabled. The secondary radio profile supports all configurations available in dot11a-radio-profile including RF zones.

Certain existing configuration parameters do not apply when split 5 GHz-radio is configured. The a-channel and g-channel configuration to set channel power of the radio no longer takes effect. In their place **radio-0-channel**, **radio-1-channel** and **radio-2-channel** commands are used to configure the channel and transmission power of the respective radios.

Feature Limitations

- Client Match does not work when split 5 GHz radio mode is enabled on the access point.
- Mesh is supported but only radio0 can be used as the mesh radio.
- Split 5 GHz mode is only supported with APs powered by DC, PoE BT or dual shared PoE AT power supply.
- Access points require reboot to enable or disable Split 5 GHz radio mode in mesh deployments.

The following procedure configures the split 5 GHz radio mode on the Instant AP,

1. Navigate to **Configuration> Access Points** page and select the **Access Point > edit > Radio** accordion.
2. Select **Enable** from the **Split 5GHz mode** drop down list box to enable the split 5 GHz radio mode. To disable the feature, select **Disable** from the **Split 5GHz mode**. The default option is disabled.
3. The Radio 2 settings are now available for configuration under the Radio 2 accordion.

4. Choose a radio mode from the **Mode** drop-down list box.
5. Select a channel assignment method
   - **Adaptive Radio Management assigned** - If this option is selected the channels for the radio is intelligently assigned by the access point.
   - **Administrator Assigned** - If this option is selected, select the channel and the transmit Power in the **Channel** and **Transmit power** fields.
6. Click **Save**.

To configure split 5 GHz radio mode for all supported APs in the network cluster.

1. Navigate to **Configuration> Networks** page and select **Show advanced options**.
2. Under **General**, toggle the **Split 5GHz mode** switch to enable or disable Split 5 GHz mode globally for supported APs in the network. The default option is disabled.
3. Click **Save**.

To configure the radio profile settings for the secondary 5 GHz radio,

1. Navigate to **Configuration > RF > Show advanced options>Radio** accordion.
2. Click **+** in the **Secondary 5GHz band** table and define the radio settings for the secondary 5 GHz radio. For information on configuration parameters for the radio profile, see Configuring Radio Settings on page 377.
3. Click **OK**.

The following configurations do not require an AP reboot to take effect.

Configuring Split 5 GHz Radio

The following command is a global configuration and a per-ap command. When configured globally, all supported APs will work in the split 5 GHz mode. To disable split 5 GHz radio on selected APs override the global setting using the per-ap command. The per-ap command takes priority over the global configuration. The default value for this command is disabled.

To enable the split 5 GHz feature, use the **split-5ghz-mode enabled** command.

```
(Instant AP) # split-5ghz-mode enabled
```

To disable the split 5 GHz feature, use the **split-5ghz-mode disabled** or **no split-5ghz-mode** command.

```
(Instant AP) # split-5ghz-mode disabled
(Instant AP) # no split-5ghz-mode
```

To configure radio profile settings of radio2, use the **rf dot11a-secondary-radio-profile <name>** command. The secondary profile is active only when split 5 GHz radio is enabled on the AP. The values of the dot11a-radio-profile is used as default by the secondary radio profile.

```
(Instant AP) # rf dot11a-secondary-radio-profile <name>
```

See *Aruba Instant 8.x CLI Reference Guide* for information on configurable parameters.

Enabling/ Disabling radios

When split 5 GHz radio is enabled, use the **radio-0-disable**, **radio-1-disable** and **radio-2-disable** commands to disable the respective radios.

```
(Instant AP) # radio-1-disable
(Instant AP) # radio-2-disable
```

Radio Channel and Transmission Power

When tri-radio is enabled, use the **radio-0-channel**, **radio-1-channel** and **radio-2-channel** to configure the static channel and transmission power for the respective radios. Please note radio0 and radio2 supports 5 GHz channels and radio1 supports 2.4 GHz channels.

```
(Instant AP) # radio-0-channel <36-64>
(Instant AP) # radio-1-channel <1-11>
(Instant AP) # radio-2-channel <100-161>
```

Radio Mode

When split 5 GHz radio is enabled, the **wifi2-mode** command is available to configure the mode for radio2. This command is a per-ap setting.

```
(Instant AP) # wifi2-mode <monitor | spectrum | access>
```

WLAN SSID profiles

To control SSIDs being created in the 5 GHz radio, use the **allowed-5ghz-radio** parameter under the particular wlan ssid-profile command to specify under which 5 GHz radio the SSID should be broadcasted. The default value for the command is all.

```
(Instant AP) #wlan ssid-profile <name>
(Instant AP) # allowed-5ghz-radio <first-dot11a-radio-only | second-dot11a-radio-only
| all>
```

To view the view configuration information of radios, use the following show commands:

- Show aps
- Show radio config
- Show radio profile
- Show ids radio

To troubleshoot radios and view debug information, use the following troubleshooting commands:

- Show ap debug radio-stats radio-id
- Show ap debug radio-info radio-id
- Show ap debug power-table radio-id

Air Slice

Aruba's key RF differentiation, Air Slice, designed for 11ax APs optimizes user experience and assures QoA to enterprise applications. Air Slice combines AppRF and UCC for classifying applications and it also supports custom flow definitions. Air Slice uses a combination of priority queuing, dynamic WMM boosting, and 11ax based radio resource scheduling to prioritize enterprise applications in the presence of competing background traffic flows to meet latency and bandwidth requirements. Air Slice solution built on OFDMA, MU-MIMO, and TWT constructs offer the following services:

- Guaranteed bit rate
- Battery life extension
- Bounded latency and jitter

Air Slice supports multiple services like gaming, IoT, voice and video, and so on. Air Slice support is available for all AP clients. However, 802.11ax clients have enhanced benefits due to efficient uplink and downlink traffic scheduling of 802.11ax standard. Air Slice also allows network administrators to select a list of applications to be prioritized.



Air Slice is supported only on 530 Series and AP-555 access points. It is mandatory to enable DPI on the AP before configuring Air Slice, else an error will be reported.

The following procedure configures Air Slice Policy and Application Monitoring on an Instant AP:

1. Navigate to **Configuration** > **System** > **General**.
2. Click the **Show advanced options** tab.
3. Slide the toggle switch next to **AirSlice policy**, to the right, to enable the feature.
4. Slide the toggle switch next to **Application monitoring**, to the right, to enable the feature.
5. Click **Save**.

The following CLI command configures Air Slice policy on the AP:

```
(Instant AP)(config)# airslice-policy
```

The following CLI command configures Application Monitoring on the AP:

```
(Instant AP)(config)# application-monitoring
```

The following CLI command is used to view the Application Monitoring list:

```
(Instant AP)# show app-monitoring list
```

The following CLI command is used to view the client statistics based on the MAC ID:

```
(Instant AP)#show ap debug airslice client-stats <mac>
```

ACL Rule Modifications

The **session acl** list and **acl rule** list are modified based on the network configuration. When rule **action** is permitted, the rule can configure the new option **markapp** with **custom appid**. Instant allows multiple rules to configure the same custom name, and once the ACL is active, the action takes effect with the custom application ID on the session.

The following procedure configures a custom application ID in the access rule:

1. Navigate to **Configuration** > **Security** > **Roles**. The settings in the Roles tab are displayed.
2. Select the role for which you want to configure access rules.
3. In the **Access rules** section, click **+** to add a new rule. The **New rule** window is displayed.
4. Ensure that the rule type is set to **Access Control**.
5. Select **Network** under the **Service** category.
6. Under **Options**, select the **Mark Application** checkbox.
7. Select one of the custom values from the drop-down list.
8. Click **OK**.



Alternatively, you can configure access rules for a wired or wireless client through the WLAN wizard or the Wired Profile window.

```
The following CLI command configures a session ACL with a custom application ID:
(Instant AP)(config)# wlan access-list session ses-acl
(Instant AP)(Session-ACL "ses-acl")# rule 10.1.1.1 255.255.255.255 20.1.1.1
255.255.255.255 match 17 0-65535 0-65535 permit markapp custom1
(Instant AP)(Session-ACL "ses-acl")#end
```

The following CLI command configures a with a rule ACL with a custom application ID:

```
(Instant AP)(config)# wlan access-rule WirelessRule
(Instant AP)(Access Rule "WirelessRule")# rule 10.1.1.1 255.255.255.255 match 17 0-
65535 0-65535 permit markapp custom1
(Instant AP)(Access Rule "WirelessRule")# access-list session ses-acl
```

The following CLI command displays the custom appid configured on the rule ACL:

```
(Instant AP)# show access-rule WirelessRule
```

The following CLI command displays the custom appid confifured on the session ACL:

```
(Instant AP)#show access-list ses-acl
```

In addition to the custom applications, Air Slice is supported only for the applications listed below:

- Zoom
- Slack
- Skype
- Lync Online
- ALG Skype for Business
- WebEx
- GoToMeeting
- Office365
- Dropbox
- Amazon AWS
- Github
- Micrsoft Excel Online
- Onedrive
- Outlook
- Microsoft Planner
- Microsoft Powerpoint Online
- Microsoft SharePoint Online
- Microsoft Sway
- Microsoft Teams
- Microsoft Word Online
- Yammer
- ALG Wifi-Calling

Support for Input-Filter on BLE Devices

When IoT transport profiles are configured, BLE-devices are filtered based on the IoT transport profiles which may include device class, UUID, or vendor filters. Only BLE devices that should be reported are stored in the BLE-table and data loss is avoided.

The following CLI command enables the entry filter:

```
(Instant AP)# ble-init-action input-filter-enable
```

The following CLI command disables the entry filter:

```
(Instant AP)# ble-init-action input-filter-disable
```

The following command is used to view the latest filtered BLE-device

```
(Instant AP)#show ap debug ble-input-filter-stats
```

Configuring Uplink VLAN for an Instant AP

Instant supports a management VLAN for the uplink traffic on an Instant AP. You can configure an uplink VLAN when an Instant AP needs to be managed from a non-native VLAN. After an Instant AP is provisioned with the uplink management VLAN, all management traffic sent from the Instant AP is tagged with the management VLAN.



Ensure that the native VLAN of the Instant AP and uplink are not the same.

The following procedure describes how to configure the uplink management VLAN on an Instant AP:

Table 33: *Steps to Configure Uplink Management VLAN*

New WebUI	Old WebUI
To configure uplink management VLAN: 1. In the **Access Points** tab, select the Instant AP to modify and click **edit**. 2. Select the **Uplink** tab. 3. In the **Uplink Management VLAN** text box, specify the VLAN. 4. Click **OK**. 5. Reboot the Instant AP.	To configure uplink management VLAN: 1. In the **Access Points** tab, select the Instant AP to modify and click **edit**. 2. Select the **Uplink** tab. 3. In the **Uplink Management VLAN** text box, specify the VLAN. 4. Click **OK**. 5. Reboot the Instant AP.

The following CLI command configures an uplink management VLAN:

```
(Instant AP)# uplink-vlan <VLAN-ID>
```

The following CLI command is used to view the uplink VLAN status:

```
(Instant AP)# show uplink-vlan
Uplink Vlan Current      :0
Uplink Vlan Provisioned  :1
```

Changing the Instant AP Installation Mode

By default, all Instant AP models initially ship with an indoor or outdoor installation mode. This means that Instant APs with an indoor installation mode are normally placed in enclosed, protected environments and those with an outdoor installation mode are used in outdoor environments and exposed to harsh elements.

In most countries, there are different channels and power that are allowed for indoor and outdoor operation. You may want to change an Instant AP's installation mode from indoor to outdoor or vice versa.

The following procedure configures an installation mode for the Instant AP:

Table 34: *Steps to Configure Installation Mode*

New WebUI	Old WebUI
1. To configure the installation mode for an Instant AP:	To configure the installation mode for an Instant AP: 1. In the **Access Points** tab, select the Instant AP to modify and click **edit**.

New WebUI	Old WebUI
2. Navigate to the **Configuration > Access Points** page. 3. Select the Instant AP from the **Access Points** list and click **Edit**. 4. Expand **Installation Type** and select one of the three installation options - **Default**, **Indoor** or **Outdoor**. 5. Click **Save** 6. Reboot the Instant AP. **NOTE:** By default, the **Default** mode is selected. This means that the Instant AP installation type is based on the Instant AP model.	2. Under the **Installation type** tab, select one of the three installation options - **Default**, **Indoor** or **Outdoor**. **NOTE:** By default, the **Default** mode is selected. This means that the Instant AP installation type is based on the Instant AP model. 3. Click **OK**. 4. Reboot the Instant AP.

The following CLI command configures the Installation Mode for an Instant AP:

```
(Instant AP)# ap-installation <type[default|indoor|outdoor]>
```

The following CLI command is used to view the installation type of the Instant APs:

```
(Instant AP)# show ap allowed-channels
```

Changing USB Port Status

The USB port can be enabled or disabled based on your uplink preferences. If you do not want to use the cellular uplink or 3G/4G modem in your current network setup, you can set the USB port status to disabled. By default, the USB port status is enabled.

The following procedure configures the USB port status:

Table 35: *Steps to Configure USB Port Status*

New WebUI	Old WebUI
To change the USB port status: 1. Navigate to the **Configuration > Access Points** page. 2. Select the Instant AP from the **Access Points** list and click **Edit**. 3. Expand **Uplink**. 4. Toggle the **USB port** switch to enable or disable the USB port. 5. Click **Save**. 6. Reboot the Instant AP.	To change the USB port status: 1. In the **Access Points** tab, select the Instant AP to modify and click **edit**. 2. Select the **Uplink** tab. 3. In the **USB port** drop down list box, select either one of the following options: a. **Disabled**—To disable the port status. b. **Enabled**—To re-enable the port status. 4. Click **OK**. 5. Reboot the Instant AP.

The following CLI command disables the USB port:

```
(Instant AP)# usb-port-disable
```

The following CLI command enables the USB port:

```
(Instant AP)# no usb-port-disable
```

The following CLI command is used to view the USB port status:

```
(Instant AP)# show ap-env
Antenna Type:External
usb-port-disable:1
```

Master Election and Virtual Controller

Instant does not require an external Mobility Controller to regulate and manage the Wi-Fi network. Instead, every Instant AP in the same broadcast domain automatically organizes together to create a virtual controller for the network. The virtual controller represents a single pane of glass that regulates and manages a Wi-Fi network at a single installation location, performing configuration and firmware management of all its member access points. The virtual controller architecture also ensures that a single AP sets up and manages the VPN tunnel to a mobility controller in the data center, if configured, and allows client traffic from all member APs to share the VPN tunnel.

The main capabilities supported by the virtual controller are listed below:

- Acts as a central point of configuration. The configuration is distributed to other Instant APs in a network.
- Provides DHCP servers to the cluster.
- Provides VPN tunnels to a Mobility Controller.
- Provides Central, AirWave, and Activate interaction.

Master Election Protocol

The Master Election Protocol enables the Instant network to dynamically elect an Instant AP to take on a virtual controller role and allow graceful failover to a new virtual controller when the existing virtual controller is not available. The election beacons are broadcast and unicast L2 frames are used between the virtual controller and the slave Instant APs. This protocol ensures stability of the network during initial startup or when the virtual controller goes down by allowing only one Instant AP to self-elect as a virtual controller. When an existing virtual controller is down, a new virtual controller is elected by the master election protocol. This protocol is initiated by any non-virtual controller Instant AP that no longer receives beacon frames from an active virtual controller.

An Instant AP is elected as a master by one of the following methods:

1. **Enforced**—In this method, Instant APs in preferred, 3G/4G uplink, mesh portal, or stand-alone mode are elected as the master. However Instant APs in mesh point, or hierarchy down side mode are not elected as the master.
2. **Random Intervals**—In this method, a quick Instant AP election takes place when the Instant APs boot. A re-election takes place when the existing master Instant AP is down. This results in random election of a master Instant AP.
3. **Versus Policy**—This is a method by which multiple Instant APs in a cluster are competing with each other to become a master. The Instant AP with higher priority, higher uptime or a bigger MAC address becomes the master. The Instant AP with lesser priority, lesser uptime or a smaller MAC address becomes the slave.

Preference to an Instant AP with 3G/4G Card

The Master Election Protocol prefers the Instant AP with a 3G/4G card when electing a virtual controller for the Instant network during the initial setup.

The virtual controller is selected based on the following criteria:

- If there is more than one Instant AP with 3G/4G cards, one of these Instant APs is dynamically elected as the virtual controller.
- When an Instant AP without 3G/4G card is elected as the virtual controller but is up for less than 5 minutes, another Instant AP with 3G/4G card in the network is elected as the virtual controller to replace it and the previous virtual controller reboots.
- When an Instant AP without 3G/4G card is already elected as the virtual controller and is up for more than 5 minutes, the virtual controller will not be replaced until it goes down.

Preference to an Instant AP with Non-Default IP

The Master Election Protocol prefers an Instant AP with non-default IP when electing a virtual controller for the Instant network during initial startup. If there are more than one Instant APs with non-default IPs in the network, all Instant APs with default IP will automatically reboot and the DHCP process is used to assign new IP addresses.

Viewing Master Election Details

The following CLI command is used to verify the status of an Instant AP and master election details:

```
(Instant AP)# show election statistics
(Instant AP)# show summary support
```

Manual Provisioning of Master Instant AP

In most cases, the master election process automatically determines the best Instant AP that can perform the role of virtual controller, which will apply its image and configuration to all other Instant APs in the same Instant AP management VLAN. When the virtual controller goes down, a new virtual controller is elected.

Provisioning an Instant AP as a Master Instant AP

The following procedure describes how to provision an Instant AP as a master Instant AP:

Table 36: *Steps to Provision an Instant AP as a Master AP*

New WebUI	Old WebUI
To provision an Instant AP as a master Instant AP: 1. Navigate to the **Configuration > Access Points** page. 2. Select the Instant AP from the **Access Points** list and click **Edit**. 3. Expand **Uplink**. 4. Toggle the **Preferred master** switch to enable or disable the option. 5. Click **Save**.	To provision an Instant AP as a master Instant AP: 1. In the **Access Points** tab, select the Instant AP to modify and click **edit**. 2. Select the **General** tab. 3. In the **Preferred master** drop down list box, select **Enabled**. This option is disabled by default. 4. Click **OK**.

The following CLI command provisions an Instant AP as a master Instant AP:

```
(Instant AP)# iap-master
```

The following CLI command is verifies if the Instant AP is provisioned as master Instant AP:

```
(Instant AP)# show ap-env
Antenna Type:Internal
Iap_master:1
```

Only one Instant AP in a cluster can be configured as the preferred master.

Adding an Instant AP to the Network

To add an Instant AP to the Instant network, assign an IP address. For more information, see Assigning an IP address to the Instant AP on page 19.

After an Instant AP is connected to the network, if the Auto-Join feature is enabled, the Instant AP inherits the configuration from the virtual controller and is listed in the **Access Points** tab.

The following procedure describes how to manually add an Instant AP to the network:

Table 37: *Steps to Manually Add an Instant AP*

New WebUI	Old WebUI
To add an Instant AP to the network: 1. Navigate to the **Configuration > Access Points** page. 2. Click **+** in the **Access Points** table. 3. In the **New Access Point** window, enter the MAC address for the new Instant AP. 4. Click **OK**.	To add an Instant AP to the network: 1. In the **Access Points** tab, click **New**. 2. In the **New Access Point** window, enter the MAC address for the new Instant AP. 3. Click **OK**.

Removing an Instant AP from the Network

The following procedure describes how to manually remove an Instant AP from the network:

Table 38: *Steps to Manually Remove an Instant AP*

New WebUI	Old WebUI
To remove an Instant AP from the network: 1. Navigate to the **Configuration > Access Points** page. 2. Select the Instant AP from the **Access Points** list and click **Delete**. 3. Click **OK** to confirm the deletion.	To remove an Instant AP from the network: 1. In the **Access Points** tab, select the Instant AP to delete. 2. Click the **x** icon displayed beside **edit** button to delete the Instant AP. 3. Click **Delete Now** to confirm the deletion.

The deleted Instant APs cannot join the Instant network anymore and are not displayed in the WebUI. However, the master Instant AP details cannot be deleted from the virtual controller database.

Support for BLE Asset Tracking

Starting from Instant 6.5.2.0, Instant APs can monitor BLE asset tags to track the location of time-sensitive, high-value assets embedded with BLE tags.

BLE tags are located through the following steps:

1. Instant AP beacons scan the network for BLE tags.
2. When a tag is detected, the Instant AP beacon sends information about the tag to the Instant AP, including the MAC address and RSSI of the tag. This data is maintained in a list by the BLE daemon process on the Instant AP.

3. The list of tags is sent from the BLE daemon process on the Instant AP to the BLE relay process on the Instant AP.
4. The Instant AP opens a secure WebSocket connection with the designated WebSocket endpoint on the management server, such as the Meridian editor.
5. After receiving the list of tags from the Instant AP, the management server calculates the location of each tag by triangulating the tag's RSSI data on a floor plan.



Each BLE tag must be heard by at least three Instant AP beacons for triangulation.

The following CLI command is used to view the list of BLE tags discovered and reported by the Instant AP.

```
(Instant AP)# show ap debug ble-table assettags
```

The following CLI command is used to manage BLE tag reporting and logging.

```
(Instant AP) (config)# ble_relay mgmt-server type ws <ws-endpoint>
```

The following CLI commands are used to view BLE tag data:

```
(Instant AP)# show ap debug ble-relay tag-report
(Instant AP)# show ap debug ble-relay disp-attr
(Instant AP)# show ap debug ble-relay ws-log
(Instant AP)# show ap debug ble-relay iot-profile
(Instant AP)# show ap debug ble-relay jobs
(Instant AP)# show ap debug ble-relay report
```

IoT Endpoints

Instant introduces an option to transport BLE information from Instant APs to endpoints over a WebSocket connection. An endpoint is a physical computing device that performs a task as part of an Internet-connected product or service. IoT transport profiles must be created to transport BLE data from Instant APs to the endpoints. Additionally, users have an option to remove IoT profiles from the Instant APs.

Instant APs contain a built-in IoT protocol that can send BLE information to the following endpoint types:

- Meridian Beacon Management
- Meridian Asset Tracking
- Telemetry-Https
- Telemetry-Websocket
- AssaAbloy
- ZF



When the meridian asset tracking endpoint is configured and the firmware is upgraded to Instant 8.7.0.0, the CA certificate should be uploaded in order to connect to the meridian server.

The following payload messages can be sent to the endpoints:

- BLE data
- Managed beacons
- Managed tags
- ZF tags
- All
- Enocean Sensors
- Enocean Switches
- iBeacon
- sBeacon
- Eddystone
- Assa Abloy
- Unclassified
- Aruba Sensors
- Mysphera
- Wi-Fi Tags
- Wi-Fi Associated Stations
- Wi-Fi Unassociated Stations
- Ability Smart Sensor
- Williot
- Zigbee Socket Device
- Serial Data
- Exposure Notification

The following CLI command configures an IoT transport profile:

```
(Instant AP)(config)# iot transportProfile sample
```

The following CLI command assigns an IoT transport profile:

```
(Instant AP)(config)# iot usetransportProfile sample
```

The following CLI command is used to view the IoT profile status:

```
(Instant AP)# show iot transportProfile
```

Zigbee-Based IoT

Assa Abloy is an industry leading provider of door lock hardware. Some door locks from Assa Abloy use ZigBee for back-end connectivity. An AP from Aruba with a USB ZigBee radio provides gateway services to relay the door lock information to a management server.

This allows an administrator to avoid deploying a network of ZigBee routers and gateways to provide connectivity to each door lock. A single network can handle both Wi-Fi and ZigBee devices. An AP from Aruba provides ZigBee gateway functionality that offers a global standard to connect many types of ZigBee networks to the Internet or with service providers. Aruba integrates ZigBee networking operations as part of the BLE daemon process.

ZigBee devices are of three kinds:

- ZigBee Coordinator (ZC)—The ZC is the most capable device. It forms the root of the network tree and may bridge to other networks. There is only one ZC in each ZigBee network.

- ZigBee Router (ZR))—A ZR runs an application function and may act as an intermediate router that transmits data from other devices.
- ZigBee End Device (ZED)—A ZED contains enough functionality to communicate with the parent node (either a ZC or ZR). A ZED cannot relay data from other devices. This relationship allows the ZED to be asleep for a significant amount of time thereby using less battery.

An AP acts as a ZC and forms the ZigBee network. It selects the channel, PAN ID, security policy, and stack profile for a network. A ZC is the only device type that can start a ZigBee network and each ZigBee network has only one ZC. After the ZC has started a network, it may allow new devices to join the network. It may also route data packets and communicate with other devices in the network. Aruba solution does not utilize a ZR.

Assa Abloy locks act as ZEDs in the network. After they connect to the ZC, they communicate with a management server (Visionline server) over an encrypted tunnel through Aruba gateway.

The BLE relay process in Aruba AP handles telemetry streams to third party servers including Visionline server from Assa-Abloy.

Support for Zigbee USB Dongle

APs which do not have an integrated Zigbee radio (for example: 300 Series access points) support Aruba Zigbee USB dongle and provide IoT services. The Aruba Zigbee USB dongle provides the same capabilities that are provided by the integrated Zigbee radio in some APs (for example: 500 Series access points). The Aruba Zigbee USB dongle uses the Nordic nRF52840 chipset and is an AP accessory that plugs into the USB port of an AP. Based on available USB ports, an AP can support multiple Aruba Zigbee USB dongles at same time and a Aruba Zigbee USB dongle can support multiple radio devices (Zigbee client devices) at the same time.

Creating a Zigbee-based IoT Transport Profile

The following procedure describes how to create a Zigbee-based IoT transport profile:

1. Navigate to **Configuration** > **Services** > **IoT**.
2. Under the **Transport Streams** section, click **+**. The **New** window will be displayed.
3. In the **Name** textbox, enter a name for the Zigbee transport profile.
4. In the **Server URL** textbox, enter a endpoint URL.
5. In the **Server type** down-down, select one of the endpoint types.
6. In the **Device classes**, select either the **Aruba Beacons** or **Aruba Sensors** checkbox.
7. Slide the **State** toggle switch to the right to enable this option.
8. Configure a **Reporting interval**.
9. If you want to configure a proxy server, enter the required details under the **Proxy** section.
10. Under **Authentication**, enter the **Access token**.
11. Select the checkboxes that apply under **Device filters** and enter the values in the text box.
12. Click **OK**.
13. Click **Save**.

The following CLI command creates a ZigBee-based IoT transport profile:

```
(Instant AP)(config)# iot transportProfile Sample-Zigbee-Transport
```

The following CLI command configures the ZigBee end point type:

```
(Instant AP)(IoT Transport Profile "Sample-Zigbee-Transport")# endpoinType <endpoint>
```

The following CLI command configures the ZigBee end point URL:

```
(Instant AP)(IoT Transport Profile "Sample-Zigbee-Transport")# endpointURL
https://192.168.1.200
```

The following CLI command configures the ZigBee username:

```
(Instant AP)(IoT Transport Profile "Sample-Zigbee-Transport")# username admin
```

The following CLI command configures the ZigBee password:

```
(Instant AP)(IoT Transport Profile "Sample-Zigbee-Transport")# password <password>
```

The following CLI command configures the ZigBee endpoint:

```
(Instant AP)(IoT Transport Profile "Sample-Zigbee-Transport")# payloadcontent
<endpoint>
```

Applying a ZigBee-Based IoT Transport Profile

The following CLI command applies the ZigBee-based IoT transport profile:

```
(Instant AP)(config)# iot useTransportProfile Sample-Zigbee-Transport
```

Configuring a ZigBee-Based IoT Radio Profile

The following CLI command creates a ZigBee-based IoT radio profile:

```
(Instant AP)(config)# iot radio-profile Sample-Zigbee-Radio
```



An AP supports up to 2 endpoint types or IoT radio profiles. The IoT radio profile name can be up to 32 characters.

The following CLI command configures the ZigBee radio mode:

```
(Instant AP)(IoT Radio Profile "Sample-Zigbee-Radio")# radio-mode zigbee
```

The following CLI command configures the radio instance on the ZigBee-based IoT radio profile:

```
(Instant AP)(IoT Radio Profile "Sample-Zigbee-Radio")# radio-instance external
```

The following CLI command configures a zigbee operation mode on the IoT radio profile:

```
(Instant AP)(IoT Radio Profile "Sample-Zigbee-Radio")# zigbee-opmode cordinator
```

The following table summarizes the relationship between radio-mode and radio-enable:

The following CLI command configures the ZigBee co-ordinator operation mode:

```
(Instant AP)(IoT Radio Profile "Sample-Zigbee-Radio")# zigbee-opmode coordinator
```



Instant currently supports only the **coordinator** opmode.

The following CLI command configures the ZigBee channel:

```
(Instant AP)(IoT Radio Profile "Sample-Zigbee-Radio")# zigbee-channel 11
```



Allowed Zigbee channels are auto and 11 through 26. The default Zigbee channel is auto.

The following CLI command is used to set the configured Zigbee based IoT radio profile on the Instant AP:

```
(Instant AP)(config) # iot use-radio-profile Sample-Zigbee-Radio
```

Viewing ZigBee-Based IoT Radio Profile

The following CLI command is used to view the list of ZigBee-based IoT radio profiles:

```
(Instant AP)# show iot radio-profile
```

The following CLI command is used to view the status of a ZigBee-based IoT radio profile:

```
(Instant AP)# show iot radio-profile Sample-Zigbee-Radio
```

The following CLI command is used to view the ZigBee radio configuration of an AP:

```
(Instant AP)# show ap debug zigbee radio-table
```

Zigbee Sockets

Zigbee Socket Device (ZSD) can be configured and applied as a filter in IoT transport. With ZSD, you can specify the source endpoint, destination endpoint, destination profile ID or destination cluster ID and the packets between the ZigBee devices and server are transmitted through the Aruba Telemetry Websocket.

The following CLI command configures a ZSD filter:

```
(Instant AP)(config)# iot transportProfile <profile_name>
(Instant AP)(IoT Transport Profile "<profile_name>")#ZSDFilter <Zigbee_Socket_Device_
Filter>
```

The following CLI command configures the Zigbee Socket Device Profile:

```
(Instant AP)(config)# zigbee socket-device-profile <profile_name>
(Instant AP)(Zigbee Socket Device Profile "<profie_name")# inbound <source_endpoint>
<endpoint> <profile> <cluster>
(Instant AP)(Zigbee Socket Device Profile "<profie_name")# outbound <source_endpoint>
<endpoint> <profile> <cluster> [aps-ack]
```

Zigbee Service Profile

The following CLI command configures or modifies a ZigBee service profile:

```
(Instant AP)(config)# iot service-profile <profile_name>
```

The following CLI command sets a Zigbee service profile on an Instant AP:

```
(Instant AP)(config)# zigbee use-service-profile <profile_name>
```

The following CLI command displays the list of ZigBee service profiles:

```
(Instant AP)(config)# show zigbee service-profile
```

The following CLI command displays the details of a specific ZigBee service profile:

```
(Instant AP)(config)# show zigbee service-profile <profile_name>
```

Aruba Sensor Values

An Aruba AP actively scans for BLE devices in the background. An AP listens to both advertisement frames and scan response frames. An AP classifies and parses the content of both types of frames and reports BLE telemetry to subscribers.

For BLE devices that an AP does not support, server type Generic-Https and Generic-Websocket can transport the broadcasting frame payload without parsing. Aruba APs support any BLE device that conforms to Aruba BLE Telemetry Advertisement Specification. Hence, even if an AP does not 't know anything else about a BLE device, it can parse and report telemetry and sensor information to a subscriber.

Configuring Aruba Sensor in IoT Transport Profile

The following CLI command configures an Aruba sensor in an IoT transport profile:

```
(Instant AP)(config) #iot transportProfile <profile_name>
(Instant AP)(IoT Data Profile "<profile_name>") #payloadContent aruba-sensors
```

Reporting Sensor Values

Some sensor values are reported periodically to the configured server. The reporting interval is configured in the IoT transport profile. However, some sensor values are reported immediately without waiting for the next reporting interval. For example, events based on intrusion, fire, water level, and so on are reported immediately.

Immediate reporting is applicable for any sensor and the reporting is based on the sensor values. Following are some of the sensor values that are reported immediately based on any change:

- Alarm water
- Alarm smoke
- Alarm fire
- Alarm glassbreak
- Alarm intrusion
- Input switch
- Input rocker
- Sensor contact
- Vendor data

Immediate reporting is applicable for telemetry-HTTPS and telemetry-websocket server types configured in the IoT transport profile. Aruba IoT infrastructure supports any BLE device that conforms to Aruba BLE telemetry advertisement specification. If an information element type is not supported, but they are still part of the vendor specification, it is stored in vendor-data field of the BLE device in the BLE database. If there is any change to this vendor-data, it is reported immediately.



Vendor data is supported for EnOcean and Aruba sensors.

BluConsole

Instant supports iOS BluConsole mobile application that allows a user to access the serial console of an AP over BLE. The BluConsole mobile application performs a secure exchange of keys with the BLE service ABLECONSOLE that runs on an AP and encrypts traffic over the BLE connection.

Before establishing a BLE connection, the BluConsole mobile application requests user permission to pair with an AP. Bonding is not performed until the user allows permission. User is requested permission every time the BluConsole mobile application connects to an AP.

HanVit Sensors

HanVit is a leading provider of BLE asset tags. When a HanVit asset tag broadcasts advertisements, an AP receives the RSSI of the asset tag and computes its location. The AP transfers the location data of a BLE asset tag along with sensor data to a management server. A management server can subscribe to the telemetry data with configuration of an IoT profile.

Configuring HanVit Sensor in IoT Transport Profile

Aruba sensors match with the following server types:

- Meridian-Asset-Tracking
- Meridian-Beacon-Management
- Telemetry-Https
- Telemetry-Websocket

The following CLI commands configure an Aruba sensor in an IoT transport profile:

```
(Instant AP)(config)# iot transportProfile Sample-Https
(Instant AP)(IoT Data Profile "Sample-Https")# endpointType telemetry-https
(Instant AP)(IoT Data Profile "Sample-Https")# payloadContent aruba-sensors

(Instant AP)(config)# iot transportProfile Sample-Websocket
(Instant AP)(IoT Data Profile "Sample-Websocket")# endpointType telemetry-websocket
(Instant AP)(IoT Data Profile "Sample-Websocket")# payloadContent aruba-sensors

(Instant AP)(config)# iot transportProfile Sample-Meridian-Asset-Tracking
(Instant AP)(IoT Data Profile "Sample-Meridian-Asset-Tracking")# endpointType
Meridian-Asset-Tracking
(Instant AP)(IoT Data Profile "Sample-Meridian-Asset-Tracking")# payloadContent aruba-
sensors

(Instant AP)(config)# iot transportProfile Sample-Meridian-Beacon-Management
(Instant AP)(IoT Data Profile "Sample-Meridian-Beacon-Management")# endpointType
Meridian-Beacon-Management
(Instant AP)(IoT Data Profile "Sample-Meridian-Beacon-Management")# payloadContent
aruba-sensors
```

SoluM ESL Gateway

SoluM is a leading provider of Electronic Shelf Label (ESL) services. An ESL tag is used to display product pricing on store shelves. Typically, ESLs are attached to the front edge of store shelves. The product pricing is automatically updated whenever the price is changed from a SoluM gateway server.

A SoluM gateway server pushes configuration information, ESL image, and SoluM gateway firmware through an Aruba AP to a SoluM gateway. A SoluM gateway is a 802.15.4 Zigbee-based USB dongle. A SoluM gateway plugs into the USB port of an Aruba AP, obtains an IP address, and transfers data from a SoluM gateway server to the ESL tags that are within the range of the SoluM gateway. The SoluM gateway works as a wired client to the ESL tags and SoluM gateway. The USB port of the AP works as a wired Ethernet port and supports bridge mode. An Ethernet port on the AP allows the SoluM gateway traffic to pass through.

In the bridge mode, the USB0 ether interface of the SoluM gateway which connects to the AP obtains an IP address (either static or dynamic). The USB ether interface which is created in the AP does not use an IP address, it only receives or sends data packets to the SoluM gateway without changing the packets.

A SoluM gateway supports hot plug in and can be plugged into an Aruba AP at any time irrespective of AP staus (up or down). The USB port of the AP is recognized as CDC-ether and works as a normal wired port. After the AP boots, it recognizes the SoluM gateway. The configured wired port profile for the USB port is used to send or receive data packets.

The SoluM gateway can obtain an IP address by using either DHCP and or using a static configuration. However, if the if static address does not match with the network, the traffic from the SoluM gateway is not allowed.

The following CLI command configures the USB port of an AP as an Ethernet port:

```
(Instant AP)(config)# enet-usb-port-profile
```

Hanshow ESL Gateway

Hanshow is a leading provider of ESL services. ESLs are attached to the front edge of store shelves. The product pricing is automatically updated whenever the price is changed from a Hanshow gateway server.

A Hanshow gateway server pushes configuration information, ESL image, and Hanshow gateway firmware through an Aruba AP to a Hanshow gateway. A Hanshow gateway is a USB dongle (running proprietary wireless protocol) that plugs into the USB port of an Aruba AP, obtains an IP address, and transfers data from a Hanshow gateway server to the ESL tags that are within the range of the Hanshow gateway. The Hanshow gateway works as a wired client to the ESL tags and Hanshow gateway. The USB port of the AP works as a wired Ethernet port and supports bridge mode. An Ethernet port on the AP allows the Hanshow gateway traffic to pass through.

In the bridge mode, the USB0 ether interface of the Hanshow gateway which connects to the AP obtains an IP address (either static or dynamic). The USB ether interface which is created in the AP does not use an IP address, it only receives or sends data packets to the Hanshow gateway without changing the packets.

A Hanshow gateway supports hot plug in and can be plugged into an Aruba AP at any time irrespective of AP status (up or down). The USB port of the AP is recognized as CDC-ether and works as a normal wired port. After the AP boots, it recognizes the Hanshow gateway. The configured wired port profile for the USB port is used to send or receive data packets.

The Hanshow gateway can obtain an IP address by using either DHCP and or using a static configuration. However, if the if static address does not match with the network, the traffic from the Hanshow gateway is not allowed.

The following CLI command configures the USB port of an AP as an Ethernet port:

```
(Instant AP)(config)# enet-usb-port-profile
```

ZF Openmatics Support for ZF BLE Tag Communication

You can manage ZF TAGs and implement BLE location service using the third-party ZF Openmatics. To support this feature, Aruba Instant APs with built-in IoT-protocol radio (BLE) are required. You can configure the Instant APs to support ZF Openmatics using the IoT profiles.

Configuring ZF Openmatics

The ZF TAG data scans and provides feedback to the ZF server if the ZF endpoint is configured in the IoT profiles.



The beaconing mode must be enabled on the BLE radio of the Instant AP.

Configure the IoT transport profile as follows to enable ZF Openmatics support on the Aruba Instant AP:

The following CLI command configures the end point type for ZF Tags:

```
(host) (IoT Data Profile "<profile-name>") #endpointtype ZF
```

The following CLI command configures the end point URL for ZF Tags:

```
(host) (IoT Data Profile "<profile-name>") # endpointURL
https://app.detagtive.com/backend
```



The https://app.detagtive.com/backend is just an example. For final URL, please refer to ZF company's latest update.

The following CLI command configures the username and password for ZF Tags:

```
(host) (IoT Data Profile "<profile-name>") #username <username>
(host) (IoT Data Profile "<profile-name>") #password <password>
```

The following CLI command configures the transport interval for ZF Tags:

```
(host) (IoT Data Profile "<profile-name>") #transportInterval 60
```



The default is 300 seconds. The recommended value for ZF is 60 seconds.

The following CLI command configure the payload content for ZF Tags:

```
(host) (IoT Data Profile "<profile-name>") #payloadContent ZF-Tag
```

The following CLI command applies the IoT profile on the Instant AP:

```
(host) (config) # iot useTransportProfile <Profile>
```

Viewing Third-Party Devices in the BLE Table

The following CLI command is used to view any third-party devices in the BLE table:

```
(host) #show ap debug ble-table generic
```

Viewing the BLE Tag Reports

The following CLI command is used to view the BLE Relay tag reports:

```
(host) #show ap debug ble-relay tag-report
```

Viewing the BLE Relay Jobs

The following CLI command is used to view the pending BLE Relay jobs:

```
(host) #show ap debug ble-relay jobs
```

IoT Data Filter

The data filter in the Iot transport profile reduces the traffic in the telemetry interfaces. The data filter is a string of numbers that map to the IoT API protobuf fields. Following is the mapping of the data filters and the protobuf fields:

Value	Description
#2	reporter
2.1	name
2.3	ipv4
2.4	ipv6
2.5	hwType
2.6	swVersion
2.7	swBuild
2.8	time
#3	reported
3.2	deviceClass
3.3	model
3.4	firmware
3.5	assetId
3.6	publicKey
3.7	lastSeen
3.9	bevent
3.10	rssi
3.11	cell
3.12	beacons
3.13	txpower
3.14	sensors
3.14.1	accelerometer
3.14.2	battery
3.14.3	temperatureC
3.14.4	humidity

Value	Description
3.14.5	voltage
3.14.6	illumination
3.14.7	motion
3.14.8	current
3.14.9	CO
3.14.10	CO2
3.14.11	VOC
3.14.12	resistance
3.14.13	pressure
3.14.14	alarm
3.14.15	contact
3.14.16	occupancy
3.14.17	mechanicalHandle
3.14.18	distance
3.14.19	capacitance
3.16	stats
3.16.1	uptime
3.16.2	adv_cnt
3.16.3	seq_nr
3.17	inputs
3.18	vendorData
3.19	vendorName
3.20	sensorTimestamp
3.21	flags
3.22	localName
3.23	identity

Wiliot Sensors

Wiliot is a leading provider of battery-free BLE tags. An Aruba AP forwards the BLE data from Wiliot sensors immediately after parsing the advertisements and scan responses. The BLE data can be either

actual advertisements or scan responses that are received by the AP. The BLE data is reported to northbound servers over websockets.

The following CLI commands allow the AP to report telemetry-websocket streams:

```
(Instant AP)(config)# iot transportProfile Sample-Websocket
(Instant AP)(IoT Data Profile "Sample-Websocket")# endpointType telemetry-websocket
(Instant AP)(IoT Data Profile "Sample-Websocket")# payloadContent wiliot
```

The following CLI command is used to view the Iot transport profile for Wiliot sensors:

```
(Instant AP)(config)# iot transportProfile Sample-Websocket
IoT Data Profile "Sample-Websocket"
-------------------------
Parameter                                       Value
---------                                       -----
Server Type                                     Telemetry-Websocket
Server URL                                      N/A
Access Token                                    N/A
Client Id                                       N/A
Username                                        N/A
Password                                        N/A
Reporting interval                              600
Device Class Filter                             wiliot
UUID Filter                                     N/A
Movement Filter                                 0
Cell Size Filter                                0
Vendor Filter                                   N/A
Age Filter                                      0
Authentication URL                              N/A
UID Namespace Filter                            N/A
URL Filter                                      N/A
Access ID                                       N/A
Zigbee Socket Device Filter                     N/A
RSSI Reporting Format                           average
choose an environment type                      office
Custom Fading Factor                            20
Iot Proxy Server                                N/A
Iot Proxy User                                  N/A
AP Group                                        N/A
Send device counts only                         Disabled
RTLS Destination MAC Address                    N/A
Data Filter                                     N/A
```

Southbound API

Instant now supports a IoT Southbound API that allows interaction with IoT devices in a generic fashion and does not require any knowledge of the device by Aruba infrastructure. The IoT southbound API runs on top of the Telemetry-WebSocket interface without any additional configuration. The IoT southbound API works asynchronously and accepts actions at any time while the WebSocket connection is up.

Intelligent Power and Temperature Monitoring

The Intelligent Power and Temperature Monitoring feature is an enhancement to the existing IPM feature of Instant APs. IPTM is the combination of both IPM and ITM functions for enhanced optimization of AP operations in changing power and temperature conditions.

In order to manage this optimization, a set of reduction steps can be configured and associated with a priority value. IPTM applies a sequence of reduction steps as defined by the priority definition until the

AP is functioning within the power budget and threshold temperature. This happens dynamically as IPTM constantly monitors the power consumption and temperature of the AP.

IPM and ITM must be enabled separately using the CLI. However, the reduction steps applied for IPM and ITM are the same and are configured under **ipm** command. The IPM and ITM settings configured for the AP can be viewed using the **show running configuration** command.

Important Points to Remember

- By default, IPM and ITM are disabled.
- IPM must be enabled for ITM to function.
- IPM cannot be disabled if ITM is enabled.
- When enabled, IPM and ITM enables all AP functionality initially. IPM and ITM then proceeds to shut down or restrict functionality if the power usage or temperature of the AP goes beyond the power budget and maximum temperature of the AP.
- IPM and ITM do not override pre-existing settings that restrict functionality. For example, when USB functionality is disabled in the provisioning profile, the AP will not enable the functionality when the reduction steps are retracted.

Intelligent Power Management

IPM measures the power utilization of the AP and dynamically adapts to the power budget. IPM dynamically limits the power requirement of the AP as per the available power resources. This is in contrast to the existing static power management method where the power profiles such as POE-AF, POE-AT, PoE-DC, or LLDP are hard-coded for each AP.



IPM is supported on all AP platforms except 203H Series, 203R Series, 207 Series, 303 Series, 303P Series, 318 Series, 320 Series, 360 Series, and 370 Series access points.

ITM must be disabled before disabling IPM.

The following CLI command enables IPM:

```
(Instant AP)(config)# ipm
(Instant AP)(ipm)# enable
```

Reporting Power Values to Central

Instant APs can measure and periodically report their power information such as current, average, minimum, and maximum power consumption values sampled over the previous one minute and report the same to Aruba Central. When Instant APs measure the power values, they send the information to the master Instant AP over a PAPI message. This information is saved and finally sent to Central.



This functionality is supported on IAP-334, IAP-335, IAP-314, IAP-315, IAP-304, IAP-305, AP-303H, AP-344, AP-345, AP-374, AP-375, AP-377, AP-318 access points.

The following CLI command is used to view the power monitoring information:

```
(Instant AP) #show aps power-monitor
```

Intelligent Thermal Management

ITM measures the internal temperature of the AP and dynamically adapts operations to reduce the internal temperature. When enabled, the operations of the AP will be throttled down when the internal

temperature exceeds the maximum threshold. The reduction steps applied to control the temperature are defined using the **ipm-power-reduction-step-prio ipm-step** parameter in the **ipm** command.



ITM is supported on 570 Series, 570EX Series, and AP-518 access points.

IPM must be enabled for ITM to function.

The following CLI command enables ITM:

```
(Instant AP)(config)# itm
```

Configuring Reduction Steps

The priority for reduction steps are configured using the **ipm-power-reduction-step-prio ipm-step** parameter in the **ipm** command. The priority values range from 1-16, 1 being the highest and 16 being the lowest. The reduction steps are applied sequentially, starting with the reduction step assigned the highest priority value. The reduction steps will be applied only if the AP exceeds the power budget or threshold temperature when IPM or ITM is enabled.



Setting a high-priority value to a maximum reduction step like **cpu_throttle_75** reduces the power and temperature level sooner than a minimum or medium reduction step like **cpu_throttle_25** or **cpu_throttle_50**. However, if the reduction step is of the same type but a different level, the smallest reduction should be allocated a higher priority value so that the reduction step takes place earlier. For example, the **cpu_throttle_25** or **radio_2ghz_power_3dB** parameter should have a higher priority level than **cpu_throttle_50** or **radio_2ghz_power_6dB**, respectively, so that IPM reduces the CPU throttle or power gradually based on the priority list.

The following are the reduction steps available for IPM and ITM:

Reduction Step	Description
cpu_throttle_25	Reduces CPU frequency to 25%
cpu_throttle_50	Reduces CPU frequency to 50%
cpu_throttle_75	Reduces CPU frequency to 75%
disable_alt_eth	Disables 2nd Ethernet port
disable_pse	Disables PSE
disable_usb	Disables USB
radio_2ghz_chain_1x1	Reduces 2 GHz chains to 1x1
radio_2ghz_chain_2x2	Reduces 2 GHz chains to 2x2
radio_2ghz_chain_3x3	Reduces 2 GHz chains to 3x3
radio_2ghz_power_3dB	Reduces 2 GHz radio power by 3dB from maximum
radio_2ghz_power_6dB	Reduces 2 GHz radio power by 6dB from maximum

Reduction Step	Description
radio_5ghz_chain_1x1	Reduces 5 GHz chains to 1x1
radio_5ghz_chain_2x2	Reduces 5 GHz chains to 2x2
radio_5ghz_chain_3x3	Reduces 5 GHz chains to 3x3
radio_5ghz_power_3dB	Reduces 5 GHz radio power by 3dB from maximum
radio_5ghz_power_6dB	Reduces 5 GHz radio power by 6dB from maximum

The following CLI commands configures the priority for reduction steps:

```
(Instant AP) #configure terminal
(Instant AP)(config) # ipm
(Instant AP)(ipm) # ipm-power-reduction-step-prio ipm-step <reduction step> priority
<priority value>
(Instant AP)(ipm) # exit
(Instant AP)(config) # exit
(Instant AP)# commit apply
committing configuration...
```

Transmit Power Calculation Support on 200 Series and 300 Series Access Points

This feature allows calculation of the transmit power of each outgoing 802.11 packet so that Instant AP adheres to the latest regulatory limits. Also, the MIMO gain is considered while calculating the transmit power. MIMO gain refers to effective increase in EIRP of a packet due to usage of multiple antennae (power gain) and various signal processing techniques such as Cyclic Delay Diversity, transmit beamforming, and so on (correlation gain).

Two new action commands, **a-ant-pol** and **g-ant-pol**, are added to configure the antenna polarization for both the radios. The polarization values can be either 0 or 1.

- 0 indicates that the external antennas are co-polarized.
- 1 indicates that the external antennas are cross polarized.

A new show command **show ap debug power-table** is added that displays the following information:

- Power limit table based on regulatory powers, user configured power, and override powers.
- Board limit table.
- A combination of all the above fields to calculate the actual transmit power of the packets.



This feature is supported on 200 Series and 300 Series access points and the command **show ap debug power-table** does not display any value for 100 Series access points.

Hardware Offloading for Increased Transmission Performance

The hardware offloading feature of Instant enhances the transmission performance of access points by offloading certain data forwarding flows from its software to its hardware. Traditionally all packet forwarding on the access point is handled by the datapath in the CPU. With the new hardware

offloading feature, a separate network processor NPU can process dataflows thereby removing the traffic overhead in the CPU. This frees CPU resources and makes it available for newer data flows and other priority operations. When enabled, Bridge traffic (IPv4), Bridge traffic (IPv6) and SNAT traffic (IPv4) will be offloaded to the network processor. This feature can be configured using the CLI, Central or AirWave management platform.



AP-535 and AP-555 support this feature.

Configuring Hardware Offloading

The following CLI command enables hardware offloading:

```
(Instant AP) # config
(Instant AP) (config) # flow-offload
```

The following CLI command disables hardware offloading:

```
(Instant AP) # config
(Instant AP) (config) # no flow-offload
```

The following CLI command is used to view the status of flow offloading:

```
(Instant AP) # show flow-offload status
```

Chapter 9
VLAN Configuration

This chapter explains the following topics:

- VLAN Pooling
- Uplink VLAN Monitoring and Detection on Upstream Devices
- Multiple Management Interface

VLAN configuration is required for networks with more devices and broadcast traffic on a WLAN SSID or wired profile. Based on the network type and its requirements, you can configure the VLANs for a WLAN SSID or wired port profile.

For more information on VLAN configuration for a WLAN SSID and wired port profile, see Configuring VLAN Settings for a WLAN SSID Profile on page 136 and Configuring VLAN for a Wired Profile on page 163, respectively.

VLAN Pooling

In a single Instant AP cluster, a large number of clients can be assigned to the same VLAN. Using the same VLAN for multiple clients can lead to a high level of broadcasts in the same subnet. To manage the broadcast traffic, you can partition the network into different subnets and use L3-mobility between those subnets when clients roam. However, if a large number of clients need to be in the same subnet, you can configure VLAN pooling, in which each client is randomly assigned a VLAN from a pool of VLANs on the same SSID. Thus, VLAN pooling allows automatic partitioning of a single broadcast domain of clients into multiple VLANs.

Uplink VLAN Monitoring and Detection on Upstream Devices

If a client connects to an SSID or a wired interface with VLAN that is not allowed on the upstream device, the client will not be assigned an IP address and thus cannot connect to the Internet. In such a scenario, the WebUI displays an alert. To prevent this issue from recurring, ensure that there is no mismatch in the VLAN configuration.

Multiple Management Interface

Users have an option to create multiple VLAN interfaces on master Instant APs. This option is not supported on slave Instant APs due to the following reasons:

- Only the master can implement NATing.
- VLAN features such as guest VLAN, DRP VLAN, VC VLAN, local DHCP VLAN, and so on are implemented only on the master.



Instant APs can report downlink wired port VLAN port information to Central. Using this information, Central can build a topology view of the user's network.

This chapter includes the following topics:

- IPv6 Notation on page 126
- Enabling IPv6 Support for Instant AP Configuration on page 126
- Firewall Support for IPv6 on page 128
- GRE Backup Tunnel on page 128
- Debugging Commands on page 129

IPv6 Notation

IPv6 is the latest version of IP that is suitable for large-scale IP networks. IPv6 supports a 128-bit address to allow 2^{128}, or approximately 3.4×1038 addresses while IPv4 supports only 2^{32} addresses.

The IP address of the IPv6 host is always represented as eight groups of four hexadecimal digits separated by colons. For example `2001:0db8:0a0b:12f0:0000:0000:0000:0001`. However, the IPv6 notation can be abbreviated to compress one or more groups of zeroes or to compress leading or trailing zeroes.

The following examples show various representations of the address `2001:0db8:0a0b:12f0:0000:0000:0000:0001`

- Valid format—`2001:db8:a0b:12f0::0:0:1`
- Invalid format—`2001:db8:a0b:12f0::::0:1`. The "`::`" sign appears only once in an address.
- With leading zeros omitted—`2001:db8:a0b:12f0:0:0:0:1`
- Switching from upper to lower case—`2001:DB8:A0B:12f0:0:0:0:1`

IPv6 uses a "/" notation which describes the number of bits in netmask as in IPv4.

```
2001:db8::1/128 - Single Host
2001:db8::/64 - Network
```



IPv6 configuration is supported on AP-303P, 303 Series, 318 Series, AP-374, AP-375, AP-377, AP-344, AP-345, AP-203H, AP-203R,AP-303H, AP-365, AP-367, IAP-207, IAP-304, IAP-305, IAP-314, IAP-315, IAP-334, and IAP-335 access points.

Enabling IPv6 Support for Instant AP Configuration

Instant APs support IPv6 address mode for the following features:

- Supported IP modes
- Configuring IPv6 Address for an Instant AP
- RADIUS over IPv6
- SNMP Over IPv6
- SNTP Over IPv6 on page 128

Supported IP modes

Instant supports two modes of IP address configuration:

- V4-only—The Instant AP would allow IPv6 clients to pass-through just like the previous Instant release.
- V4-prefer—Supports both IPv4 and IPv6 addresses. If the Instant AP gets both IPv4 and IPv6 responses for a DNS query, then the Instant AP would prefer the IPv4 DNS address instead of the IPv6 DNS address.

When the IP mode is set to v4-prefer mode, the Instant AP derives a link local IPv6 address and attempts to acquire a routable IPv6 address by monitoring RA packets. Instant AP assigns itself to both SLAAC and DHCPv6 client address. Instant APs also support IPv6 DNS server addresses and use these for DNS resolution.

The following CLI command enables IPv4 mode or dual stack mode:

```
(Instant AP)(config)# ip-mode {v4-only|v4-prefer}
```

Configuring IPv6 Address for an Instant AP

The following procedure describes how to enable the IPv6 mode on the Instant AP and also configure a virtual controller IPv6 address:

Table 39: *Steps to Configure Uplink Management VLAN*

New WebUI	Old WebUI
To enable IPv6 and configure virtual controller IPv6 address: 1. Navigate to the **Configuration** > **System** page. 2. Under **General**, toggle the **Allow IPv6 Management** switch to enable. 3. Enter the IPv6 address in the **Virtual Controller IPv6** address text box. 4. Click **Save**.	To enable IPv6 and configure virtual controller IPv6 address: 1. Select the **System** option from the top right corner of the page. 2. Under **General**, select the **Allow IPv6 Management** check box. 3. Enter the IP address in the **Virtual Controller IPv6** address text box. 4. Click **OK**.

The following CLI command configures an IPv6 address for an Instant AP:

```
(Instant AP)(config)# virtual-controller-ipv6 <ipv6 address>
```



The virtual controller IPv6 address can be configured only after enabling the v4-prefer mode in the Instant CLI.

RADIUS over IPv6

With the address mode set to v4-prefer, the Instant AP supports an IPv6 IP address for the RADIUS server. The authentication server configuration can also include the NAS IPv6 address (that defaults to the routable IPv6 address when not configured). RADIUS server supports hostname configuration using IP or FQDN configurations also.

The following CLI command configures an IPv6 address for the RADIUS server:

```
(Instant AP)(config)# wlan auth-server radiusIPv6
(Instant AP)(Auth Server "radiusIPv6")# ip <host>
(Instant AP)(Auth Server "radiusIPv6")# nas-ip <ip_ipv6>
```

SNMP Over IPv6

In this release, you can configure a community string to authenticate messages sent between the virtual controller and the SNMP agent, where the IPv6 address will be used as the virtual controller address.For more information on configuring SNMP parameters, see Configuring SNMP on page 507.

The following CLI command is used to view the SNMP configuration:

```
(Instant AP)# show running-config|include snmp
snmp-server community e96a5ff136b5f481b6b55af75d7735c16ee1f61ba082d7ee
snmp-server host 2001:470:20::121 version 2c aruba-string inform
```

SNTP Over IPv6

The following CLI command is used to view the SNTP configuration:

```
(Instant AP)# show running-config|include ntp
ntp-server 2001:470:20::121
```



This feature is supported only on global IPv6 addresses. It is not supported on link local IPv6 addresses.

Firewall Support for IPv6

For a given client, a single ACL is used to firewall both IPv4 and IPv6 rules. A rule **any any match any any any permit** in the access rule configuration will expand to two different ACL entries:

- any any any P6
- any any any P4

Similarly, if any IPv6 specific rule is added. For example, if any DHCPv6 or FTPv6 rule is added, the ACE would be expanded as follows:

any 2002::/64 17 0-65535 546-547 6—*destined to network 2002::/64 DHCPv6 is denied*.

any 2001::10/128 6 0-65535 20-21 6—*destined to host 2001::10 FTP is denied*.

For all ACLs the Instant AP will have an implicit IPv4 and IPv6 **allow all** acl rule.

GRE Backup Tunnel

Instant supports configuring a GRE tunnel over IPv6 between an Instant AP and a GRE terminating device such as a wireless access gateway or a controller. Starting from Aruba Instant 8.4.0.0, every Instant AP in a cluster is able to establish a GRE tunnel over IPv6. Each Instant AP can support a primary tunnel and a backup tunnel configuration. However, only one of these tunnels can be active at any given time under manual GRE configuration. This feature also introduces GRE tunnel failover, wherein if the primary GRE tunnel is not reachable, the Instant APs will automatically failover to the backup GRE tunnel. The Instant AP uses icmp pings to detect reachability of the primary and backup tunnel endpoints. At any point of time, only one GRE tunnel can stay active.



If a controller is used as the GRE tunnel endpoint, you must manually configure the GRE tunnel in the controller while using manual GRE in the Instant AP.

Configuring GRE Backup Tunnel Parameters

The following CLI command configures a primary GRE tunnel endpoint:

```
(Instant AP)(config)# gre primary <name>
```

The following CLI command configures a backup GRE tunnel endpoint:

```
(Instant AP)(config)# gre backup <name>
```

The following CLI command removes the backup or primary GRE tunnel configuration

```
(Instant AP)(config)# no gre backup | no gre primary
```

The following CLI command removes the entire GRE configuration:

```
(Instant AP)(config)# no gre backup
(Instant AP)(config)# no gre primary
```

The following CLI command prevents the SSID from being disabled during a GRE tunnel failover or recovery:

```
(Instant AP)(config)# gre disable-reconnect-user-on-failover
```

The following CLI command configures the timer after which the SSIDs should come up once the tunnel status is UP:

```
(Instant AP)(config)# gre reconnect-time-on-failover <Time in secs>
```

The following CLI command configures the number of ping packets to be missed to mark the tunnel status as DOWN:

```
(Instant AP)(config)# gre ping-retry-count <new_count>
```

The following CLI command configures the time interval at which a ping probe packet needs to be sent:

```
(Instant AP)(config)# gre ping-frequency <time_in_secs>
```

The following CLI command disables the hold on timer from running on the Instant AP:

```
(Instant AP)(config)# gre disable-preemption
```

The following CLI command configures the hold down time interval before tunnel recovery from backup to primary:

```
(Instant AP)(config)# gre hold-time <time_in_secs>
```

Verifying the Configuration

The following CLI command is used to view the various parameters configured for the GRE tunnel on the Instant AP:

```
(Instant AP)# show gre config
```

The following CLI command displays the various parameters that indicate the status of the GRE tunnel:

```
(Instant AP)# show gre status
```

Debugging Commands

The following CLI commands are used to troubleshoot issues pertaining to IPv6 configuration:

- `show ipv6 interface brief` and `show ipv6 interface details`— displays the configured IPv6 address, and any duplicate addresses.
- `show ipv6 route`—displays the IPv6 routing information.
- `show datapath ipv6 session`—displays IPv6 sessions.
- `show datapath ipv6 user`—displays IPv6 client details.
- `show clients` and `show clients debug`—displays the details about Instant AP clients.

Chapter 11
Wireless Network Profiles

A wireless (Wi-Fi) network profile contains the SSID (network name), password key, and security information to be able to connect to a wireless network. During start up, a wireless client searches for radio signals or beacon frames that originate from the nearest Instant AP. After locating the Instant AP, the following transactions take place between the client and the Instant AP:

- Authentication—The Instant AP communicates with a RADIUS server to validate or authenticate the client.
- Wi-Fi Connection—After successful authentication, the client establishes a Wi-Fi connection with the Instant AP.

This chapter provides the following information:

- Configuring Wireless Network Profiles on page 130
- Fast Roaming for Wireless Clients on page 148
- Configuring Modulation Rates on a WLAN SSID on page 153
- Disabling Short Preamble for Wireless Client on page 156
- Multi-User-MIMO on page 153
- Management Frame Protection on page 154
- High Efficiency WLAN (HEW) on page 154
- Multi Band Operation (MBO) on page 155
- Disabling a WLAN SSID Profile on page 156
- Editing a WLAN SSID Profile on page 157
- Deleting a WLAN SSID Profile on page 157
- Wireless Client Bridge on page 159

Configuring Wireless Network Profiles

Instant wireless networks are categorized as:

- **Employee network**—An Employee network is a classic Wi-Fi network. This network type is used by the employees in an organization and it supports passphrase-based or 802.1X-based authentication methods. Employees can access the protected data of an enterprise through the employee network after successful authentication. The employee network is selected by default during a network profile configuration.
- **Voice network**—This Voice network type allows you to configure a network profile for devices that provide only voice services—for example, devices such as handsets or applications that require voice traffic prioritization.
- **Guest network**—The Guest wireless network is created for guests, visitors, contractors, and any non-employee users who use the enterprise Wi-Fi network. The virtual controller assigns the IP address for the guest clients. Captive portal or passphrase-based authentication methods can be set for this wireless network. Typically, a guest network is an unencrypted network. However, you can specify the encryption settings when configuring a guest network.

When a client is associated to the Voice network, all data traffic is marked and placed into the high-priority queue in the QoS.

Workflow to Configure a WLAN SSID Profile

To configure a new wireless network profile, complete the following procedures:

- Step 1: Configuring WLAN Settings
- Step 2: Configuring VLAN Settings
- Step 3: Configuring Security Settings
- Step 4: Configuring Access Rules for a Network

Configuring WLAN Settings for an SSID Profile

The following procedure configures WLAN settings for an SSID profile using the WebUI or the CLI.

Table 40: *Configuring WLAN Settings*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **Networks** page. 2. Under **Networks**, click **+**. The **Create a new network** window is displayed. 3. Under **Basic** option, Enter a name that uniquely identifies a wireless network in the **Name** field. **NOTE:** The SSID name must be unique and may contain any special character except for **'** and **".** 4. In the **Type** drop-down list, select **Wireless.** 5. Based on the type of network profile, select any of the following options under **Primary usage**: ▪ **Employee** ▪ **Voice** ▪ **Guest** 6. Click the **Show advanced options** link at the bottom of the page.	1. Under the **Networks** tab of the Instant main window, select **New**. The **New WLAN** window is displayed. 2. Enter a name that uniquely identifies a wireless network in the **Name** field. **NOTE:** The SSID name must be unique and may contain any special character except for **'** and **".** 3. Based on the type of network profile, select any of the following options under **Primary usage**: ▪ **Employee** ▪ **Voice** ▪ **Guest** 4. Click the **Show advanced options** link at the bottom of the window. The advanced options for configuration are displayed.

Once the initial setup is complete, configure the following parameters to create your WLAN profile as required:

Table 41: *WLAN Configuration Parameters*

Parameter	Description
Broadcast/Multicast	
Broadcast filtering	Select any of the following values: ▪ **All**—When set to **All**, the Instant AP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. ▪ **ARP**—When set to **ARP**, the Instant AP drops all broadcast and multicast frames

Table 41: *WLAN Configuration Parameters*

Parameter	Description
	except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols; additionally, it converts ARP requests to unicast and send frames directly to the associated client. The broadcast filtering option is set to **ARP** by default when an SSID profile is created. ▪ **Unicast-ARP-Only**—When set to **Unicast-ARP-Only**, the Instant AP allows all broadcast and multicast frames as it is, however the ARP requests are converted to unicast frames and sends them to the associated clients. ▪ **Disabled**—When set to **Disabled**, all broadcast and multicast traffic is forwarded to the wireless interfaces.
Multicast transmission optimization	Click the toggle switch if you want the Instant AP to select the optimal rate for sending 802.11 broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When this parameter is enabled, multicast traffic can be sent at up to 24 Mbps. The default rate of sending frames for 2.4 GHz is 1 Mbps and that for 5 GHz is 6 Mbps. This parameter is disabled by default.
Dynamic multicast optimization	Click the toggle switch to allow the Instant AP to convert multicast streams into unicast streams over the wireless link. Enabling DMO enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. **NOTE:** When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.
DMO channel utilization threshold	Specify a value to set a threshold for DMO channel utilization. With DMO, the Instant AP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90% and the maximum threshold value is 100%. When the threshold is reached or exceeds the maximum value, the Instant AP sends multicast traffic over the wireless link.
Transmit Rates	
Transmit Rates	Specify the following parameters: ▪ **2.4 GHz**—If the 2.4 GHz band is configured on the Instant AP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps. ▪ **5 GHz**—If the 5 GHz band is configured on the Instant AP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps.
802.11	
Band	Select a value to specify the band at which the network transmits radio signals. You can set the band to **2.4 GHz**, **5 GHz**, or **All**. The **All** option is selected by default.
DTIM interval	The **DTIM interval** indicates the DTIM period in beacons, which can be configured for every WLAN SSID profile. The DTIM interval determines how often the Instant AP should deliver the buffered broadcast and multicast frames to associated clients in the powersave mode. The default value is 1 beacon, which means the client checks for buffered data on the Instant AP at every beacon. You can also configure a higher DTIM value for power saving.

Table 41: *WLAN Configuration Parameters*

Parameter	Description
Min RSSI for probe request	Sets a minimum RSSI threshold for probe requests.
Min RSSI for auth request	Sets a minimum RSSI threshold for authentication requests.
High Throughput	Disables/ Enables 802.11n high throughput functionality. Disabling **High Throughput** automatically disables **Very High Throughput** and **High Efficiency** modes. High throughput settings are applied only to the respective SSID. Disable **High Throughput** on the SSID to service 802.11a and 802.11g only legacy clients. Enabled by default.
Very high throughput	Enables the VHT function on Instant AP devices that support VHT. For 802.11ac Instant APs, the VHT function is enabled by default. However, you can disable the VHT function if you want the 802.11ac Instant APs to function as 802.11n Instant APs. If VHT is configured or disabled on an SSID, the changes will apply only to the SSID on which it is enabled or disabled.
High efficiency	Defines 802.11ax spectrum efficiency and area throughput on both the 2.4 GHz and 5 GHz frequency bands.
Zone	Specify the zone name for the SSID profile. When the zone is defined in SSID profile and if the same zone is defined on an Instant AP, the SSID is created on that Instant AP. Enter multiple zone name as comma-separated values. For more information on configuring zone details, see Configuring Zone Settings on an Instant AP on page 84.
Time Range	Click **Edit**, select a Time Range Profile from the list, and specify if the profile must be enabled or disabled for the SSID, and then click **OK**.
Bandwidth Limits	Select the required options under **Bandwidth Limits**: ▪ **Airtime**—Click the toggle switch and specify an aggregate amount of airtime that all clients in this network can use for sending and receiving data. Specify the airtime percentage. ▪ **Each radio**—Click the toggle switch to specify an aggregate amount of throughput that each radio is allowed to provide for the connected clients. ▪ **Downstream** and **Upstream**—Specify the downstream and upstream rates within a range of 1 to 65,535 Kbps for the SSID users. If the assignment is specific for each user, select the **Per user** check box. **NOTE:** The bandwidth limit set in this method is implemented at a per-AP level and not cluster level.
WMM	Configure the following options for WMM traffic management. WMM supports voice, video, best effort, and background access categories. To allocate bandwidth for the following types of traffic, specify a percentage value under **Share**. To configure DSCP mapping, specify a value under **DSCP Mapping**. ▪ **Background WMM**—For background traffic such as file downloads or print jobs. ▪ **Best effort WMM**—For best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS. ▪ **Video WMM**—For video traffic generated from video streaming.

Table 41: *WLAN Configuration Parameters*

Parameter	Description
	▪ **Voice WMM**—For voice traffic generated from the incoming and outgoing voice communication. **NOTE:** The WMM traffic management feature is not supported on AP-203H, AP-203R, AP-203RP, AP-207, 200 Series, 340 Series, 500 Series, and 510 Series access points. For more information on WMM traffic and DSCP mapping, see WMM Traffic Management on page 391.
	For voice traffic and Spectralink Voice Prioritization, configure the following parameters: ▪ **Traffic Specification (TSPEC)**—To prioritize time-sensitive traffic such as voice traffic initiated by the client, click the **Traffic Specification (TSPEC)** toggle switch. ▪ **TSPEC Bandwidth**—To reserve bandwidth, set the TPSEC bandwidth to the desired value within the range of 200–600,000 Kbps. The default value is 2000 Kbps. ▪ **Spectralink Voice Protocol (SVP)**—Click the toggle switch to prioritize voice traffic for SVP handsets.
Miscellaneous	
Content filtering	Click the toggle switch to route all DNS requests for the non-corporate domains on this network.
Inactivity timeout	Specify an interval for session timeout in seconds, minutes, or hours. If a client session is inactive for the specified duration, the session expires and the user is required to log in again. You can specify a value within the range of 60–86,400 seconds (24 hours) for a client session. The default value is 1000 seconds.
Deauth inactive clients	Click the toggle switch to allow the Instant AP to send a deauthentication frame to the inactive client and clear client entry.
SSID	Select the **Hide** check box if you do not want the SSID (network name) to be visible to users. Select the **Disable** check box if you want to disable the SSID. On selecting this, the SSID will be disabled, but will not be removed from the network. By default, all SSIDs are enabled.
Out of service (OOS)	Configures the SSID state when a connection link of the AP is down. To configure out of service for an SSID, the link condition of the AP and the SSID state should be configured. The SSID can be enabled or disabled automatically when the following conditions are met: ▪ **VPN down** - Connection to the VPN network is down. ▪ **Uplink down** - The uplink connection of the AP is down. ▪ **Internet down** - The connection to the Internet is down. ▪ **Primary uplink down** - The primary uplink connection of the AP is down. The SSID status will change according to the configuration when the link condition is met. For example, when **Internet down**, **Disabled** is set for **Out of Service**, the SSID will be disabled when the Internet connection is down and change back to enabled when the Internet connection is restored. **NOTE:** When **Internet Down** condition is set in the SSID, the Instant AP will check for

Table 41: *WLAN Configuration Parameters*

Parameter	Description
	uplink by pinging the IP defined in the Internet Failover IP. To configure the Internet Failover IP, seeUplink Preferences and Switching.
OOS time (global)	Configures the hold time interval in seconds within a range of 30–300 seconds, after which the out-of-service operation is triggered. For example, if the VPN is down and the configured hold time is 45 seconds, the effect of this out-of-service state impacts the SSID availability after 45 seconds.
Max clients threshold	Specify the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value within the range of 0–255. The default value is 64. **NOTE:** When the **Max clients threshold** parameter is configured, the value is applicable to every Instant AP in a cluster.
SSID Encoding	To encode the SSID, select UTF-8. By default, the SSIDs are not encoded. **NOTE:** When a wireless SSID is encoded, by default, UTF-8 is added to the access rules that are active on the SSID. However this does not apply for the access rules that are configured separately for the SSID. UTF-8 is not supported for wired networks.
ESSID	Name that uniquely identifies a wireless network. The network name, or ESSID can be up to 32 ASCII characters, if it contains Unicode, depending on the language, the maximum characters vary. For example, ESSID could be up to 10 Chinese characters or 16 extended ASCII characters. If the ESSID includes spaces, you must enclose it in quotation marks.
Deny inter user bridging	When enabled, the bridging traffic between two clients that are connected to the same SSID on the same VLAN is disabled. The clients can connect to the Internet, but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision.
Openflow	When enabled, users can run and manage multiple instances of the control-plane and dataplane from a centralized location. OpenFlow also ensures uniform policy enforcement.
Max IPv4 users	Allows you to configure the maximum number of IPv4 users for wireless client bridging. The default value is 2 and the maximum threshold value is 32 users.

Click **Next** to configure VLAN settings. For more information, see Configuring VLAN Settings for a WLAN SSID Profile on page 136.

The following CLI commands configure WLAN settings for an SSID profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# essid <ESSID-name>
(Instant AP)(SSID Profile <name>)# type {<Employee>|<Voice>|<Guest>}
(Instant AP)(SSID Profile <name>)# broadcast-filter {All|ARP|Unicast-ARP-
Only|Disabled}
(Instant AP)(SSID Profile <name>)# dtim-period <number-of-beacons>
(Instant AP)(SSID Profile <name>)# multicast-rate-optimization
(Instant AP)(SSID Profile <name>)# dynamic-multicast-optimization
(Instant AP)(SSID Profile <name>)# dmo-channel-utilization-threshold
(Instant AP)(SSID Profile <name>)# a-max-tx-rate <rate>
(Instant AP)(SSID Profile <name>)# a-min-tx-rate <rate>
(Instant AP)(SSID Profile <name>)# g-max-tx-rate <rate>
(Instant AP)(SSID Profile <name>)# g-min-tx-rate <rate>
```

```
(Instant AP)(SSID Profile <name>)# zone <zone>
(Instant AP)(SSID Profile <name>)# bandwidth-limit <limit>
(Instant AP)(SSID Profile <name>)# per-user-bandwidth-limit <limit>
(Instant AP)(SSID Profile <name>)# air-time-limit <limit>
(Instant AP)(SSID Profile <name>)# wmm-background-dscp <dscp>
(Instant AP)(SSID Profile <name>)# wmm-background-share <share>
(Instant AP)(SSID Profile <name>)# wmm-best-effort-dscp <dscp>
(Instant AP)(SSID Profile <name>)# wmm-best-effort-share <share>
(Instant AP)(SSID Profile <name>)# wmm-video-dscp <dscp>
(Instant AP)(SSID Profile <name>)# wmm-video-share <share>
(Instant AP)(SSID Profile <name>)# wmm-voice-dscp <dscp>
(Instant AP)(SSID Profile <name>)# wmm-voice-share <share>
(Instant AP)(SSID Profile <name>)# rf-band {<2.4>|<5>|<all>}
(Instant AP)(SSID Profile <name>)# content-filtering
(Instant AP)(SSID Profile <name>)# mfp-capable
(Instant AP)(SSID Profile <name>)# mfp-required
(Instant AP)(SSID Profile <name>)# hide-ssid
(Instant AP)(SSID Profile <name>)# out-of-service <def> <name>
(Instant AP)(SSID Profile <name>)# time-range <profile name> {<Enable>|<Disable>}
(Instant AP)(SSID Profile <name>)# inactivity-timeout <interval>
(Instant AP)(SSID Profile <name>)# work-without-uplink
(Instant AP)(SSID Profile <name>)# local-probe-req-thresh <threshold>
(Instant AP)(SSID Profile <name>)# max-clients-threshold <number-of-clients>
(Instant AP)(SSID Profile <name>)# max-ipv4-users <threshold>
```

Temporal Diversity and Maximum Retries

When clients are not responding to 802.11 packets with the **temporal-diversity** parameter disabled, which is the default setting, Instant APs can attempt only hardware retries. But if this parameter is enabled when the clients are not responding to 802.11 packets, Instant APs can perform two hardware retries. When the hardware retry attempts fail, Instant APs can perform software retries.

The **max-retries** parameter indicates the maximum number of attempts the Instant AP performs when clients are not responding to 802.11 packets. By default, the Instant AP attempts a maximum of eight retries when clients are not responding to 802.11 packets.

The following example shows the configuration of **temporal-diversity** and **max-retries** in a WLAN SSID profile:

```
(Instant AP) (config) # wlan ssid-profile Name
(Instant AP) (SSID Profile "Name") # temporal-diversity
(Instant AP) (SSID Profile "Name") # max-retries 3
```

Configuring VLAN Settings for a WLAN SSID Profile

If you are creating a new SSID profile, complete the WLAN Settings procedure before configuring the VLAN. For more information, see Configuring WLAN Settings for an SSID Profile on page 131.

You can configure VLAN settings for an SSID profile using the Instant WebUI or the CLI.

Table 42: *Configuring VLAN Settings*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Networks**. 2. In the **Networks** page, select the network you want to configure and click **edit**. 3. Under the **VLAN** tab, select any of the following options for **Client IP assignment**: ▪ **Virtual Controller managed**—On selecting this option, the wired client	1. In the **Networks** tab, select the network you want to edit and click **edit**. 2. Select the **VLAN** tab. 3. Select any one for the following options for **Client IP assignment**: ▪ **Virtual Controller managed**—On selecting this option, the wired client

New WebUI	Old WebUI
obtains the IP address from the virtual controller. When this option is used, the source IP address is translated to the physical IP address of the master Instant AP for all client traffic that goes through this interface. The virtual controller can also assign a guest VLAN to the client. ▪ **Network assigned**—On selecting this option, the IP address is obtained from the network.	obtains the IP address from the virtual controller. When this option is used, the source IP address is translated to the physical IP address of the master Instant AP for all client traffic that goes through this interface. The virtual controller can also assign a guest VLAN to the client. ▪ **Network assigned**—On selecting this option, the IP address is obtained from the network.

Based on the type of client IP assignment mode selected, you can configure the VLAN assignment for clients as described in the following table:

Table 43: *IP and VLAN Assignment for WLAN SSID Clients*

Client IP Assignment	Client VLAN Assignment
Virtual Controller managed	If **Virtual Controller managed** is selected for client IP assignment, the virtual controller creates a private subnet and VLAN on the Instant AP for the wireless clients. The NAT for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multisite wireless network. On selecting this option, the following client VLAN assignment options are displayed: ▪ **Default**—When selected, the default VLAN as determined by the virtual controller is assigned for clients. ▪ **Custom**—When selected, you can specify a custom VLAN assignment option. You can select an existing DHCP scope for client IP and VLAN assignment . For more information on DHCP scopes, see Configuring DHCP Scopes on page 294.
Network assigned	If **Network assigned** is selected, you can specify any of the following options for the **Client VLAN assignment**. ▪ **Default**—On selecting this option, the client obtains the IP address in the same subnet as the Instant APs. By default, the client VLAN is assigned to the native VLAN on the wired network. ▪ **Static**—On selecting this option, you need to specify any one of the following in the **VLAN ID** text box: a single VLAN, a comma separated list of VLANS, or a range of VLANs for all clients on this network. Select this option for configuring VLAN pooling. ▪ **Dynamic**—On selecting this option, you can assign the VLANs dynamically from a DHCP server. To create VLAN assignment rules, click **+** to assign the user to a VLAN. In the **New VLAN Assignment Rules** window, enter the following information: • **Attribute**—Select an attribute returned by the RADIUS server during authentication. • **Operator**—Select an operator for matching the string. • **String**—Enter the string to match . • **VLAN**—Enter the VLAN to be assigned.

Click **Next** to configure security settings for the network. For more information, see Points to Remember on page 145.

The following CLI command assigns a VLAN ID for the WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# vlan <vlan-ID>
```

The following CLI command configures a new VLAN assignment rule:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-vlan <attribute> {{contains|ends-
with|equals|matches-regular-expression|not-equals|starts-with} <operand> <vlan>|value-
of}
```

Enforcing DHCP

Instant allows you to configure a WLAN SSID profile to enforce DHCP on Instant AP clients.

When DHCP is enforced:

- A layer-2 user entry is created when a client associates with an Instant AP.
- The client DHCP state and IP address are tracked.
- When the client obtains an IP address from DHCP, the DHCP state changes to complete.
- If the DHCP state is complete, a layer-3 user entry is created.
- When a client roams between the Instant APs, the DHCP state and the client IP address will be synchronized with the new Instant AP.

By default, enforcing DHCP feature is disabled.

The following command is used to enforce DHCP on a WLAN SSID profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# enforce-dhcp
```

Configuring Security Settings for a WLAN SSID Profile

The following procedure describes how to configure security settings for an Employee or Voice network. If you are creating a new SSID profile, configure the WLAN and VLAN settings before defining security settings. For more information, see Configuring WLAN Settings for an SSID Profile on page 131 and Configuring VLAN Settings for a WLAN SSID Profile on page 136.

Table 44: *Configuring Security Settings*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Networks** page 2. Under **Networks** select the network you want to configure and click **Edit**. 3. Under **Security** specify any of the following types of security levels by moving the slider to a desired level: a. **Enterprise**—On selecting the enterprise security level, the authentication options applicable to the enterprise network are displayed. b. **Personal**—On selecting the personal security level, the authentication options applicable to	1. In the **Networks** tab, select the network you want to edit and click **edit**. 2. Select the **Security** tab. 3. Specify any of the following types of security levels by moving the slider to a desired level: a. **Enterprise**—On selecting the enterprise security level, the authentication options applicable to the enterprise network are displayed. b. **Personal**—On selecting the personal security level, the authentication options applicable to the personalized network are displayed.

New WebUI	Old WebUI
the personalized network are displayed. c. **Open**—On selecting the open security level, the authentication options applicable to an open network are displayed.	c. **Open**—On selecting the open security level, the authentication options applicable to an open network are displayed.

Based on the security level selected, specify the following parameters.

Table 45: *Configuration Parameters for WLAN Security Settings in an Employee or Voice Network*

Parameter	Description	Security Level
Key Management	Click the **Enterprise** security level, select any of the following options from the **Key management** drop-down list: ■ WPA3-Enterprise (CCM 128) ■ WPA3-Enterprise (CCM 256) ■ WPA3-Enterprise (CSNA) ■ WPA2 Enterprise ■ WPA Enterprise ■ Both (WPA2 & WPA) ■ Dynamic WEP with 802.1X—If you do not want to use a session key from the RADIUS server to derive pairwise unicast keys, set **Session Key for LEAP** to **Enabled**. This is required for old printers that use dynamic WEP through LEAP authentication. The **Session Key for LEAP** feature is set to **Disabled** by default.	Applicable to **Enterprise** and **Personal** security levels only. For the **Open** security level, no encryption settings are required.
	For the **Personal** security level, select any of the following encryption keys from the **Key management** drop-down list. ■ WPA3 Personal ■ WPA2 Personal ■ WPA Personal (Both TKIP and AES Encryption) ■ WPA Personal (TKIP Encryption only) ■ WPA Personal (AES Encryption only) ■ Both (WPA2 & WPA) ■ Static WEP If a WPA2, WPA encryption, or Both (WPA2 & WPA) is selected, configure the passphrase: 1. Select a passphrase format from the **Passphrase format** drop-down list. The options available are 8–63 alphanumeric characters and 64 hexadecimal characters. 2. Enter a passphrase in the **Passphrase** text box. To reconfirm, update the passphrase in the **Retype** text box. **NOTE:** The **Passphrase** may contain any special character except for **".** For **Static WEP**, specify the following parameters: 1. Select an appropriate value for **WEP key size** from the WEP key size drop-down list. You can specify 64-bit or 128-bit .	

Table 45: *Configuration Parameters for WLAN Security Settings in an Employee or Voice Network*

Parameter	Description	Security Level
	2. Select an appropriate value for Tx key from the **Tx Key** drop-down list. You can specify **1**, **2**, **3**, or **4**. 3. Enter an appropriate **WEP key** and reconfirm.	
EAP Offload	To terminate the EAP portion of 802.1X authentication on the Instant AP instead of the RADIUS server, click the **EAP Offload** toggle switch. Enabling termination can reduce network traffic to the external RADIUS server by terminating the authorization protocol on the Instant AP. By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS server, and the Instant AP acts as a relay for this exchange. When **EAP Offload** is enabled, the Instant AP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server. It can also reduce the number of exchange packets between the Instant AP and the authentication server. **NOTE:** ▪ Instant supports the configuration of primary and backup authentication servers in an EAP termination-enabled SSID. ▪ If you are using LDAP for authentication, ensure that Instant AP termination is configured to support EAP.	**Enterprise** security level
Authentication server 1 and Authentication server 2	Select any of the following options from the **Authentication server 1** drop-down list: ▪ Select an authentication server from the list if an external server is already configured. To modify the server parameters, click the **edit** icon. ▪ Select **+** to add a new server. For information on configuring external servers, see External RADIUS Server on page 231. ▪ To use an internal server, select **InternalServer** and add the clients that are required to authenticate with the internal RADIUS server. If an external server is selected, you can also configure another authentication server.	**Enterprise**, **Personal**, and **Open** security levels.
Load balancing	Click the toggle switch if you are using two RADIUS authentication servers, so that the load across the two RADIUS servers is balanced. For more information on the dynamic load balancing mechanism, see Dynamic Load Balancing between Two Authentication Servers on page 230.	**Enterprise**, **Personal**, and **Open** security levels.
Reauth interval	Specify a value for **Reauth interval**. When set to a value greater than zero, Instant APs periodically reauthenticate all associated and authenticated clients. The following list provides descriptions for three reauthentication interval configuration scenarios: ▪ When Reauth interval is configured on an SSID performing L2 authentication (MAC or 802.1X authentication)—When reauthentication fails, the clients are disconnected. If the SSID is	**Enterprise**, **Personal**, and **Open** security levels.

Table 45: *Configuration Parameters for WLAN Security Settings in an Employee or Voice Network*

Parameter	Description	Security Level
	performing only MAC authentication and has a pre-authentication role assigned to the client, the client will get a post-authentication role only after a successful reauthentication. If reauthentication fails, the client retains the pre-authentication role. ▪ When Reauth interval is configured on an SSID performing both L2 and L3 authentication (MAC with captive portal authentication)—When reauthentication succeeds, the client retains the role that is already assigned. If reauthentication fails, a pre-authentication role is assigned to the client. ▪ When Reauth interval is configured on an SSID performing only L3 authentication (captive portal authentication)—When reauthentication succeeds, a pre-authentication role is assigned to the client that is in a post-authentication role. Due to this, the clients are required to go through captive portal to regain access.	
Blacklisting	To enable blacklisting of the clients with a specific number of authentication failures, Click the **Blacklisting** toggle switch and specify a value for **Max authentication failures**. The users who fail to authenticate the number of times specified in **Max authentication failures** are dynamically blacklisted.	**Enterprise**, **Personal**, and **Open** security levels.
Accounting	Select any of the following options: ▪ To enable accounting, select **Use authentication servers** from the **Accounting** drop-down list. On enabling the accounting function, Instant APs post accounting information to the RADIUS server at the specified **Accounting interval**. ▪ To use a separate server for accounting, select **Use separate servers**. The accounting server is distinguished from the authentication server specified for the SSID profile. ▪ To disable the accounting function, select **Disabled**.	**Enterprise**, **Personal**, and **Open** security levels.
Authentication survivability	To enable authentication survivability, click the **Authentication survivability** toggle switch. Specify a value in hours for **Cache timeout (global)** to set the duration after which the authenticated credentials in the cache must expire. When the cache expires, the clients are required to authenticate again. You can specify a value within a range of 1–99 hours and the default value is 24 hours. **NOTE:** The authentication survivability feature requires ClearPass Policy Manager 6.0.2 or later, and is available only when the **New** server option is selected. On setting this parameter to **Enabled**, Instant authenticates the previously connected clients using EAP-PEAP authentication even when connectivity to ClearPass Policy Manager is temporarily lost. The Authentication survivability feature is not applicable when a RADIUS server is configured as an internal server.	**Open, Personal (MPSK-AES)** and **Enterprise** security levels.
MAC authentication	To enable MAC-address-based authentication for **Personal** and **Open** security levels, enable the **MAC authentication** toggle switch. For **Enterprise** security level, the following options are available:	**Enterprise**, **Personal**, and **Open** security levels.

Table 45: *Configuration Parameters for WLAN Security Settings in an Employee or Voice Network*

Parameter	Description	Security Level
	▪ **Perform MAC authentication before 802.1X**—Select this check box to use 802.1X authentication only when the MAC authentication is successful. ▪ **MAC authentication fail-thru**—On selecting this check box, the 802.1X authentication is attempted when the MAC authentication fails. **NOTE:** If Enterprise Security level is chosen, the server used for mac authentication will be the same as the server, defined for 802.1x authentication. You will not be able to use the Instant APs internal database for mac authentication and external RADIUS server for 802.1x authentication on the same SSID.	
Delimiter character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the Instant AP will use the delimiter in the MAC authentication request. For example, if you specify colon as the delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. **NOTE:** This option is available only when MAC authentication is enabled.	**Enterprise**, **Personal**, and **Open** security levels.
Uppercase support	Click the toggle switch to allow the Instant AP to use uppercase letters in MAC address string for MAC authentication. **NOTE:** This parameter is available only when MAC authentication is enabled.	**Enterprise**, **Personal**, and **Open** security levels.
Upload Certificate	Click **Upload Certificate** and browse to upload a certificate file for the internal server. For more information on certificates, see Authentication Certificates on page 254.	**Enterprise**, **Personal**, and **Open** security levels
Fast Roaming	You can configure the following fast roaming options for the WLAN SSID: ▪ **Opportunistic Key Caching**: You can enable **Opportunistic Key Caching (OKC)** when **WPA2 Enterprise** and **Both (WPA2 & WPA)** encryption types are selected. If OKC is enabled, a cached PMK is used when the client roams to a new Instant AP. This allows faster roaming of clients without the need for a complete 802.1X authentication. ▪ **802.11r**: Selecting this check box enables fast BSS transition. The Fast BSS Transition mechanism minimizes the delay when a client transitions from one BSS to another within the same cluster. This option is available only when WPA2 Enterprise and WPA2 personal encryption keys are selected. ▪ **802.11k**: Selecting this check box enables 802.11k roaming on the SSID profile. The 802.11k protocol enables Instant APs and clients to	**Enterprise**, **Personal**, and **Open** security levels.

Table 45: *Configuration Parameters for WLAN Security Settings in an Employee or Voice Network*

Parameter	Description	Security Level
	dynamically measure the available radio resources. When 802.11k is enabled, Instant APs and clients send neighbor reports, beacon reports, and link measurement reports to each other. ▪ **802.11v**: Selecting this check box enables the 802.11v-based BSS transition. 802.11v standard defines mechanisms for wireless network management enhancements and BSS transition management. It allows client devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables an Instant AP to request a voice client to transition to a specific Instant AP, or suggest a set of preferred Instant APs to a voice client, due to network load balancing or BSS termination. It also helps the voice client identify the best Instant AP to transition to as they roam.	

Click **Next** to configure access rules. For more information, see Configuring Access Rules for a WLAN SSID Profile on page 146.

The following commands configure enterprise security settings for the Employee and Voice network SSID profiles:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# opmode {wpa2-aes|wpa2-psk-aes|wpa-tkip|wpa-psk-
tkip|wpa-tkip,wpa2-aes|wpa-psk-tkip,wpa2-psk-aes|static-wep|dynamic-wep|mpsk-aes|wpa3-
sae-aes|wpa3-aes-ccm-128|wpa3-cnsa|wpa3-aes-gcm-256}}
(Instant AP)(SSID Profile <name>)# leap-use-session-key
(Instant AP)(SSID Profile <name>)# termination
(Instant AP)(SSID Profile <name>)# auth-server <server-name>
(Instant AP)(SSID Profile <name>)# external-server
(Instant AP)(SSID Profile <name>)# server-load-balancing
(Instant AP)(SSID Profile <name>)# blacklist
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# l2-auth-failthrough
(Instant AP)(SSID Profile <name>)# auth-survivability
(Instant AP)(SSID Profile <name>)# radius-accounting
(Instant AP)(SSID Profile <name>)# radius-accounting-mode {user-association|user-
authentication}
(Instant AP)(SSID Profile <name>)# radius-interim-accounting-interval <minutes>
(Instant AP)(SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant AP)(SSID Profile <name>)# max-authentication-failures <number>
(Instant AP)(SSID Profile <name>)# okc
(Instant AP)(SSID Profile <name>)# dot11r
(Instant AP)(SSID Profile <name>)# dot11k
(Instant AP)(SSID Profile <name>)# dot11v
(Instant AP)(SSID Profile <name>)# exit
(Instant AP)(config)# auth-survivability cache-time-out
```

To configure personal security settings for the Employee and Voice users:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# opmode {enhanced-open|wpa2-psk-aes|wpa-tkip|wpa-
psk-tkip|wpa-psk-tkip,wpa2-psk-aes|static-wep|mpsk-aes}
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# auth-server <server-name>
(Instant AP)(SSID Profile <name>)# external-server
(Instant AP)(SSID Profile <name>)# server-load-balancing
(Instant AP)(SSID Profile <name>)# blacklist
```

```
(Instant AP)(SSID Profile <name>)# max-authentication-failures <number>
(Instant AP)(SSID Profile <name>)# radius-accounting
(Instant AP)(SSID Profile <name>)# radius-accounting-mode {user-association|user-
authentication}
(Instant AP)(SSID Profile <name>)# radius-interim-accounting-interval <minutes>
(Instant AP)(SSID Profile <name>)# radius-reauth-interval <minutes>
```

To configure open security settings for Employee and Voice users of a WLAN SSID profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# opmode opensystem
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# auth-server <server-name>
(Instant AP)(SSID Profile <name>)# external-server
(Instant AP)(SSID Profile <name>)# server-load-balancing
(Instant AP)(SSID Profile <name>)# blacklist
(Instant AP)(SSID Profile <name>)# max-authentication-failures <number>
(Instant AP)(SSID Profile <name>)# radius-accounting
(Instant AP)(SSID Profile <name>)# radius-accounting-mode {user-association|user-
authentication}
(Instant AP)(SSID Profile <name>)# radius-interim-accounting-interval <minutes>
(Instant AP)(SSID Profile <name>)# radius-reauth-interval <minutes>
```

Configuring Multiple PSK For WLAN SSID Profiles

WPA2 PSK-based deployments generally consist of a single passphrase configured as part of the WLAN SSID profile. This single passphrase is applicable for all clients that associate with the SSID. Starting from Aruba Instant 8.4.0.0, multiple PSKs in conjunction with ClearPass Policy Manager are supported WPA2 PSK-based deployments. Every client connected to the WLAN SSID will have its own unique PSK.

MPSK enhances the WPA2 PSK mode by allowing device-specific or group-specific passphrases, which are generated at ClearPass Policy Manager and sent to the Instant AP.

A MPSK passphrase requires MAC authentication against a ClearPass Policy Manager server. The MPSK passphrase works only with wpa2-psk-aes encryption and not with any other PSK based encryption. The Aruba-MPSK-Passphrase radius VSA is added and the ClearPass Policy Manager server populates this VSA with the encrypted passphrase for the device.

A user registers the device on a ClearPass Policy Manager guest-registration or device-registration webpage and receives a device-specific or group-specific passphrase. The device associates with the SSID using wpa2-psk-aes encryption and uses MPSK passphrase. The Instant AP performs MAC authentication of the client against the ClearPass Policy Manager server. On successful MAC authentication, the ClearPass Policy Manager returns Access-Accept with the VSA containing the encrypted passphrase. The Instant AP generates a PSK from the passphrase and performs 4-way key exchange. If the device uses the correct per-device or per-group passphrase, authentication succeeds. If the ClearPass Policy Manager server returns Access-Reject or the client uses incorrect passphrase, authentication fails.



When multiple PSK is enabled on the WLAN SSID profile, make sure that MAC authentication is not configured for RADIUS authentication. Multiple PSK and MAC authentication are mutually exclusive and follows a special procedure which does not require enabling MAC authentication in the WLAN SSID manually. Also, ensure that the RADIUS server configured for the WLAN SSID profile is not an internal server.

The following procedure configures MPSK authentication using the WebUI:

1. Navigate to the **Configuration** > **Networks** page.
2. Under **Networks** select the network you want to configure and click the edit icon.
3. Select **Security** tab. In the **Security Level** drop-down list box select **Personal**.
4. Select **MPSK-AES** from the **Key Management** drop-down list box.
5. Ensure a RADIUS server is selected from the **Authentication server 1** drop-down list box for MPSK authentication. Additionally, you may select a second authentication server for MPSK authentication from the **Authentication server 2** drop-down list box.

The following CLI command enables the multiple PSK feature on the WLAN SSID profile:

```
(Instant AP)(configure)# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile <profile_name>)# opmode mpsk-aes
```

The following CLI command is used to verify the status of the MPSK configuration on the WLAN SSID profile:

```
(Instant AP)# show network <ssid profile name>
```

RADIUS Accounting with MPSK

Instant supports RADIUS accounting with multiple PSKs in conjunction with ClearPass Policy Manager for WPA2 PSK-based deployments. When RADIUS accounting is enabled and MPSK authentication is successful, the AP sends an accounting start message to the ClearPass Policy Manager server to gather the accounting updates. The accounting updates are periodically sent based on the time interval configured on the AP.

The following procedure configures RADIUS accounting with MPSK using the WebUI:

1. Navigate to the **Configuration** > **Networks** page.
2. Under **Networks** select the network you want to configure and click the edit icon.
3. Select **Security** tab. In the **Security Level** drop-down list box select **Personal**.
4. Select **MPSK-AES** from the **Key Management** drop-down list box.
5. Ensure a RADIUS server is selected from the **Authentication server 1** drop-down list box for MPSK authentication.
   a. Select one of the following from the **Accounting** drop-down list box:
   b. **Use authentication servers**—Choose this option to use the same authentication servers for accounting.
6. **Use separate servers**—Choose this option to configure **Accounting server 1** and **Accounting server 2** separately.
7. Enter a value in minutes in the **Accounting interval** text box.
8. Click **Next** and then **Finish**.

The following CLI command configures RADIUS accounting with MPSK:

```
(Instant AP)(configure)# wlan ssid-profile <profile-name>
(Instant AP)(WLAN SSID Profile "name")# opmode mpsk-aes
(Instant AP)(WLAN SSID Profile "name")# radius-accounting
```

The following CLI command configures an accounting interval:

```
(Instant AP)(configure)# wlan ssid-profile <profile-name>
(Instant AP)(WLAN SSID Profile "name")# radius-interim-accounting-interval <minutes>
```

The following configurations are mutually exclusive with MPSK for the WLAN SSID profile and does not require to be configured manually:

- MPSK and MAC authentication
- MPSK and Blacklisting
- MPSK and internal RADIUS server

The Instant AP stores the MPSK passphrase in its local cache for client roaming. The cache is shared between all the Instant APs within a single cluster. The cache can also be shared with standalone Instant APs in a different cluster provided the APs belong to the same multicast VLAN. Each Instant AP will first search the local cache for the MPSK information. If the local cache has the corresponding mPSK passphrase, the Instant AP skips the mac authentication procedure, and provides access to the client. If the MPSK passphrase is not found in the local cache, you must manually configure the MPSK passphrase as shown in the above section.

The cached MPSK passphrase can be used only if the client connects to the same WLAN SSID. The entire MPSK local cache is erased in the following scenarios:

- If the cached MPSK does not work.
- The client is manually disconnected
- The client is disconnected from the CoA.



The MPSK passphrase in the local cache automatically expires if the client disconnects and does not connect again during the inactivity-timeout window.

To view the details of the MPSK local cache:

```
(Instant AP)# show ap mpskcache
```

Local Multiple PSK Operating Mode

In the Local MPSK operating mode, you can define upto 24 pre-shared keys per SSID on the gateway or the Instant AP without actually requiring an external policy engine like ClearPass Policy Manager. These local PSKs would serve as an extension of the base pre-shared key functionality. Local MPSK only supports passphrases in the form of strings. It does not support passphrases in the form of hex. The local MPSK is currently supported only on a **employee** type and **personal** sercurity level SSID.

The following CLI commands configure a local MPSK profile:

```
(Instant AP)(config)# wlan-mpsk-local <profile_name>
(Instant AP)(MPSK Local "profile_name")# mpsk-local-passphrase <key_name> <key>
```

Configuring Access Rules for a WLAN SSID Profile

he following procedure configures access rule settings for Employee and Voice networks only.If you are creating a new SSID profile, complete the WLAN settings and configure VLAN and security parameters, before defining access rules. For more information, see Configuring WLAN Settings for an SSID Profile on page 131, Configuring VLAN Settings for a WLAN SSID Profile on page 136, and Points to Remember on page 145.Captive Portal for Guest Access.

You can configure up to 128 access rules for an Employee, Voice , or Guest network using the Instant UI or the CLI.

Table 46: *Configuring Access Rules*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Networks**. 2. Under **Networks** select the network you want to configure and click **Edit**. 3. Select **Access** tab. In the **Access Rules** drop-down list box select one of the following type: ▪ **Unrestricted**—Select this option to set unrestricted access to the network. ▪ **Network-based**—Select this option to set common rules for all users in a network. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. 4. To define an access rule: a. Click **+**. b. Select appropriate options in the **New Rule** window. c. Click **OK**.	1. In the **Networks** tab, select the network to configure and click **edit**. 2. Select the **Access** tab 3. Specify any of the following types of security levels by moving the slider to a desired level: ▪ **Unrestricted**—Select this option to set unrestricted access to the network. ▪ **Network-based**—Select this option to set common rules for all users in a network. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. 4. To define an access rule: a. Click **New**. b. Select appropriate options in the **New Rule** window. c. Click **OK**.

- **Role-based**—Select this option to enable access based on user roles. For role-based access control:
  - Create a user role if required. For more information, see Configuring User Roles.
  - Create access rules for a specific user role. For more information, see Configuring ACL Rules for Network Services on page 260. You can also configure an access rule to enforce captive portal authentication for an SSID that is configured to use 802.1X authentication method. For more information, see Configuring Captive Portal Roles for an SSID on page 200.
  - Create a role assignment rule. For more information, see Configuring Derivation Rules on page 282.
- **Enforce Machine Authentication**— Select this check box to configure access rights to clients based on whether the client device supports machine authentication.
- Click **Finish**.

The following CLI command configures access control rules for a WLAN SSID:

```
(Instant AP)(config)# wlan access-rule <name>
(Instant AP)(Access Rule <name>)# rule <dest> <mask> <match> {<protocol> <start-port>
<end-port> {permit|deny|src-nat [vlan <vlan_id>|tunnel]|dst-nat{<IP-address>
<port>|<port>}}| app <app> {permit|deny}| appcategory <appgrp>|webcategory <webgrp>
{permit|deny}| webreputation <webrep> [<option1....option9>]
```

The following CLI command configures access control rules based on the SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-by-ssid
```

The following CLI command configures role assignment rules:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role <attribute>{{equals|not-equals|starts-
with|ends-with|contains|matches-regular-expression}<operator><role>|value-of}
```

The following CLI command configures a pre-authentication role:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-pre-auth <role>
```

The following CLI command configures machine and user authentication roles:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-machine-auth <machine_only> <user_only>
```

The following CLI command configures unrestricted access:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-unrestricted
```

Example

The following example configures access rules for the wireless network:

```
(Instant AP)(config)# wlan access-rule WirelessRule
```

ESSID and VLAN Configuration

In addition to the WLAN SSID, you can set a unique ESSID and also configure a unique a VLAN for each Instant AP in a cluster. Clients will be able to connect to the defined SSIDs and can configure the defined VLANs in the Instant AP cluster.

You can configure the ESSID and VLAN settings by using the Instant CLI.

The following CLI command configures ESSID and VLAN settings in a WLAN profile:

```
(Instant AP)(config)# wlan ssid-profile TechPubsAP
(Instant AP)(SSID Profile "TechPubsAP")# essid $per-ap-ssid
(Instant AP)(SSID Profile "TechPubsAP")# vlan $per-ap-vlan
```

The following CLI command configure a unique ESSID:

```
(Instant AP)# per-ap-ssid pcap
```

To configure VLAN settings:

```
(Instant AP)# per-ap-vlan 123
```

To verify the ESSID and VLAN configurations:

```
(Instant AP)# show ap-env
Antenna Type:Internal
Need USB field:Yes
per_ap_ssid:pcap
per_ap_vlan:123
installation_type:indoor
uap_controller_less:1
flex_radio_mode:2.4ghz
ap2xx_prestandard_poeplus_detection:1
```



For information on configuring a native VLAN on a wired profile, see Configuring VLAN for a Wired Profile on page 163.

Fast Roaming for Wireless Clients

Instant supports the following features that enable fast roaming of clients:

- OKC
- Fast BSS Transition (802.11r Roaming)
- Radio Resource Management (802.11k)
- BSS Transition Management (802.11v)
- Fast Roaming for Wireless Clients

OKC

Instant now supports OKC-based roaming. In OKC-based roaming, the Instant AP stores one PMK per client, which is derived from the last 802.1X authentication completed by the client in the network. The cached PMK is used when a client roams to a new Instant AP. This allows faster roaming of clients between the Instant APs in a cluster, without requiring a complete 802.1X authentication.



OKC roaming (when configured in the 802.1X Authentication profile) is supported on WPA2 clients. If the wireless client (the 802.1X supplicant) does not support this feature, a complete 802.1X authentication is required whenever a client roams to a new Instant AP.

Configuring an Instant AP for OKC Roaming

The following procedure describes how to enable OKC roaming on a WLAN SSID by using the Instant WebUI and CLI:

Table 47: *Configuring OKC Roaming*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Networks** page 2. Under **Networks** select the network you want to configure and click **Edit**. 3. Select the **Security** tab. 4. In the **Security Level** drop-down list box, select **Enterprise**. 5. In the **Key management** drop-down list box, select **WPA2 Enterprise** or **Both (WPA2 & WPA)**. 6. Under **Fast Roaming,** toggle the **Opportunistic Key Caching (OKC)** switch to enable. 7. Click **Next** and then **Finish**.	1. In the **Networks** tab, select the network you want to edit and click **edit**. 2. Select the **Security** tab. 3. Move the security level slider to **Enterprise**. 4. Select the **WPA2 Enterprise** or **Both (WPA2 & WPA)** option from the **Key management** drop-down list. 5. Under **Fast Roaming** select the **Opportunistic Key Caching (OKC)** checkbox to enable OKC. 6. Click **Next** and then **Finish**.

The following CLI command enables OKC roaming on a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile "<name>")# opmode {wpa2-aes| wpa-tkip,wpa-aes,wpa2-
tkip,wpa2-aes}
(Instant AP)(SSID Profile "<name>")# okc
```

The following CLI command disables OKC roaming on a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile "<name>")# opmode {wpa2-aes|wpa-tkip,wpa-aes,wpa2-tkip,wpa2-
aes}
(Instant AP)(SSID Profile "<name>")# no okc
```

Fast BSS Transition (802.11r Roaming)

802.11r is a roaming standard defined by IEEE. When enabled, 802.11r reduces roaming delay by pre-authenticating clients with multiple target Instant APs before a client roams to an Instant AP. With 802.11r implementation, clients pre-authenticate with multiple Instant APs in a cluster.

As part of the 802.11r implementation, Instant supports the Fast BSS Transition protocol. The Fast BSS Transition mechanism reduces client roaming delay when a client transitions from one BSS to another within the same cluster. This minimizes the time required to resume data connectivity when a BSS transition happens.



Fast BSS Transition is operational only if the wireless client supports 802.11r standard. If the client does not support 802.11r standard, it falls back to the normal WPA2 authentication method.

Configuring an Instant AP for 802.11r support

The following procedure describes how to configure 802.11r support for a WLAN SSID by using the Instant WebUI and CLI:

Table 48: *Configuring 802.11r Roaming*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Networks** page 2. Under **Networks** select the network you want to configure and click **Edit**. 3. Select the **Security** tab. 4. Under **Fast Roaming**, toggle the **802.11r** switch to enable. 5. Click **Next** and then **Finish**.	1. In the **Networks** tab, select the network you want to edit and click **edit**. 2. Select the **Security** tab. 3. Under **Fast Roaming**, select the **802.11r** check box. 4. Click **Next** and then **Finish**.

The following CLI command enables 802.11r roaming on a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# dot11r
```

Mobility Domain Identifier

In a network of standalone Instant APs within the same management VLAN, 802.11r roaming does not work. This is because the mobility domain identifiers do not match across Instant APs. They are auto-generated based on a virtual controller key. Instant introduces a an option for users to set a mobility domain identifier for 802.11r SSIDs. For standalone Instant APs in the same management VLAN, 802.11r roaming works only when the mobility domain identifier is configured with the same value.

You can configure a mobility domain identifier by using the Instant WebUI or the CLI.

Table 49: *Configuring Mobility Domain Identifier*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Networks** page 2. Under **Networks** select the network you want to configure and click **Edit**. 3. Select the **Security** tab. 4. Under **Fast Roaming**, toggle the **802.11r** switch to enable. 5. In the **MDID** text box, enter the mobility domain identifier. 6. Click **Next** and then **Finish**.	1. In the **Networks** tab, select the network you want to edit and click **edit**. 2. Select the **Security** tab. 3. Under **Fast Roaming**, select the **802.11r** check box. 4. In the **MDID** text box enter the mobility domain identifier. 5. Click **Next** and then **Finish**.

The following CLI command enables MDID on a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# mdid <Mobility domain ID>
```

Radio Resource Management (802.11k)

The 802.11k standard provides mechanisms for Instant APs and clients to dynamically measure the available radio resources and enables stations to query and manage their radio resources. In an 802.11k-enabled network, Instant APs and clients can share radio and link measurement information, neighbor reports, and beacon reports with each other. This allows the WLAN network infrastructural elements and clients to assess resources and make optimal mobility decisions to ensure QoS and seamless continuity.

Instant supports the following radio resource management information elements with 802.11k support enabled:

- **Power Constraint IE**—The power constraint element contains the information necessary to allow a client to determine the local maximum transmit power in the current channel.
- **AP Channel Report IE**—The Instant AP channel report element contains a list of channels in a regulatory class where a client is likely to find an Instant AP, including the Instant AP transmitting the Instant AP channel report.
- **Radio Resource Management Enabled Capabilities IE**—The RRM-enabled capabilities element signals support for radio measurements in a device. The clients use this IE to specify their radio measurement capabilities.
- **BSS Load Element**—The BSS load element contains information on the density of clients and traffic levels in the QBSS.
- **TPC Report IE**—The TPC IE contains transmit power and link margin information.
- **Quiet IE**: The Quiet IE defines an interval during which no transmission occurs in the current channel. This interval may be used to assist in making channel measurements without interference from other stations in the BSS.
- **Extended Capabilities IE**—The extended capabilities IE carries information about the capabilities of an IEEE 802.11 station.

Beacon Report Requests and Probe Responses

The beacon request frame is sent by an Instant AP to request a client to report the list of beacons detected by the client on all channels.

- The beacon request is sent using the radio measurement request action frame.
- It is sent only to those clients that have the capability to generate beacon reports. The clients indicate their capabilities through the *RRM enabled capabilities IE* sent in the association request frames.
- By default, the beacon request frames are sent at a periodicity of 60 seconds.

Configuring a WLAN SSID for 802.11k Support

The following procedure describes how to enable 802.11k support on a WLAN SSID by using the Instant WebUI or the CLI.

Table 50: *Configuring 802.11k Fast Roaming*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Networks** page 2. Under **Networks** select the network you want to	1. In the **Networks** tab, select the network you want to edit and click **edit**.

New WebUI	Old WebUI
configure and click **Edit**. 3. Select the **Security** tab. 4. Under **Fast Roaming**, toggle the **802.11k** switch to enable. 5. Click **Next** and then **Finish**.	2. Select the **Security** tab. 3. Under **Fast Roaming**, select the **802.11k** check box. 4. Click **Next** and then **Finish**.

To allow the Instant AP and clients to exchange neighbor reports, ensure that Client Match is enabled through **RF > ARM > Client match > Enabled** in the WebUI or by executing the **client-match** command in the **arm** configuration sub-command mode.

The following CLI command enables the 802.11k profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# dot11k
```

The following CLI command is used to view the beacon report details:

```
(Instant AP)# show ap dot11k-beacon-report <mac>
```

The following CLI command is used to view the neighbor details:

```
(Instant AP)# show ap dot11k-nbrs
```

Example

```
(Instant AP)(config)# wlan ssid-profile dot11k-profile
(Instant AP)(SSID Profile "dot11k-profile")# dot11k
```

BSS Transition Management (802.11v)

The 802.11v standard provides Wireless Network Management enhancements to the IEEE 802.11 MAC and PHY. It extends radio measurements to define mechanisms for wireless network management of stations including BSS transition management.

Instant APs support the generation of the BSS transition management request frames to the 802.11k clients when a suitable Instant AP is identified for a client through Client Match.

Configuring a WLAN SSID for 802.11v Support

The following procedure describes how to enable 802.11v support on a WLAN SSID by using the Instant WebUI or the CLI.

Table 51: *Configuring 802.11v Fast Roaming*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Networks** page 2. Under **Networks** select the network you want to configure and click **Edit**. 3. Select the **Security** tab. 4. Under **Fast Roaming**, toggle the **802.11v** switch to enable. 5. Click **Next** and then **Finish**.	1. In the **Networks** tab, select the network you want to edit and click **edit**. 2. Select the **Security** tab. 3. Under **Fast Roaming**, select the **802.11v** check box. 4. Click **Next** and then **Finish**.

The following CLI command enables the 802.11v profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
```

```
(Instant AP)(SSID Profile <name>)# dot11v
```

Example

```
(Instant AP)(config)# wlan ssid-profile dot11v-profile
(Instant AP)(SSID Profile "dot11v-profile")# dot11v
```

Configuring Modulation Rates on a WLAN SSID

Instant APs allow you to enable or disable modulation rates for a radio band; HT MCS set; and VHT MCS rates set, when configuring a WLAN SSID profile. For example, the 802.11g band supports the modulation rate including 1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps and 802.11a band supports a modulation rate set including 6, 9, 12, 18, 24, 36, 48, 54 Mbps.

The 802.11 radio profiles support basic modulation and transmission rates. The 802.11g basic modulation rates determine the 802.11b or 802.11g rates for the data that are advertised in beacon frames and probe response and 802.11g transmission rates determine the 802.11b or 802.11g rates at which the Instant AP can transmit data.

For 802.11n clients, you can now configure an HT MCS rate set so that the SSID does not broadcast the disabled MCS rates list.

For 802.11ac clients, only 10 MCS rates supported in the 802.11ac mode and Instant APs use a combination of VHT MCSs and spatial streams to convey the supported MCS rates.

The following CLI command is used to configure modulation rates:

```
(Instant AP)# config terminal
(Instant AP)(config)# wlan ssid-profile <ssid_profile>
(Instant AP)(SSID Profile "<ssid_profile>")# a-basic-rates 6 9 12 18
(Instant AP)(SSID Profile "<ssid_profile>")# a-tx-rates 36 48 54
(Instant AP)(SSID Profile "<ssid_profile>")# supported-mcs-set 1,3,6,7
(Instant AP)(SSID Profile "<ssid_profile>")# vht-support-mcs-map 7, 9, 8
```

Multi-User-MIMO

The MU-MIMO feature allows the 802.11ac Wave 2 Instant APs to send multiple frames to multiple clients simultaneously over the same frequency spectrum. With MU-MIMO, Instant APs can support simultaneous directional RF links and up to four simultaneous full-rate Wi-Fi connections (for example, smart phone, tablet, laptop, multimedia player, or other client device).

The MU-MIMO feature is enabled by default on WLAN SSIDs to allow Instant APs to use the MU beamformer bit in beacon frames to broadcast to clients. When disabled, the MU beamformer bit is set to unsupported.

Enabling or Disabling MU-MIMO

The MU-MIMO feature is enabled by default on a WLAN SSID profile. The following CLI command is used to disable this feature:

```
(host)(config)# wlan ssid-profile <ssid_profile>
(host)(SSID Profile "<ssid_profile>")# vht-mu-txbf-disable
```

The following CLI command is used to re-enable MU-MIMO on a WLAN SSID profile:

```
(host)(config)# wlan ssid-profile <ssid_profile>
(host)(SSID Profile "<ssid_profile>")# no vht-mu-txbf-disable
```

RTS/CTS Flow Control

The RTS/CTS mechanism allows devices to reserve the RF medium and minimize the frame collisions introduced by hidden stations. When RTS is enabled, a higher number of retransmissions occurring on the WLAN triggers the RTS/CTS handshake and the transmitter station sends an RTS frame to the receiver station. The receiver station responds with a CTS frame. The RTS/CTS frames are sent only when the packet size exceeds the RTS threshold. By default, the RTS threshold is set to 2333 octets.

Configuring RTS/CTS Threshold

You can set the RTS/CTS threshold value within the range of 0–2347 octets. By default, the RTS/CTS threshold is set to 2333.

The following CLI command is used to configure the RTS/CTS threshold:

```
(Instant AP)(config)# wlan ssid-profile <ssid_profile>
(Instant AP)(SSID Profile "<ssid_profile>")# rts-threshold <threshold>
```

To disable RTS/CTS, set the RTS threshold value to 0.

Management Frame Protection

Instant supports the IEEE 802.11w standard, also known as Management Frame Protection. The Management Frame Protection increases the security by providing data confidentiality of management frames. Management Frame Protection uses 802.11i framework that establishes encryption keys between the client and Instant AP.

The following command is used to enable Management Frame Protection on the Instant AP:

```
(Instant AP)(config)# wlan ssid-profile myAP
(Instant AP)(SSID Profile "myAP")# mfp-capable
(Instant AP)(SSID Profile "myAP")# mfp-required
```

If the *mfp-required* parameter is enabled, the SSID supports only the clients that exhibit the Management Frame Protection functionality.

If the *mfp-capable* parameter enabled, the SSID supports Management Frame Protection capable clients and non-Management Frame Protection clients.



The Management Frame Protection configuration is a per-SSID configuration.

Management Frame Protection can be enabled only on WPA2-PSK and WPA2-enterprise SSIDs. The 802.11r fast roaming option will not take effect when MFP is enabled.

High Efficiency WLAN (HEW)

Instant supports the IEEE 802.11ax standard, also known as High-Efficiency WLAN (HEW). HEW improves spectrum efficiency and area throughput in dense deployment scenarios of APs or stations in both indoor and outdoor environments. HEW enhances the 802.11 PHY and MAC channels on both 2.4 GHz and 5 GHz frequency bands.

HEW includes the following key features:

- Backward compatible with 802.11a/b/g/n/ac.
- Better power management for longer battery life.

Configuring High Efficiency on a WLAN SSID

Most deployments do not require manual configuration of the high-efficiency SSID profile as this option is enabled by default. However, you can configure advanced high-efficiency SSID profile settings or modify default SSID profile values using the Instant WebUI or CLI.

The following procedure describes how to enable or disable High Efficiency on a WLAN SSID:

1. Navigate to the **Configuration** > **Networks** page.
2. Under **Networks** select the WLAN network you want to configure and click the edit icon.
3. Click **Show advanced options** at the bottom of the window.
4. Under the **802.11** group, slide the **High efficiency** toggle switch to the right to enable the high efficiency function, or slide the toggle switch to the left if you want to disable high efficiency on the WLAN SSID.
5. Click **Next** and then **Finish**.

The following CLI command enables High Efficiency on a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile "<profile_name>")# high-efficiency-enable
```

The following CLI command disables High Efficiency on a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile "<profile_name>")# high-efficiency-disable
```

Multi Band Operation (MBO)

The MBO feature enables the WLAN network to utilize the available spectrum efficiently, and helps in optimizing the connectivity experience for end-users. MBO, also known as Agile Multiband is a pre-requisite for 802.11ax certification, therefore any AP or STA that supports 802.11ax will have the MBO capabilities.

MBO allows the APs and STAs exchange information and facilitates efficient use of multiple frequency bands or channels that are available in the APs and the STAs. MBO is supported on 510 Series, 530 Series and 550 Series access points.

Enabling **mbo-enable** on the WLAN SSID profile will automatically enable the following:

- **mfp-capable** and **dot11k** functionalities on the SSID profile.
- **advertise-enabled-capabilities-ie** and **country-ie** parameters in the rrm-ie-profile.
- **interworking-enable** in the hotspot profile if not enabled.

MBO on Instant APs can only be configured using the CLI. Use the **mbo-enable** command under **wlan ssid-profile** to enable MBO.

The following CLI command enables MBO on a WLAN SSID profile.

```
(Instant AP) (config) # wlan ssid-profile <profile name>
(Instant AP) (wlan ssid-profile <profile name>) #mbo-enable
```

To enable Cellular Data Capability attribute of MBO on the Instant AP, use the **cdc-enable** command in the WLAN SSID profile. This feature will only take effect if Multi Band Operation is enabled on the WLAN SSID.

The following CLI command enables Cellular Data Capability on the SSID.

```
(Instant AP) (config) # wlan ssid-profile <profile name>
(Instant AP) (wlan ssid-profile <profile name>) #cdc-enable
```

Configuring 802.11k Profile

The 802.11k protocol provides mechanisms for APs and clients to dynamically measure the available radio resources. In an 802.11k enabled network, APs and clients can send neighbor reports, beacon reports, and link measurement reports to each other. This allows the APs and clients to take appropriate connection actions.

The **dot11k-profile** configures attributes for information exchange between the peers. A default **dot11k**-profile will be used for MBO if no **dot11k-profile** is configured. A dot11k profile can be configured using the **dot11k-profile** command. The configured **dot11k-profile** should be attached to the respective **wlan ssid-profile** using the **dot11k-profile <profile name>** parameter. For information on configuring dot11k-profile, see **dot11k-profile** command in the *Aruba Instant 8.x CLI Reference Guide*.

Radio Resource Management Information Elements

Aruba Instant supports the following radio resource management (RRM) information elements for APs with 802.11k support enabled. These settings can be enabled the CLI. The rrm-ie-profile configured should be attached to the **dot11k-profile** command using the **rrm-ie-profile <profile-name>** command.

By default the **advertise-enabled-capabilities-ie** and **country-ie** parameters are enabled in the rrm-ie-profile. To disable these parameters use the **rrm-ie-profile** command. For information on configuring rrm-ie-profile, see rrm-ie-profile command in the *Aruba Instant 8.x CLI Reference Guide*.

Beacon Report Requests

The beacon report requests are sent only to 802.11k-compliant clients that advertise Beacon Report Capability in their RRM Enabled Capabilities IE. The beacon request frames are sent every 60 seconds. The content of the report requests can be defined in the Beacon Report Request profile using the CLI. The beacon report request profile configured should be attached to the dot11k-profile command using the **bcn-rpt-req-profile <profile-name>** command.

The beacon report request profile is configured using the **bcn-rpt-req-profile** command. To configure a bcn-rpt-req-profile, see bcn-rpt-req-profile command in the *Aruba Instant 8.x CLI Reference Guide*.

Disabling Short Preamble for Wireless Client

To improve the network performance and communication between the Instant AP and its clients, you can enable or disable the transmission and reception of short preamble frames. If the short preamble is optional for the wireless devices connecting to an SSID, you can disable short preamble through the Instant AP CLI. Short preamble is enabled by default.

The following CLI command disables the short preamble on a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <ssid_profile>
(Instant AP)(SSID Profile "<ssid_profile>")# short-preamble-disable
```

Disabling a WLAN SSID Profile

The following procedure describes how to disable an SSID profile in the Instant WebUI or the CLI.

Table 52: *Disabling a WLAN SSID Profile*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Networks** page 2. Under **Networks** select the network you want to	1. In the **Networks** tab, select the network you want to edit and click **edit**.

New WebUI	Old WebUI
configure and click **Edit**. 3. Under **Basic** click **Show advanced options** at the bottom of the page. 4. In the **SSID** field under **Miscellaneous**, select the **Disable** check box to disable the SSID. The SSID is enabled by default. 5. Click **Next** until **Finish** to save the setting.	2. Under **WLAN Settings**, click **Show advanced options** at the bottom of the window. 3. In the **SSID** field under **Miscellaneous**, select the **Disable** check box to disable the SSID. The SSID is enabled by default. 4. Click **Next** until **Finish** to save the setting.

The following CLI command disables a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# disable
```

The following CLI command enables a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# enable
```

Editing a WLAN SSID Profile

The following procedure describes how to edit a WLAN SSID profile by using the Instant WebUI.

Table 53: *Editing a WLAN SSID Profile*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Networks** page 2. Under **Networks** select the network you want to configure and click **Edit**. 3. Modify the settings as required under the respective tabs. 4. Click **Next** until **Finish** to save the setting.	1. In the **Networks** tab, select the network you want to edit and click **edit**. 2. Modify the settings as required under the respective tabs. 3. Click **Next** until **Finish** to save the changes.

Deleting a WLAN SSID Profile

The following procedure describes how to delete a WLAN SSID profile by using the Instant WebUI:

Table 54: *Deleting a WLAN SSID Profile*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Networks** page 2. Under **Networks** select the WLAN SSID you want to delete and click **Delete**. 3. Modify the settings as required under the respective tabs. Click **Delete Now** to confirm deletion.	1. In the **Networks** tab, select the WLAN SSID you want to delete and click **x** beside the edit button. 2. Click **Delete Now** to confirm deletion.

Enhancements to WLAN SSID Configuration

Instant 8.4.0.0 introduces support for configuration of up to 32 SSID profiles for cluster-based Instant APs. When an SSID profile is created, an access rule with the same name is created.

Pre-Authentication and Post-Authentication Role

When you configure captive-portal authentication, two post-authentication ACLs with the same and a pre-authentication role are created in the Instant AP datapath. Therefore, you cannot drastically increase the count of the SSID profile.

Mapping WLAN Index and Virtual AP

Prior to the introduction of this enhancement, the mapping method of WLAN SSID profile and virtual AP was determined by the WLAN index. But this mapping method is not supported when 32 SSID profiles are configured. To support this mapping, Instant introduces the advanced-zone feature. The benefit of this feature is that the same ESSIDs can be broadcast on Instant APs that are part of the same Instant AP zone in a cluster.



When the advanced-zone feature is enabled and a zone is already configured with 16 SSIDs, ensure to remove the zone from two WLAN SSID profiles if you want to disable extended SSID. This action can be performed only when extended SSID is disabled.

You can configure the advanced-zone feature by using the CLI.

In the CLI

```
(Instant AP)# advanced-zone
```

Extended SSID

When extended SSID is disabled, the maximum count of zones in an SSID profile reduces to 14. This is because, the first two virtual APs are reserved for mesh. The **show ap debug network-bssid** command displays the mapping relationship between WLAN SSID profile and virtual APs.

DPI

DPI manager gathers session data periodically from the Instant AP datapath. Data is chunked every time a CLI command is executed to display per-AP statistics. It shows a complete cluster view that can display apps, app category, web category, and web reputation. To show a per-SSID view display, users must collect DPI manager's statistics data from an Instant AP to its master. The master adds the data and displays the statistics.

When data path sends the statistics data to the DPI manager, it is aware of the virtual AP ID but not the WLAN index. The DPI manager computes the statistics with the WLAN index. So except for the configured WLAN SSID, the Instant AP datapath must be aware of the mapping relationship of the WLAN index and virtual AP ID.

You can view the mapping of the WLAN index and BSSID by using the CLI.

In the CLI

```
(Instant AP)# show ap debug network-bssid
```

Time-Range and Out of Service

The following features make the WLAN SSID profile dynamically inactive even if the SSID zone matches with Instant AP zone:

- Time-range
- Out of service

To avoid the flapping of the WLAN index and virtual AP mapping, the WLAN SSID profile is disabled because of either time-range or out of service. The virtual AP status is set to inactive and not unused.

AirWave or Central Impact

AirWave or Central servers can view the WLAN index and BSSID mapping when Instant APs (master and slave) send WLAN information to the servers.

Wireless Client Bridge

A wireless client bridge connects two wired networks together over Wi-Fi. The wireless bridge acts as a client, logging in to the primary router and getting an Internet connection, which it passes on to the devices connected to its LAN Jacks. A wireless client can typically receive one IP address at a time from a DHCP server. However, the wireless bridge acting as a client can obtain multiple IPv4 address from the devices connected to it. Instant supports the Aruba 501 Wireless Client Bridge which enables you to easily integrate devices with no native wireless support into a WLAN network. It provides strong enterprise-class layered security features, including an IEEE 802.1X supplicant, to protect the network from intrusions. The Aruba 501 Wireless Client Bridge can bridge up to 15 Ethernet client devices running a legacy networking protocol to the WLAN – extending wireless network access to a wide range of protocols. This bridge provides the benefits of wireless mobility for devices like electronic cash registers, scales, servers, printers, medical equipment and other devices. It can be deployed in any location where a WLAN signal is available – saving the time and expense of installing Ethernet cables for wired network access.

Configuring Wireless Client Bridge

The wired client devices connected to the client bridge have different IPv4 address which might be configured statically or assigned by DHCP server dynamically. The Aruba 501 wireless client bridge changes the client mac address in DHCP request sent from its wired client devices. The DHCP server then offers different IPs for these requests. The client bridge will then forward the offers to real client devices. The source MAC address of the client devices will be changed to the MAC address of the wireless client bridge. Hence, from the AP view, one MAC will have multiple IP addresses.

The following procedure configures a wireless client bridge:

1. Navigate to the **Configuration** > **Networks** page.
2. Under **Networks** select the WLAN network for which you want to configure the wireless client bridge.
3. Click **Show advanced options** at the bottom of the window.
4. Under the **Miscellaneous** group, enter the maximum number of IPv4 users in the **Max IPv4 users** text box. The default number of IPv4 users is 2, and the maximum threshold limit is 32 users.
5. Click **Next** and then **Finish**.

The following CLI command configures wireless client bridging on a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile "<profile_name>")# max-ipv4-users <threshold>
```

The following CLI command disables wireless client bridging on a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile "<profile_name>")# no max-ipv4-users
```

The following CLI command is used to view the maximum number of IPv4 users configured on a WLAN SSID:

```
(Instant AP)# show network <ssid-profile-name>
```

Chapter 12
Wired Profiles

This chapter describes the following procedures:

- Configuring a Wired Profile on page 161
- Assigning a Profile to Ethernet Ports on page 170
- Enabling 802.3az Energy Efficient Ethernet Standard on page 170
- Editing a Wired Profile on page 171
- Deleting a Wired Profile on page 171
- LACP on page 172
- Understanding Hierarchical Deployment on page 173
- Loop Protection on page 174

Configuring a Wired Profile

The Ethernet ports allow third-party devices such as VoIP phones or printers (which support only wired connections) to connect to the wireless network. You can also configure an ACL for additional security on the Ethernet downlink.

The wired profile configuration for Employee network involves the following procedures:

1. Configuring Wired Settings on page 161
2. Configuring VLAN for a Wired Profile on page 163
3. In the Old WebUI on page 165
4. Configuring Access Rules for a Wired Profile on page 167

For information on creating a wired profile for guest network, see Captive Portal for Guest Access.

Configuring Wired Settings

You can configure wired settings for a wired profile by using the Instant WebUI or the CLI.

In the Old WebUI

1. Click the **Wired** link under **More** on the Instant main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks**. The **New Wired Network** window is displayed.
3. Click the **Wired Settings** tab and configure the following parameters:
   a. **Name**—Specify a name for the profile.
   b. **Primary Usage**—Select **Employee** or **Guest**.
   c. **Speed/Duplex**—Ensure that appropriate values are selected for **Speed/Duplex**. Contact your network administrator if you need to assign speed and duplex parameters.
   d. **POE**—Set **POE** to **Enabled** to enable PoE.

e. **Admin Status**—Ensure that an appropriate value is selected. The **Admin Status** indicates if the port is up or down.

4. Click **Show advanced options** and configure the following parameters as required:
   a. **Content Filtering**—Select **Enabled** for **Content Filtering**.
   b. **Uplink**—Select **Enabled** to configure uplink on this wired profile. If **Uplink** is set to **Enabled** and this network profile is assigned to a specific port, the port will be enabled as Uplink port. For more information on assigning a wired network profile to a port, see Assigning a Profile to Ethernet Ports on page 170.
   c. **Spanning Tree**—Select the **Spanning Tree** check box to enable STP on the wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP will not operate on the uplink port and is supported only on Instant APs with three or more ports. By default, Spanning Tree is disabled on wired profiles.
   d. **Inactivity Timeout**—Specify the time out interval within the range of 60–86,400 seconds for inactive wired clients. The default interval is 1000 seconds.
5. Click **Next**. The **VLAN** tab details are displayed.
6. Configure VLAN for the wired profile. For more information, see Configuring VLAN for a Wired Profile on page 163.

In the New WebUI

1. Navigate to the **Configuration** > **Networks**.
2. Under **Networks**, click **+** to create a new network.
3. Under **Name & Usage**, select **Wired** from the **Type** drop-down list box.
4. Configure the following parameters:
   a. **Name**—Specify a name for the profile.
   b. **Primary usage**—Select **Employee** or **Guest**.
   c. **POE**— Toggle the **POE** switch to enable PoE.
   d. **Admin status**—Ensure that an appropriate value is selected. The **Admin status** indicates if the port is up or down.
5. Click **Show advanced options** and configure the following parameters as required:
   a. **Speed/Duplex**—Ensure that appropriate values are selected for **Speed/Duplex**. Contact your network administrator if you need to assign speed and duplex parameters.
   b. **Content filtering**—Select **Enabled** for **Content filtering**.
   c. **Uplink**—Enable the **Uplink** option to configure uplink on this wired profile. If this option is enabled and this network profile is assigned to a specific port, the port will be enabled as Uplink port. For more information on assigning a wired network profile to a port, see Assigning a Profile to Ethernet Ports on page 170.
   d. **Spanning Tree**—Enable the **Spanning Tree** option to enable STP on the wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP will not operate on the uplink port and is supported only on Instant APs with three or more ports. By default, Spanning Tree is disabled on wired profiles.

e. **Inactivity Timeout**—Specify the time out interval within the range of 60–86,400 seconds for inactive wired clients. The default interval is 1000 seconds.

6. Click **Next**. The **VLAN** tab details are displayed.
7. Configure VLAN for the wired profile. For more information, see Configuring VLAN for a Wired Profile on page 163.

In the CLI

To configure the settings for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# type {<employee>|<guest>}
(Instant AP)(wired ap profile <name>)# speed {10|100|1000|auto}
(Instant AP)(wired ap profile <name>)# duplex {half|full|auto}
(Instant AP)(wired ap profile <name>)# no shutdown
(Instant AP)(wired ap profile <name>)# poe
(Instant AP)(wired ap profile <name>)# uplink-enable
(Instant AP)(wired ap profile <name>)# content-filtering
(Instant AP)(wired ap profile <name>)# spanning-tree
```

Configuring VLAN for a Wired Profile



If you are creating a new wired profile, complete the Wired Settings procedure before configuring the VLAN settings. For more information, see Configuring Wired Settings on page 161.

You can configure VLAN using the Instant WebUI or the CLI.

In the Old WebUI

To configure a VLAN:

1. In the **VLAN** tab, enter the following information.
   a. **Mode**—You can specify any of the following modes:
      - **Access**—Select this mode to allow the port to carry a single VLAN specified as the native VLAN.
      - **Trunk**—Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.

   b. Specify any of the following values for **Client IP Assignment**:
      - **Virtual Controller managed**: Select this option to allow the virtual controller to assign IP addresses to the wired clients. When the virtual controller assignment is used, the source IP address is translated to the physical IP address of the master Instant AP for all client traffic that goes through this interface. The virtual controller can also assign a guest VLAN to a wired client.
      - **Network assigned**: Select this option to allow the clients to receive an IP address from the network to which the virtual controller is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required.

   c. If the **Trunk** mode is selected:
      - Specify the VLAN in **Allowed VLANs**, enter a list of comma separated digits or ranges, for example, 1,2,5 or 1–4, or all. The Allowed VLAN refers to the VLANs carried by the port in Access mode.

- If **Client IP assignment** is set to **Network assigned**, specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1–4093.

d. If the **Access** mode is selected:
   - If **Client IP assignment** is set to **Virtual Controller managed**, proceed to step 2.
   - If **Client IP assignment** is set to **Network assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode.

2. **Client VLAN assignment**—You can specify any of the following options.
   - **Default**—Select this option to set the default VLAN.
   - **Custom**—Select this option to configure a custom VLAN.
3. Click **Next**. The **Security** tab details are displayed.
4. Configure security settings for the wired profile. For more information, see In the Old WebUI on page 165.

In the New WebUI

To configure a VLAN:

1. In the **VLAN** tab, enter the following information.
   a. **Mode**—You can specify any of the following modes:
      - **Access**—Select this mode to allow the port to carry a single VLAN specified as the native VLAN.
      - **Trunk**—Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.

   b. Specify any of the following values for **Client IP Assignment**:
      - **Virtual Controller managed**: Select this option to allow the virtual controller to assign IP addresses to the wired clients. When the virtual controller assignment is used, the source IP address is translated to the physical IP address of the master Instant AP for all client traffic that goes through this interface. The virtual controller can also assign a guest VLAN to a wired client.
      - **Network assigned**: Select this option to allow the clients to receive an IP address from the network to which the virtual controller is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required.

   c. If the **Trunk** mode is selected:
      - Specify the VLAN in **Allowed VLANs**, enter a list of comma separated digits or ranges, for example, 1,2,5 or 1–4, or all. The Allowed VLAN refers to the VLANs carried by the port in Access mode.
      - If **Client IP assignment** is set to **Network assigned**, specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1–4093.

   d. If the **Access** mode is selected:
      - If **Client IP assignment** is set to **Virtual Controller managed**, proceed to step 2.
      - If **Client IP assignment** is set to **Network assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode.

2. **Client VLAN assignment**—You can specify any of the following options.
   - **Default**—Select this option to set the default VLAN.
   - **Custom**—Select this option to configure a custom VLAN.
3. Click **Next**. The **Security** tab details are displayed.
4. Configure security settings for the wired profile. For more information, see In the Old WebUI on page 165.

In the CLI

To configure VLAN settings for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# switchport-mode {trunk|access}
(Instant AP)(wired ap profile <name>)# allowed-vlan <vlan>
(Instant AP)(wired ap profile <name>)# native-vlan {<guest|1…4095>}
```

To configure a new VLAN assignment rule:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# set-vlan <attribute>{equals|not-equals|starts-
with|  ends-with|contains| matches-regular-expression} <operator> <VLAN-ID>|value-of}
```

Configuring Security Settings for a Wired Profile



If you are creating a new wired profile, complete the Wired Settings and VLAN procedures before specifying the security settings. For more information, see Configuring Wired Settings on page 161 and Configuring VLAN Settings for a WLAN SSID Profile on page 136.

Configuring Security Settings for a Wired Employee Network

You can configure security parameters for the Employee network by using the Instant WebUI or the CLI.

To configure security parameters for the Employee network:

1. Configure the following parameters in the **Security** tab.

   Port type—To support trusted ports in an Instant AP, select **Trusted**. When the Port type is trusted, MAC and 802.1X authentication parameters cannot be configured. The Port Type is **Untrusted** by default.

   In a trusted mode, Instant APs will not create any user entry. A predefined ACL is applied to the trusted port in order to control the client traffic that needs to be source NATed.

   - **MAC authentication**—To enable MAC authentication, select **Enabled**. The MAC authentication is disabled by default.
   - **802.1X authentication**—To enable 802.1X authentication, select **Enabled**. The 802.1X authentication is disabled by default.
   - **MAC authentication fail-thru**—To enable authentication fail-thru, select **Enabled**. When this feature is enabled, 802.1X authentication is attempted when MAC authentication fails. The **MAC authentication fail-thru** check box is displayed only when both **MAC authentication** and **802.1X authentication** are **Enabled**.

   Select any of the following options for **Authentication server 1**:

- **New**—On selecting this option, an external RADIUS server must be configured to authenticate the users. For information on configuring an external server, see External RADIUS Server on page 231.Authentication and User Management on page 207
- **Internal server**— If an internal server is selected, add the clients that are required to authenticate with the internal RADIUS server. Click the **Users** link to add users. For information on adding a user, see Overview of Instant AP Users on page 207.

Accounting—Select any of the following options:

- **Disabled**—Disables accounting.
- **Use authentication servers**—When selected, the authentication servers configured for the wired profile are used for accounting purposes.
- **Use separate servers**—Allows you to configure separate accounting servers.
- **Accounting interval**—Allows you set an accounting interval within the range of 0–60 minutes for sending interim accounting information to the RADIUS server.
- **Reauth interval**—Specify the interval at which all associated and authenticated clients must be reauthenticated.

Load balancing—Set this to **Enabled** if you are using two RADIUS authentication servers, so that the load across the two RADIUS servers is balanced. For more information on the dynamic load balancing mechanism, see Dynamic Load Balancing between Two Authentication Servers on page 230.



- The **Accounting** parameter does not appear if the **Internal server** option is selected as the authentication server.

2. Click **Next**. The **Access** tab details are displayed.

To configure security parameters for the Employee network:

1. Configure the following parameters in the **Configuration** > **Networks** > **Security** tab.

   Port type—To support trusted ports in an Instant AP, select **Trusted**. When the Port type is trusted, MAC and 802.1X authentication parameters cannot be configured. The Port Type is **Untrusted** by default.

   In a trusted mode, Instant APs will not create any user entry. A predefined ACL is applied to the trusted port in order to control the client traffic that needs to be source NATed.

   - **MAC authentication**—Click the toggle switch to enable MAC authentication. The MAC authentication is disabled by default.
   - **802.1X authentication**—Click the toggle switch to enable 802.1X authentication. The 802.1X authentication is disabled by default.
   - **MAC authentication fail-thru**—Click the toggle switch to enable authentication fail-thru. When this feature is enabled, 802.1X authentication is attempted when MAC authentication fails. The **MAC authentication fail-thru** option is displayed only when both **MAC authentication** and **802.1X authentication** parameters are enabled.

   Select an existing RADIUS authentication server or **+** in the **Authentication server 1** drop-down list. When**+** is selected, an external RADIUS server must be configured to authenticate the users. For information on configuring an external server, see External RADIUS Server on page 231.Authentication and User Management on page 207

- **Internal server**— If an internal server is selected, add the clients that are required to authenticate with the internal RADIUS server. Click the **Users** link to add users. For information on adding a user, see Overview of Instant AP Users on page 207.

Accounting—Select any of the following options.

- **Disabled**—Disables accounting.
- **Use authentication servers**—When selected, the authentication servers configured for the wired profile are used for accounting purposes.
- **Use separate servers**—Allows you to configure separate accounting servers.
- **Accounting interval**—Allows you set an accounting interval within the range of 0–60 minutes for sending interim accounting information to the RADIUS server.
- **Reauth interval**—Specify the interval at which all associated and authenticated clients must be reauthenticated.

Load balancing—Click the toggle switch if you are using two RADIUS authentication servers, so that the load across the two RADIUS servers is balanced. For more information on the dynamic load balancing mechanism, see Dynamic Load Balancing between Two Authentication Servers on page 230



The **Accounting** parameter does not appear if the **Internal server**option is selected as the authentication server.

2. Click **Next**. The **Access** tab details are displayed.

To configure security settings for an employee network:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# mac-authentication
(Instant AP)(wired ap profile <name>)# l2-auth-failthrough
(Instant AP)(wired ap profile <name>)# auth-server <name>
(Instant AP)(wired ap profile <name>)# server-load-balancing
(Instant AP)(wired ap profile <name>)# radius-accounting
(Instant AP)(wired ap profile <name>)# radius-accounting-mode {user-association|user-
authentication}
(Instant AP)(wired ap profile <name>)# radius-interim-accounting-interval <minutes>
(Instant AP)(wired ap profile <name>)# radius-reauth-interval <Minutes>
(Instant AP)(wired ap profile <name>)# trusted
```

Configuring Access Rules for a Wired Profile

The Ethernet ports allow third-party devices such as VoIP phones or printers (that support only wired connections) to connect to the wireless network. You can also configure an ACL for additional security on the Ethernet downlink.



If you are creating a new wired profile, complete the Wired Settings and configure the VLAN and security parameters before defining access rules. For more information, see Configuring Wired Settings on page 161, Configuring VLAN for a Wired Profile on page 163, and In the Old WebUI on page 165.

You can configure access rules by using the Instant WebUI or the CLI.

In the Old WebUI

To configure access rules:

1. On the **Access** tab, configure the following access rule parameters.
   a. Select any of the following types of access control:
      - **Role-based**—Allows the users to obtain access based on the roles assigned to them.
      - **Network-based**—Allows the users to be authenticated based on access rules specified for a network.
      - **Unrestricted**—Allows the users to obtain unrestricted access on the port.
   b. If the **Role-based** access control is selected, perform the following steps:
      - Under **Roles**, select an existing role for which you want to apply the access rules, or click **New** and add the required role. The list of roles defined for all networks is displayed under **Roles**.



The default role with the same name as the network is automatically defined for each network. The default roles cannot be modified or deleted.

   - Select the access rule associated with a specific role and modify if required. To add a new access rule, click **New** in the **Access Rules** window. You can configure up to 64 access rules. For more information on configuring access rules, see Configuring ACL Rules for Network Services on page 260.
   - Configure rules to assign roles for an authenticated client. You can also configure rules to derive VLANs for the wired network profile. For more information on role assignment rules and VLAN derivation rules, see Configuring Derivation Rules on page 282 and Configuring VLAN Derivation Rules on page 288.
   - Select the **Assign pre-authentication role** check box to add a pre-authentication role that allows some access to the users before client authentication.
   - Select the **Enforce Machine Authentication** check box, to configure access rights to clients based on whether the client device supports machine authentication. Select the **Machine auth only** and **User auth only** rules. Machine Authentication is only supported on Windows devices and devices such as iPads.



If **Enforce Machine Authentication** is enabled, both the device and the user must be authenticated for the role assignment rule to apply.

2. Click **Finish**.

In the New WebUI

To configure access rules:

1. In the **Access** tab, configure the following access rule parameters.
   a. In the **Access Rules** drop-down list box, select any of the following types of access control:
      - **Role-based**—Allows the users to obtain access based on the roles assigned to them.
      - **Network-based**—Allows the users to be authenticated based on access rules specified for a network.
      - **Unrestricted**—Allows the users to obtain unrestricted access on the port.
   b. If the **Role-based** access control is selected, perform the following steps:

- Under **Roles**, select an existing role for which you want to apply the access rules, or click **+** and add the required role. The list of roles defined for all networks is displayed under **Roles**.



The default role with the same name as the network is automatically defined for each network. The default roles cannot be modified or deleted.

- Select the access rule associated with a specific role and modify if required. To add a new access rule, click **+** in the **Access Rules for <network>** window. You can configure up to 64 access rules. For more information on configuring access rules, see Configuring ACL Rules for Network Services on page 260.
- Configure rules to assign roles for an authenticated client. You can also configure rules to derive VLANs for the wired network profile. For more information on role assignment rules and VLAN derivation rules, see Configuring Derivation Rules on page 282 and Configuring VLAN Derivation Rules on page 288.
- In the **Role Assignment Rules** window, click the **Enforce Machine Authentication** toggle switch to configure access rights to clients based on whether the client device supports machine authentication. Select the **Machine auth only** and **User auth only** rules. Machine Authentication is only supported on Windows devices and devices such as iPads.
- Toggle the **Enforce MAC auth only role** switch to specify roles for only MAC authenticated users.



If **Enforce Machine Authentication** is enabled, both the device and the user must be authenticated for the role assignment rule to apply.

2. Click **Next**.
3. In the **Assignment** tab, click **Finish**. For more information, refer to Assigning a Profile to Ethernet Ports on page 170

In the CLI

To configure access rules for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# access-rule-name <name>
```

To configure role assignment rules:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# set-role <attribute>{{equals|not-equal|starts-
with| ends-with|contains|matches-regular-expression}<operator> <role>|value-of}
```

To configure a pre-authentication role:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# set-role-pre-auth <role>
```

To configure machine and user authentication roles:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# set-role-machine-auth  <machine_only>  <user-
only>
```

To configure unrestricted access:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# set-role-unrestricted
```

Assigning a Profile to Ethernet Ports

You can assign profiles to Ethernet ports using the Instant WebUI or the CLI:

In the Old WebUI

To assign wired profiles to Ethernet ports:

1. Click the **Wired** link under **More** on the Instant main window. The **Wired** window is displayed.
2. To assign an Ethernet downlink profile to Ethernet 0 port:
   a. Ensure that the wired bridging on the port is enabled. For more information, see Configuring Wired Bridging on Ethernet 0 for Mesh Point on page 479.
   b. Under **Network assignments**, select and assign a profile from the **0/0** drop-down list.
   c. To assign a wired profile to Ethernet 0/1 port, select the profile from the **0/1** drop-down list.
   d. If the Instant AP supports Ethernet 2, Ethernet 3, and Ethernet 4 ports, assign profiles to other Ethernet ports by selecting a profile from the **0/2**, **0/3**, and **0/4** drop-down lists.
   e. Click **OK**.

In the New WebUI

To assign wired profiles to Ethernet ports:

1. Navigate to the **Configuration** > **Networks** page.
2. Select the wired network profile to which you want to assign Ethernet ports and click **Edit**.
3. Go to the **Assignment** tab.
4. To assign an Ethernet downlink profile to Ethernet 0 port:
   a. Ensure that the wired bridging on the port is enabled. For more information, see Configuring Wired Bridging on Ethernet 0 for Mesh Point on page 479.
   b. Select and assign a profile from the **0/0** drop-down list.
   c. To assign a wired profile to Ethernet 0/1 port, select the profile from the **0/1** drop-down list.
   d. If the Instant AP supports Ethernet 2, Ethernet 3, and Ethernet 4 ports, assign profiles to other Ethernet ports by selecting a profile from the **0/2**, **0/3**, and **0/4** drop-down lists.
5. Click **Finish**.

In the CLI

To assign profiles to Ethernet ports:

```
(Instant AP)(config)# enet0-port-profile <name>
(Instant AP)(config)# enet1-port-profile <name>
(Instant AP)(config)# enet2-port-profile <name>
(Instant AP)(config)# enet3-port-profile <name>
(Instant AP)(config)# enet4-port-profile <name>
```

Enabling 802.3az Energy Efficient Ethernet Standard

Most new models of Aruba APs support the 802.3az or Energy Efficient Ethernet standard, which allows the APs to consume less power during periods of low data activity. This setting can be enabled for provisioned Instant APs or Instant AP groups through the wired port profile. After enabling EEE, the wired port profile can be linked individually to the ethernet ports. If this feature is enabled for an Instant AP group, any Instant APs in the group that do not support 802.3az will ignore this setting.



802.3az or EEE is not supported on AP-315, and 330 Series access points.

In the CLI

To enable 802.3az Energy Efficient Ethernet standard on an Instant AP and associate it with an ethernet port:

```
(Instant AP)(config)# wired-port-profile <profile_name>
(Instant AP)(wired ap profile <profile_name>)# dot3az
(Instant AP)(wired ap profile <profile_name>)# exit
(Instant AP)(config)# enet0-port-profile <profile_name>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

To view the dot3az status for the ethernet ports:

```
(Instant AP)# show port status
Port Status
-----------
Port  Type  Admin-State  Oper-State  STP-State  Dot3az
----  ----  -----------  ----------  ---------  ------
eth0  5GE   up           up          N/A        Enable
eth1  GE    up           down        N/A        Disable
```

Editing a Wired Profile

You can edit a wired profile by using the Instant WebUI.

In the Old WebUI

To edit a wired profile:

1. Click the **Wired** link under **More** on the Instant main window. The **Wired** window is displayed.
2. In the **Wired Networks** window, select the wired profile to modify.
3. Click **Edit**. The **Edit Wired Network** window is displayed.
4. Modify the required settings.
5. In the **Access** tab, click **Finish** to save the modifications.

In the New WebUI

To edit a wired profile:

1. Navigate to the **Configuration** > **Networks** page.
2. Under Networks, select the wired profile and click **Edit**.
3. Modify the required settings under the respective tabs.
4. Click **Next** until **Finish** to save the modifications.

Deleting a Wired Profile

You can delete a wired profile by using the Instant WebUI.

In the Old WebUI

To delete a wired profile:

1. Click the **Wired** link under **More** on the Instant main window. The **Wired** window is displayed.
2. In the **Wired** window, select the wired profile to delete.
3. Click **Delete**. The wired profile will be deleted.

In the New WebUI

To delete a wired profile:

1. Navigate to the **Configuration** > **Networks** page.
2. Under **Networks**, select the wired profile to delete and click **Delete**.
3. Click **Delete Now** to confirm deletion.

LACP

LACP provides a standardized means for exchanging information with a partner system by forming a dynamic LAG and increasing the bandwidth of the connection. The LACP feature is automatically enabled on the Instant AP during boot when connected to a partner system with LACP enabled. The Instant AP dynamically detects the LACP configuration by checking if any LACP PDU packet is received on the Ethernet interface from the partner system. LACP is supported on 802.11ac and 802.11ax access points with two Ethernet ports and is based on the IEEE standard 802.3ad.

If a controller in the cluster has the LACP capability, the Ethernet 0 and Ethernet 1 interfaces of the access point can be combined using LAG to form a single logical interface (port-channel). Port-channels can be used to increase bandwidth or configure link redundancy between the two devices. Instant APs support link aggregation using either standard port-channel (configuration based) or LACP (protocol signaling based). You can deploy supported access points with LACP to utilize the high throughput (greater than 1 Gbps) capabilities of the AP radios.



To configure LACP, connect only the eth0 port of the Access Point to the controller. Allow the AP to receive its full configuration , reboot the AP and then connect the eth1 port. This is because the eth1 port of 320 Series, 330 Series, 340 Series, 510 Series, 530 Series, and 550 Series access points is a downlink port by default.

320 Series, 330 Series, 340 Series, 510 Series, 530 Series and 550 Series access points support this feature.

Enabling Port-Channel on a Switch

1. Creating a port-channel and applying a switching-profile to a port-channel Profile:

```
(host) (config) #interface port-channel <0-63>
(host) (port-channel "1") #switching-profile <profile name>
```

2. Creating and Applying a Dynamic Port-Channel Profile to an Interface:

```
(host)(config)# interface-profile lacp-profile <profile-name>
```

```
group-id <0-63>
mode active
(host)(config)# interface gigabitethernet <slot/module/port>
lacp-profile <profile-name>
```

Verifying LACP Configuration on the Instant AP

There is no configuration required on the Instant AP for enabling LACP support. However, you can view the status of LACP on Instant APs by using the following command:

```
(Instant AP)# show lacp status
AP LACP Status
--------------
Link Status  LACP Rate  Num Ports  Actor Key  Partner Key  Partner MAC
-----------  ---------  ---------  ---------  -----------  -----------
Up           slow       2          17         3            00:1a:1e:1e:8c:40
Slave Interface Status
----------------------
Slave I/f Name  Permanent MAC Addr  Link Status  Member of LAG  Link Fail Count
--------------  ------------------  -----------  -------------  ---------------
eth0            70:3a:0e:cd:5e:d6   Up           Yes            1
eth1            70:3a:0e:cd:5e:d7   Up           Yes            1
```

Enabling Static LACP Configuration

Instant APs support dynamic LACP configuration managed by the partner device. When the partner device is LACP enabled, the AP inherits LACP configurations from the partner device and establishes the connection. LACP can also be configured to be managed by the AP by configuring static LACP. If static LACP is configured, the AP will boot with this LACP configuration.

To enable or disable static LACP configuration, use the following commands in the CLI:

To enable the static LACP mode on Instant APs:

```
(Instant AP)# lacp-mode enable
```

To disable the static LACP mode on Instant APs:

```
(Instant AP)# lacp-mode disable
```

Verifying Static LACP Mode

To verify the static LACP configuration, execute the following command in the Instant AP CLI:

```
(Instant AP)# show ap-env
Antenna Type:Internal
name:TechPubsAP
per_ap_ssid:1234
per_ap_vlan:abc
lacp_mode:enable
```

Understanding Hierarchical Deployment

An Instant AP with more than one wired port can be connected to the downlink wired port of another Instant AP. An Instant AP with a single Ethernet port can be provisioned to use Ethernet bridging, so that Ethernet 0 port is converted to a downlink wired port.

You can also form an Instant AP network by connecting the downlink port of an Instant AP to other Instant APs. Only one Instant AP in the network uses its downlink port to connect to the other Instant APs. This Instant AP (called the root Instant AP) acts as the wired device for the network, provides DHCP service and an L3 connection to the ISP uplink with NAT. The root Instant AP is always the master of the

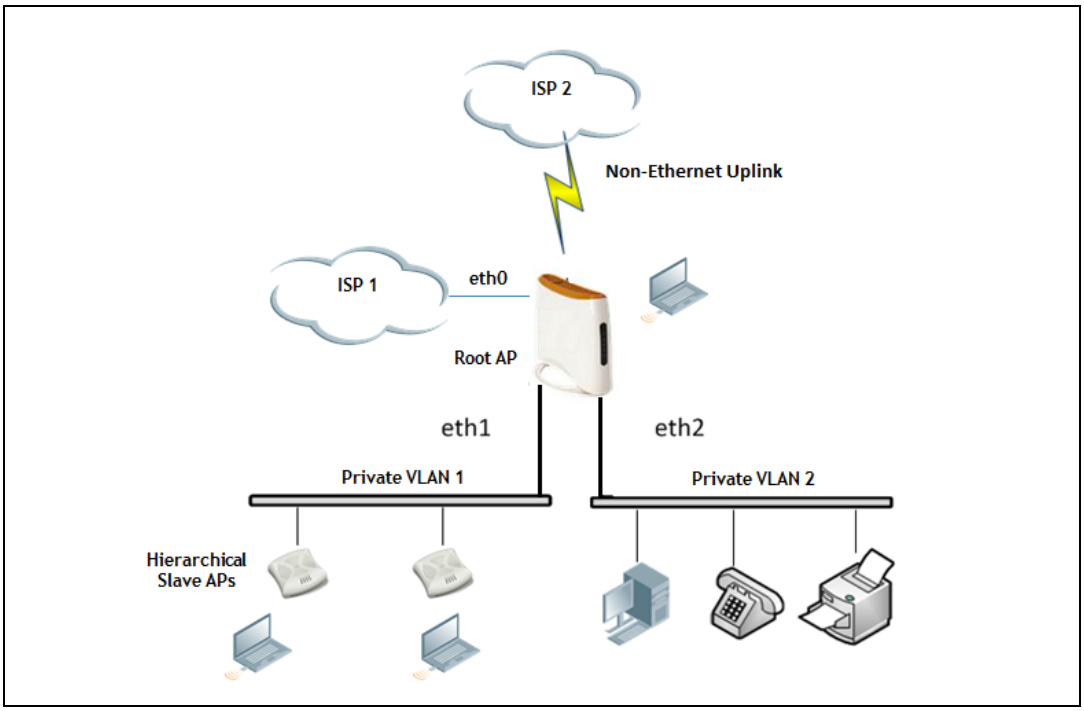
Instant network. In a single Ethernet port platform deployment, the root Instant AP must be configured to use the 3G uplink.

A typical hierarchical deployment consists of the following:

- A direct wired ISP connection or a wireless uplink.
- One or more DHCP pools for private VLANs.
- One downlink port configured on a private VLAN without authentication for connecting to slave Instant APs. Ensure that the downlink port configured in a private VLAN is not used for any wired client connection. Other downlink ports can be used for connecting to the wired clients.

The following figure illustrates a hierarchical deployment scenario:

Figure 4 *Hierarchical Deployment*



Loop Protection

Aruba Instant 8.4.0.0 introduces the loop protection feature that detects and avoids the formation of loops on the Ethernet ports of an Instant AP.

The loop protect feature can be enabled on all Instant APs that have multiple Ethernet ports and it supports tunnel, split-tunnel, and bridge modes.

The loop protection feature prevents the formation of loops when:

- An unmanaged switch is connected to one port of an Instant AP and a loop forms in the unmanaged switch.
- The WAN port (port 0) and either of ports 1, 2, 3, or 4, if it exists, in an AP are connected to the same switch.
- Multiple ports in an Instant AP are connected to an unmanaged switch.

The loop protection feature transmits a proprietary loop detection packet on one Ethernet port of an Instant AP at the configured loop-protect interval (default value is 2 seconds). The loop protect feature transmits the loop detection packet without a VLAN tag irrespective of whether the Ethernet port of the

Instant AP is connected in access mode or trunk mode. That is, for trunk mode, loop protect is supported only in the native VLAN.

- If the same packet is received on the same Ethernet port of the Instant AP, a loop in the downstream switch is detected and the Ethernet port of the Instant AP is shut down.
- If the same packet is received on the WAN port (port 0) of the Instant AP, a loop between the Ethernet and WAN ports of the AP is detected and the Ethernet port of the Instant AP is shut down.
- If the same packet is received on another Ethernet port of the Instant AP, a loop between the Ethernet ports of the Instant AP is detected and the Ethernet port of the Instant AP port with lower priority is shut down. The Ethernet port with smaller port ID has high priority.

The Ethernet port of the Instant AP that is shut down because of loop protection is marked with status **Loop-ERR**. A user can either the recover the shut down port from the Instant AP with manual intervention or enable automatic recovery mode and configure a automatic recovery interval. At the expiry of the automatic recovery interval, the **Loop-ERR** status of the Ethernet port is cleared and the Ethernet port is re-enabled automatically.

To prevent the downstream switch from dropping the loop detection packet, for example during broadcast storm state, if the Instant AP takes longer time, or if the Instant AP fails to detect a loop, a broadcast storm-control mechanism is provided as part of the loop protection feature. During broadcast-storm control, an Instant AP counts the broadcast packets received on each of its Ethernet port and determines the packet rate in an interval. If the broadcast packet rate on one Ethernet port exceeds the configured threshold (default value is 2000 packets per second), the Ethernet port is shut down.

Configuring Loop Protection

In the CLI

To configure loop protection for the wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# loop-protect
(Instant AP)(wired ap profile <name>)# loop-detection-interval 5
```

To configure automatic recovery for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# auto-recovery
(Instant AP)(wired ap profile <name>)# auto-recovery-interval 50
```

To configure broadcast storm control:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# storm-control-broadcast
(Instant AP)(wired ap profile <name>)# storm-control-threshold 110
```

Chapter 13
Captive Portal for Guest Access

This chapter provides the following information:

- Understanding Captive Portal on page 176
- Configuring a WLAN SSID for Guest Access on page 177
- Configuring Wired Profile for Guest Access on page 183
- IGMP on page 186
- Configuring Internal Captive Portal for Guest Network on page 186
- Configuring External Captive Portal for a Guest Network on page 189
- Configuring Facebook Login on page 196
- Configuring Guest Logon Role and Access Rules for Guest Users on page 198
- Configuring Captive Portal Roles for an SSID on page 200
- Configuring Walled Garden Access on page 202
- Disabling Captive Portal Authentication on page 203
- Configuring Facebook Express Wi-Fi on page 203

Understanding Captive Portal

Instant supports the captive portal authentication method, where a web page is presented to the guest users when they try to access the Internet from hotels, conference centers, or Wi-Fi hotspots. The web page also prompts the guest users to authenticate or accept the usage policy and terms. Captive portals are used at many Wi-Fi hotspots and can be used to control wired access as well.

The Instant captive portal solution consists of the following:

- The captive portal web login page hosted by an internal or external server.
- The RADIUS authentication or user authentication against Instant AP's internal database.
- The SSID broadcast by the Instant AP.

Using Instant, the administrators can create a wired or WLAN guest network based on captive portal authentication for guests, visitors, contractors, and any non-employee users who can use the enterprise Wi-Fi network. The administrators can also create guest accounts and customize the captive portal page with organization-specific logo, terms, and usage policy. With captive portal authentication and guest profiles, the devices that connect to the guest SSID are assigned IP addresses and an initial role. When a guest user tries to access a URL through HTTP or HTTPS, the captive portal web page prompting the user to authenticate with a username and password is displayed.

Types of Captive Portal

Instant supports the following types of captive portal authentication:

- **Internal captive portal**—For Internal captive portal authentication, an internal server is used for hosting the captive portal service. It supports the following types of authentication:

- **Internal Authenticated**—When **Internal Authenticated** is enabled, a guest user must authenticate in the captive portal page to access the Internet. The guest users who are required to authenticate must already be added to the user database.
- **Internal Acknowledged**—When **Internal Acknowledged** is enabled, a guest user must accept the terms and conditions to access the Internet.

- **External captive portal**—For external captive portal authentication, an external portal on the cloud or on a server outside the enterprise network is used.

Walled Garden

The administrators can also control the resources that the guest users can access and the amount of bandwidth or airtime they can use at any given time. When an external captive portal is used, the administrators can configure a walled garden, which determines access to the URLs requested by the guest users. For example, a hotel environment where the unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents. The users who do not sign up for the Internet service can view only the “allowed” websites (typically hotel property websites).

The administrators can allow or block access to specific URLs by creating a whitelist and blacklist. When the users attempt to navigate to other websites, which are not in the whitelist of the walled garden profile, the users are redirected to the login page. If the requested URL is on the blacklist, it is blocked. If it appears on neither list, the request is redirected to the external captive portal.

Configuring a WLAN SSID for Guest Access

The following procedure describes how to configure a WLAN Guest SSID:

Table 55: *Steps to Configure WLAN Guest SSID*

New WebUI	Old WebUI
To create an SSID for guest access: 1. Navigate to the **Configuration** > **Networks** page. 2. Under **Networks**, click **+**. 3. Under Basic option, Enter a name that uniquely identifies a wireless network in the **Name** field. **NOTE:** The SSID name must be unique and may contain any special character except for **'** and **".** 1. In the **Type** drop-down list, select **Wireless.** 2. In the **Primary usage** drop-down menu, select **Guest**. 3. Click the **Show advanced options** link. The advanced options for configuration are displayed.	To create an SSID for guest access: 1. In the **Networks** tab of the Instant main window, click the **New** link. The **New WLAN** window is displayed. 2. Enter a name that uniquely identifies a wireless network in the **Name (SSID)** text box. 3. Select **Guest** from the **Primary usage** drop-down menu. 4. Click the **Show advanced options** link. The advanced options for configuration are displayed.

Enter the required values for the following configuration parameters:

Table 56: *WLAN Configuration Parameters*

Parameter	Description
Broadcast filtering	Select any of the following values:

Table 56: *WLAN Configuration Parameters*

Parameter	Description
	▪ **All**—When set to **All**, the Instant AP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. ▪ **ARP**—When set to **ARP**, the Instant AP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols and additionally converts ARP requests to unicast and send frames directly to the associated client. ▪ **Unicast-ARP-Only** — When set to **Unicast-ARP-Only**, the Instant AP allows all broadcast and multicast frames as it is, however the ARP requests are converted to unicast frames and sends them to the associated clients. The broadcast filtering is set to **Unicast-ARP-Only** by default when an SSID profile is created. ▪ **Disabled**— When set to **Disabled**, all broadcast and multicast traffic is forwarded to the wireless interfaces.
Multicast transmission optimization	Select **Enabled** if you want the Instant AP to select the optimal rate for sending 802.11 broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When this option is enabled, multicast traffic can be sent at up to 24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and 5 GHz is 6 Mbps. This option is disabled by default.
Dynamic multicast optimization	Select **Enabled** to allow Instant AP to convert multicast streams into unicast streams over the wireless link. Enabling DMO enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. **NOTE:** When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.
DMO channel utilization threshold	Specify a value to set a threshold for DMO channel utilization. With DMO, the Instant AP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90% and the maximum threshold value is 100%. When the threshold is reached or exceeds the maximum value, the Instant AP sends multicast traffic over the wireless link.
Transmit Rates	Specify the following parameters: ▪ **2.4 GHz**—If the 2.4 GHz band is configured on the Instant AP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps. ▪ **5 GHz**—If the 5 GHz band is configured on the Instant AP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps.
Band	Select a value to specify the band at which the network transmits radio signals. You can set the band to **2.4 GHz**, **5 GHz**, or **All**. The **All** option is selected by default.
DTIM interval	The **DTIM interval** indicates the DTIM period in beacons, which can be configured for every WLAN SSID profile. The DTIM interval determines how often the Instant AP should deliver the buffered broadcast and multicast frames to associated clients in the powersave mode. The default value is 1 beacon, which means the client checks for buffered data on the Instant AP at every beacon. You can also configure a higher DTIM value for power saving.

Table 56: *WLAN Configuration Parameters*

Parameter	Description
Min RSSI for probe request	Sets a minimum RSSI threshold for probe requests.
Min RSSI for auth request	Sets a minimum RSSI threshold for authentication requests.
High Throughput	Disables/ Enables 802.11n high throughput functionality. Disabling **High Throughput** automatically disables **Very High Throughput** and **High Efficiency** modes. High throughput settings are applied only to the respective SSID. Disable **High Throughput** on the SSID to service 802.11a and 802.11g only legacy clients. Enabled by default.
Very high throughput	Enables VHT function on Instant AP devices that support VHT. For 802.11ac Instant APs, the VHT function is enabled by default. However, you can disable the VHT function if you want the 802.11ac Instant APs to function as 802.11n Instant APs. If VHT is configured or disabled on an SSID, the changes will apply only to the SSID on which it is enabled or disabled.
Zone	Specify the zone for the SSID. When the zone is defined in SSID profile and if the same zone is defined on an Instant AP, the SSID is created on that Instant AP. For more information on configuring zone details, see Configuring Zone Settings on an Instant AP on page 84. The following constraints apply to the zone configuration: ▪ An Instant AP can belong to only one zone and only one zone can be configured on an SSID. ▪ If an SSID belongs to a zone, all Instant APs in this zone can broadcast this SSID. If no Instant AP belongs to the zone configured on the SSID, the SSID is not broadcast. ▪ If an SSID does not belong to any zone, all Instant APs can broadcast this SSID.
Time Range	Click **Edit**, select a Time Range Profile from the list and specify if the profile must be enabled or disabled for the SSID, and then click **OK**.
Bandwidth Limits	Under **Bandwidth Limits**: ▪ **Airtime**—Select this check box and specify an aggregate amount of airtime that all clients in this network can use for sending and receiving data. Specify the airtime percentage. ▪ **Each radio**—Select this check box to specify an aggregate amount of throughput that each radio is allowed to provide for the connected clients. ▪ **Downstream** and **Upstream**—Specify the downstream and upstream rates within a range of 1 to 65,535 Kbps for the SSID users. If the assignment is specific for each user, select the **Peruser** check box.
WMM	Configure the following options for WMM traffic management. WMM supports voice, video, best effort, and background access categories. To allocate bandwidth for the following types of traffic, specify a percentage value under **Share**. To configure DSCP mapping, specify a value under **DSCP Mapping**. ▪ **Background WMM**—For background traffic such as file downloads or print jobs. ▪ **Best effort WMM**—For best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS.

Table 56: *WLAN Configuration Parameters*

Parameter	Description
	▪ **Video WMM**—For video traffic generated from video streaming. ▪ **Voice WMM**— For voice traffic generated from the incoming and outgoing voice communication. For more information on WMM traffic and DSCP mapping, see WMM Traffic Management on page 391
	For voice traffic and Spectralink Voice Prioritization, configure the following parameters: ▪ **Traffic Specification (TSPEC)**—To prioritize time-sensitive traffic such as voice traffic initiated by the client, select the **Traffic Specification (TSPEC)** check box. ▪ **TSPEC Bandwidth**—To reserve bandwidth, set the TPSEC bandwidth to the desired value within the range of 200–600,000 Kbps. The default value is 2000 Kbps. ▪ **Spectralink Voice Protocol (SVP)**—Select the check box to prioritize voice traffic for SVP handsets.
Content filtering	Select **Enabled** to route all DNS requests for the non-corporate domains to the configured DNS on this network.
Inactivity timeout	Specify an interval for session timeout in seconds, minutes or hours. If a client session is inactive for the specified duration, the session expires and the users are required to log in again. You can specify a value within the range of 60-86,400 seconds or up to 24 hours for a client session. The default value is 1000 seconds.
Deauth Inactive Clients	Select **Enabled** to allow the Instant AP to send a deauthentication frame to the inactive client and clear client entry.
SSID	Select the **Hide** check box if you do not want the SSID (network name) to be visible to users. Select the **Disable** check box if you want to disable the SSID. On selecting this, the SSID will be disabled, but will not be removed from the network. By default, all SSIDs are enabled.
ESSID	Enter the ESSID. If the value defined for ESSID value is not the same as profile name, the SSIDs can be searched based on the ESSID value and not by its profile name.
Out of service (OOS)	Configures the SSID state when a connection link of the AP is down. To configure out of service for an SSID, the link condition of the AP and the SSID state should be configured. The SSID can be enabled or disabled automatically when the following conditions are met: ▪ **VPN down** - Connection to the VPN network is down. ▪ **Uplink down** - The uplink connection of the AP is down. ▪ **Internet down** - The connection to the Internet is down. ▪ **Primary uplink down** - The primary uplink connection of the AP is down. The SSID status will change according to the configuration when the link condition is met. For example, when **Internet down**, **Disabled** is set for **Out of Service**, the SSID will be disabled when the Internet connection is down and change back to enabled when the Internet connection is restored. **NOTE:** When **Internet Down** condition is set in the SSID, the Instant AP will check for uplink by pinging the IP defined in the Internet Failover IP. To configure the Internet Failover IP, seeUplink Preferences and Switching.

Table 56: *WLAN Configuration Parameters*

Parameter	Description
OOS time (global)	Configure a hold time interval in seconds within a range of 30 to 300 seconds, after which the out-of-service operation is triggered. For example, if the VPN is down and the configured hold time is 45 seconds, the effect of this out-of-service state impacts the SSID availability after 45 seconds.
Max clients threshold	Specify the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value within the range of 0 to 255. The default value is 64.
SSID Encoding	To encode the SSID, select UTF8. By default, the SSIDs are not encoded.
Deny inter user bridging	When enabled, the bridging traffic between two clients connected to the same SSID on the same VLAN is disabled. The clients can connect to the Internet, but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision.
Openflow	When enabled, users can run and manage multiple instances of the control-plane and dataplane from a centralized location. OpenFlow also ensures uniform policy enforcement.

Click **Next** to configure VLAN settings. The VLAN tab contents are displayed.

1. Select any for the following options for **Client IP assignment**:
   - **Virtual Controller managed**—On selecting this option, the client obtains the IP address from the virtual controller. When this option is used, the source IP address is translated to the physical IP address of the master Instant AP for all client traffic that goes through this interface. The virtual controller can also assign a guest VLAN to the client.
   - **Network assigned**—On selecting this option, the IP address is obtained from the network.
2. Based on the type client IP assignment mode selected, you can configure the VLAN assignment for clients as described in the following table:

Table 57: *IP and VLAN Assignment for WLAN SSID Clients*

Client IP Assignment	Client VLAN Assignment
Virtual Controller managed	If the **Virtual Controller managed** is selected for client IP assignment, the virtual controller creates a private subnet and VLAN on the Instant AP for the wireless clients. The NAT for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network. On selecting this option, the following client VLAN assignment options are displayed: ▪ **Default**: When selected, the default VLAN as determined by the virtual controller is assigned for clients. ▪ **Custom**: When selected, you can specify a custom VLAN assignment option. You can select an existing DHCP scope for client IP and VLAN assignment or you can create a new DHCP scope by selecting **New**. For more information on DHCP scopes, see Configuring DHCP Scopes on page 294.
Network assigned	If the **Network assigned** is selected, you can specify any of the following options for the **Client VLAN assignment**. ▪ **Default**—On selecting this option, the client obtains the IP address in the same

Table 57: *IP and VLAN Assignment for WLAN SSID Clients*

Client IP Assignment	Client VLAN Assignment
	subnet as the Instant APs. By default, the client VLAN is assigned to the native VLAN on the wired network. ■ **Static**—On selecting this option, you need to specify a single VLAN, a comma separated list of VLANS, or a range of VLANs for all clients on this network. Select this option for configuring VLAN pooling. ■ **Dynamic**—On selecting this option, you can assign the VLANs dynamically from a DHCP server. To create VLAN assignment rules, click **New** to assign the user to a VLAN. In the **New VLAN Assignment Rule** window, enter the following information: • **Attribute**—Select an attribute returned by the RADIUS server during authentication. • **Operator**—Select an operator for matching the string. • **String**—Enter the string to match • **VLAN**—Enter the VLAN to be assigned.

3. Click **Next** to configure internal or external captive portal authentication, roles, and access rules for the guest users.



If the client IP assignment mode is set to **Network assigned** in a guest SSID profile, the guest clients can log out of the captive portal network by accessing the https://securelogin.arubanetworks.com/auth/logout.html URL.

The following CLI commands configure the WLAN settings for an WLAN SSID guest profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# essid <ESSID-name>
(Instant AP)(SSID Profile <name>)# type <Guest>
(Instant AP)(SSID Profile <name>)# broadcast-filter <type>
(Instant AP)(SSID Profile <name>)# dtim-period <number-of-beacons>
(Instant AP)(SSID Profile <name>)# multicast-rate-optimization
(Instant AP)(SSID Profile <name>)# dynamic-multicast-optimization
(Instant AP)(SSID Profile <name>)# dmo-channel-utilization-threshold
(Instant AP)(SSID Profile <name>)# a-max-tx-rate <rate>
(Instant AP)(SSID Profile <name>)# a-min-tx-rate <rate>
(Instant AP)(SSID Profile <name>)# g-max-tx-rate <rate>
(Instant AP)(SSID Profile <name>)# g-min-tx-rate <rate>
(Instant AP)(SSID Profile <name>)# zone <zone>
(Instant AP)(SSID Profile <name>)# bandwidth-limit <limit>
(Instant AP)(SSID Profile <name>)# per-user-bandwidth-limit <limit>
(Instant AP)(SSID Profile <name>)# air-time-limit <limit>
(Instant AP)(SSID Profile <name>)# wmm-background-share <percentage-of-traffic_share>
(Instant AP)(SSID Profile <name>)# wmm-best-effort-share<percentage-of-traffic-share>
(Instant AP)(SSID Profile <name>)# wmm-video-share <percentage-of-traffic_share>
(Instant AP)(SSID Profile <name>)# wmm-voice-share <percentage-of-traffic_share>
(Instant AP)(SSID Profile <name>)# rf-band {<2.4>|<5.0>|<all>}
(Instant AP)(SSID Profile <name>)# content-filtering
(Instant AP)(SSID Profile <name>)# hide-ssid
(Instant AP)(SSID Profile <name>)# inactivity-timeout <interval>
(Instant AP)(SSID Profile <name>)# local-probe-req-thresh <threshold>
(Instant AP)(SSID Profile <name>)# max-clients-threshold <number-of-clients>
```

The following CLI command manually assigns a VLAN for WLAN SSID users:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# vlan <vlan-ID>
```

The following CLI command creates a new VLAN assignment rule:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-vlan <attribute>{equals|not-equals|starts-
with|ends-with|contains|matches-regular-expression} <operator> <VLAN-ID>|value-of}
```

Configuring Wired Profile for Guest Access

The following procedure describes how to configure wired settings for a wired profile:

Table 58: *Steps to Configure Uplink Management VLAN*

New WebUI	Old WebUI
To configure a wired profile: 1. Navigate to the **Configuration** > **Networks** page. 2. Under **Networks**, click **+**. 3. Under **Basic**, In the **Name** field enter a name that uniquely identifies the network. 4. In the **Type** drop-down list, select **Wired.** 5. Click the **Show advanced options** link at the bottom of the page. Specify the following parameters as required. 6. In the same section, configure the following parameters: a. **Primary Usage**—Select **Guest**. b. **Speed/Duplex**—Ensure that appropriate values are selected for **Speed/Duplex**. Contact your network administrator if you need to assign speed and duplex parameters. c. **POE**—Set **POE** to **Enabled** to enable PoE. d. **Admin Status**—Ensure that an appropriate value is selected. The **Admin Status** indicates if the port is up or down. e. **Content Filtering**—Select **Enabled** for **Content Filtering**. f. **Uplink**—Select **Enabled** to configure uplink on this wired profile. If **Uplink** is set to **Enabled** and this network profile is assigned to a specific port, the port will be enabled as Uplink port. For more information on assigning a wired network profile to a port, see Assigning a Profile to Ethernet Ports on page 170. g. **Spanning Tree**—Select the **Spanning Tree**	To configure a wired profile: 1. Click the **Wired** link under **More** on the Instant main window. The **Wired** window is displayed. 2. Click **New** under **Wired Networks**. The **New Wired Network** window is displayed. 3. Click the **Wired Settings** tab and enter the following information: a. **Name**—Specify a name for the profile. b. **Primary Usage**—Select **Guest**. c. **Speed/Duplex**—Ensure that appropriate values are selected for **Speed/Duplex**. Contact your network administrator if you need to assign speed and duplex parameters. d. **POE**—Set **POE** to **Enabled** to enable PoE. e. **Admin Status**—Ensure that an appropriate value is selected. The **Admin Status** indicates if the port is up or down. f. **Content Filtering**—Select **Enabled** for **Content Filtering**. g. **Uplink**—Select **Enabled** to configure uplink on this wired profile. If **Uplink** is set to **Enabled** and this network profile is assigned to a specific port, the port will be enabled as Uplink port. For more information on assigning a wired network profile to a port, see Assigning a Profile to Ethernet Ports on page 170. h. **Spanning Tree**—Select the **Spanning Tree** check box to enable STP on the wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all

New WebUI	Old WebUI
check box to enable STP on the wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP will not operate on the uplink port and is supported only on Instant APs with three or more ports. By default Spanning Tree is disabled on wired profiles. h. **Inactivity Timeout**—Specify the time out interval within the range of 60–86,400 seconds for inactive wired clients. The default interval is 1000 seconds. 7. Click **Next**. The VLAN tab details are displayed. 8. Enter the following information. a. **Mode**—You can specify any of the following modes: ▪ **Access**—Select this mode to allow the port to carry a single VLAN specified as the native VLAN. ▪ **Trunk**—Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs. In this mode, you can configure the native VLAN and the allowed VLAN. b. Specify any of the following values for **Client IP Assignment**: ▪ **Virtual Controller managed**: Select this option to allow the virtual controller to assign IP addresses to the wired clients. When the virtual controller assignment is used, the source IP address is translated to the physical IP address of the master Instant AP for all client traffic that goes through this interface. The virtual controller can also assign a guest VLAN to a wired client. ▪ **Network assigned**: Select this option to allow the clients to receive an IP address from the network to which the virtual controller is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required. c. If the **Trunk** mode is selected: ▪ Specify the **Allowed VLAN**, enter a list	downlink ports, regardless of forwarding mode. STP will not operate on the uplink port and is supported only on Instant APs with three or more ports. By default Spanning Tree is disabled on wired profiles. i. **Inactivity Timeout**—Specify the time out interval within the range of 60–86,400 seconds for inactive wired clients. The default interval is 1000 seconds. 4. Click **Next**. The VLAN tab details are displayed. 5. Enter the following information. a. **Mode**—You can specify any of the following modes: ▪ **Access**—Select this mode to allow the port to carry a single VLAN specified as the native VLAN. ▪ **Trunk**—Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs. In this mode, you can configure the native VLAN and the allowed VLAN. b. Specify any of the following values for **Client IP Assignment**: ▪ **Virtual Controller managed**: Select this option to allow the virtual controller to assign IP addresses to the wired clients. When the virtual controller assignment is used, the source IP address is translated to the physical IP address of the master Instant AP for all client traffic that goes through this interface. The virtual controller can also assign a guest VLAN to a wired client. ▪ **Network assigned**: Select this option to allow the clients to receive an IP address from the network to which the virtual controller is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required. c. If the **Trunk** mode is selected: ▪ Specify the **Allowed VLAN**, enter a list of comma separated digits or ranges: for example, 1,2,5 or 1–4, or all. The

New WebUI	Old WebUI
of comma separated digits or ranges: for example, 1,2,5 or 1–4, or all. The Allowed VLAN refers to the VLANs carried by the port in Access mode. ▪ If the **Client IP Assignment** is set to **Network assigned**, specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1–4093. d. If the **Access** mode is selected: ▪ If the **Client IP Assignment** is set to **Virtual Controller managed**, proceed to step 2. ▪ If the **Client IP Assignment** is set to **Network assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode. 9. **Client VLAN assignment**—You can specify any of the following options. ▪ **Default**—Select this option to set the default VLAN. ▪ **Custom**—Select this option to configure a custom VLAN. 10. Click **Next** to configure internal or external captive portal authentication, roles, and access rules for the guest users.	Allowed VLAN refers to the VLANs carried by the port in Access mode. ▪ If the **Client IP Assignment** is set to **Network assigned**, specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1–4093. d. If the **Access** mode is selected: ▪ If the **Client IP Assignment** is set to **Virtual Controller managed**, proceed to step 2. ▪ If the **Client IP Assignment** is set to **Network assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode. 6. **Client VLAN assignment**—You can specify any of the following options. ▪ **Default**—Select this option to set the default VLAN. ▪ **Custom**—Select this option to configure a custom VLAN. 7. Click **Next** to configure internal or external captive portal authentication, roles, and access rules for the guest users.

The following CLI commands configure the settings for the wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# type <guest>
(Instant AP)(wired ap profile <name>)# speed {10|100|1000|auto}
(Instant AP)(wired ap profile <name>)# duplex {half|full|auto}
(Instant AP)(wired ap profile <name>)# no shutdown
(Instant AP)(wired ap profile <name>)# poe
(Instant AP)(wired ap profile <name>)# uplink-enable
(Instant AP)(wired ap profile <name>)# content-filtering
(Instant AP)(wired ap profile <name>)# spanning-tree
```

The following CLI commands configure VLAN settings for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# switchport-mode {trunk|access}
(Instant AP)(wired ap profile <name>)# allowed-vlan <vlan>
(Instant AP)(wired ap profile <name>)# native-vlan {<guest|1…4095>}
```

The following CLI commands configure a new VLAN assignment rule:

```
(Instant AP)(config)# wired-port-profile <name>
```

```
(Instant AP)(wired ap profile <name>)# set-vlan <attribute>{equals|not-equals|starts-
with|ends-with|contains|matches-regular-expression} <operator> <VLAN-ID>|value-of}
```

IGMP

IP multicast is a network addressing method used to simultaneously deliver a single stream of information from a sender to multiple clients on a network. Unlike broadcast traffic which is meant for all the hosts on a single domain, multicast traffic is sent only to specific hosts that are configured to receive such traffic. Clients that want to receive multicast traffic can join a multicast group through IGMP messages.

- Aruba Instant supports basic functionalities of IGMPv2 and IGMPv3 such as Multicast Group Join and Multicast Group Leave.
- Aruba Instant does not support Source Filtering, Multicast Group Query, Proxy, or Snooping.
- IGMP is not active on wired ports.

Dynamic Mulitcast Optimization

DMO is an additional feature that is independent from IGMP, by converting multicast streams into unicast streams over a wireless link to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients. To configure this feature, refer to Configuring WLAN Settings for an SSID Profile on page 131.

Multicast Transmission Optimization

Multicast transmission optimization is an additional feature that is independent from IGMP, wherein the Instant AP selects the optimal rate for sending 802.11 broadcast and multicast frames based on the lowest of unicast rates across all associated clients. To configure this feature, refer to Configuring WLAN Settings for an SSID Profile on page 131.

Configuring Internal Captive Portal for Guest Network

For internal captive portal authentication, an internal server is used for hosting the captive portal service. The following procedure describes how to configure internal captive portal authentication when adding or editing a guest network created for wireless or wired profile:

Table 59: *Steps to Configure Internal Captive Portal*

New WebUI	Old WebUI
To configure internal captive portal authentication: 1. Navigate to the **Configuration** > **Networks** page. ▪ To create a new network profile, click **+**. ▪ To modify an existing profile, select the profile and click **edit**. 2. Under **Basic**, set **Primary usage** to **Guest**.	To configure internal captive portal: 1. Navigate to the WLAN wizard or Wired window. ▪ To configure internal captive portal authentication for a WLAN SSID, on the **Networks** tab, click **New** to create a new network profile or **edit** to modify an existing profile. ▪ To configure internal captive portal authentication for a wired profile, click **More** > **Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network profile, or click **Edit** to select

New WebUI	Old WebUI
	and modify an existing profile. 2. Set **Primary usage** to **Guest**.

Click the **Security** tab and assign values for the below configuration parameters:

Table 60: *Internal Captive Portal Configuration Parameters*

Parameter	Description
Splash page type	Select any of the following from the drop-down list. ▪ **Internal - Authenticated**—When **Internal Authenticated** is enabled, the guest users are required to authenticate in the captive portal page to access the Internet. The guest users who are required to authenticate must already be added to the user database. ▪ **Internal - Acknowledged**—When **Internal Acknowledged** is enabled, the guest users are required to accept the terms and conditions to access the Internet.
MAC authentication	Select **Enabled** from the **Mac Authentication** drop-down list to enable MAC authentication.
Delimiter character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the Instant AP will use the delimiter in the MAC authentication request. For example, if you specify colon as the delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. **NOTE:** This option is available only when MAC authentication is enabled.
Uppercase support	Set to **Enabled** to allow the Instant AP to use uppercase letters in MAC address string for MAC authentication. **NOTE:** This option is available only if MAC authentication is enabled.
WISPr (applicable for WLAN SSIDs only)	Select **Enabled** if you want to enable WISPr authentication. For more information on WISPr authentication, see WISPr Authentication on page 221. **NOTE:** The WISPr authentication is applicable only for Internal-Authenticated splash pages and is not applicable for wired profiles.
Auth server 1 **Auth server 2**	Select any one of the following: ▪ A server from the list of servers, if the server is already configured. ▪ **Internal Server** to authenticate user credentials at run time. ▪ Select **New** for configuring a new external RADIUS or LDAP server for authentication.
Load balancing	Select **Enabled** to enable load balancing if two authentication servers are used.

Table 60: *Internal Captive Portal Configuration Parameters*

Parameter	Description
Reauth interval	Select a value to allow the Instant APs to periodically reauthenticate all associated and authenticated clients.
Blacklisting (applicable for WLAN SSIDs only)	If you are configuring a wireless network profile, select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures in the **Max auth failures** text box.
Accounting mode (applicable for WLAN SSIDs only)	Select an accounting mode from the **Accounting mode** drop-down list for posting accounting information at the specified accounting interval. When the accounting mode is set to **Authentication**, the accounting starts only after client authentication is successful and stops when the client logs out of the network. If the accounting mode is set to **Association**, the accounting starts when the client associates to the network successfully and stops when the client is disconnected.
Accounting interval	Configure an accounting interval in minutes within the range of 0–60, to allow Instant APs to periodically post accounting information to the RADIUS server.
Encryption (Applicable for WLAN SSIDs only)	Select **Enabled** to configure encryption parameters. Select an encryption and configure a passphrase.
Splash Page Visuals	Under **Splash Page Visuals**, use the editor to specify display text and colors for the initial page that will be displayed to the users when they connect to the network. The initial page asks for user credentials or email, depending on the splash page type (Internal - Authenticated or Internal - Acknowledged). To customize the splash page design, perform the following steps: ■ To change the color of the splash page, click the **Splash page** rectangle and select the required color from the **Background Color** palette. ■ To change the welcome text, click the first square box in the splash page, type the required text in the **Welcome** text box, and click **OK**. Ensure that the welcome text does not exceed 127 characters. ■ To change the policy text, click the second square box in the splash page, type the required text in the **Policy** text box, and click **OK**. Ensure that the policy text does not exceed 255 characters. ■ To upload a custom logo, click **Upload your own custom logo Image**, browse the image file, and click **upload image**. Ensure that the image file size does not exceed 16 KB. ■ To redirect users to another URL, specify a URL in **Redirect URL**. ■ Click **Preview** to preview the captive portal page. **NOTE:** You can customize the captive portal page using double-byte characters. Traditional Chinese, Simplified Chinese, and Korean are a few languages that use double-byte characters. Click the banner, term, or policy in the **Splash Page Visuals** to modify the text in the red box. These fields accept double-byte characters or a combination of English and double-byte characters.

Click **Next** to configure access rules.

The following CLI commands configure internal captive portal authentication:

```
(Instant AP)(config)# wlan ssid-profile <name>
```

```
(Instant AP)(SSID Profile <name>)# essid <ESSID-name>
(Instant AP)(SSID Profile <name>)# type <Guest>
(Instant AP)(SSID Profile <name>)# captive-portal <internal-authenticated> exclude-
uplink {3G|4G|Wifi|Ethernet}
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# auth-server <server1>
(Instant AP)(SSID Profile <name>)# radius-reauth-interval <Minutes>
```

The following CLI commands configure internal captive portal authentication for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# type <guest>
(Instant AP)(wired ap profile <name>)# captive-portal {<internal-
authenticated>|<internal-acknowledged>} exclude-uplink {3G|4G|Wifi|Ethernet}
(Instant AP)(wired ap profile <name>)# mac-authentication
(Instant AP)(wired ap profile <name>)# auth-server <server1>
(Instant AP)(wired ap profile <name>)# radius-reauth-interval <Minutes>
```

The following CLI commands customize internal captive portal splash page:

```
(Instant AP)(config)# wlan captive-portal
(Instant AP)(Captive Portal)# authenticated
(Instant AP)(Captive Portal)# background-color <color-indicator>
(Instant AP)(Captive Portal)# banner-color <color-indicator>
(Instant AP)(Captive Portal)# banner-text <text>
(Instant AP)(Captive Portal)# decoded-texts <text>
(Instant AP)(Captive Portal)# redirect-url <url>
(Instant AP)(Captive Portal)# terms-of-use <text>
(Instant AP)(Captive Portal)# use-policy <text>
```

The following CLI command configures a customized logo from a TFTP server to the Instant AP:

```
(Instant AP)# copy config tftp <ip-address> <filename> portal logo
```

Configuring External Captive Portal for a Guest Network

This section provides the following information:

- External Captive Portal Profiles on page 189
- Creating an External Captive Portal Profile on page 190
- Configuring an SSID or Wired Profile to Use External Captive Portal Authentication on page 191
- External Captive Portal Redirect Parameters on page 193

External Captive Portal Profiles

You can now configure external captive portal profiles and associate these profiles to a user role or SSID. You can create a set of captive portal profiles in the **External Captive Portal** window (accessed from the **Security** tab of the old WebUI and the **Configuration** > **Security** tab of the new WebUI) and associate these profiles with an SSID or a wired profile. You can also create a new captive portal profile on the **Security** tab of the WLAN wizard or a Wired Network window. In the current release, you can configure up to 16 external captive portal profiles.

When the captive portal profile is associated to an SSID, it is used before user authentication. If the profile is associated to a role, it is used only after the user authentication. When a captive portal profile is applied to an SSID or wired profile, the users connecting to the SSID or wired network are assigned a role with the captive portal rule. The guest user role allows only DNS and DHCP traffic between the client and the network, and directs all HTTP or HTTPS requests to the captive portal unless explicitly permitted to allow all types of traffic.

Creating an External Captive Portal Profile

The following procedure describes how to create an external captive portal profile:

Table 61: *Steps to Create an External Captive Portal Profile*

New WebUI	Old WebUI
To create an external captive portal profile: 1. Navigate to **Configuration** > **Security** page. 2. Expand **External Captive Portal**. 3. Click **+**. The **New** popup window is displayed.	To create an external captive portal profile: 1. Go to **Security** > **External Captive Portal**. 2. Click **New**. The **New** popup window is displayed

Specify values for the following parameters:

Table 62: *External Captive Portal Profile Configuration Parameters*

Parameter	Description
Name	Enter a name for the profile.
Type	Select any one of the following types of authentication: ▪ **Radius Authentication**—Select this option to enable user authentication against a RADIUS server. ▪ **Authentication Text**—Select this option to specify an authentication text. The specified text will be returned by the external server after a successful user authentication.
IP or hostname	Enter the IP address or the host name of the external splash page server.
URL	Enter the URL for the external captive portal server.
Port	Enter the port number.
Use https (Available only if RADIUS Authentication is selected)	Select **Enabled** to enforce clients to use HTTPS to communicate with the captive portal server.
Captive Portal failure	Allows you to configure Internet access for the guest clients when the external captive portal server is not available. Select **Deny Internet** to prevent clients from using the network, or **Allow Internet** to allow the guest clients to access Internet when the external captive portal server is not available.
Automatic URL Whitelisting	Select **Enabled** to enable the automatic whitelisting of URLs. On selecting the check box for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically whitelisted. The automatic URL whitelisting is disabled by default.
Auth Text (Available only if Authentication Text is selected)	If the External Authentication splash page is selected, specify the authentication text to be returned by the external server after successful authentication.
Server Offload	Select **Enabled** to enable server offload. The server offload feature ensures that the non-browser client applications are not unnecessarily redirected to the external portal server and thereby reducing the load on the external captive portal server. The **Server Offload** option is **Disabled** by default.

Parameter	Description
Prevent frame overlay	When the **Prevent frame overlay** option is enabled, a frame can display a page only if it is in the same domain as the main page. This option is **Disabled** by default and can be used to prevent the overlay of frames.
Use VC IP in Redirect URL	Sends the IP address of the virtual controller in the redirection URL when external captive portal servers are used. This option is disabled by default.
Redirect URL	Specify a redirect URL if you want to redirect the users to another URL.

Click **OK**.

The following CLI commands configure an external captive portal profile:

```
(Instant AP)(config)# wlan external-captive-portal [profile_name]
(Instant AP)(External Captive Portal)# server <server>
(Instant AP)(External Captive Portal)# port <port>
(Instant AP)(External Captive Portal)# url <url>
(Instant AP)(External Captive Portal)# https
(Instant AP)(External Captive Portal)# redirect-url <url>
(Instant AP)(External Captive Portal)# server-fail-through
(Instant AP)(External Captive Portal)# no auto-whitelist-disable
(Instant AP)(External Captive Portal)# server-offload
(Instant AP)(External Captive Portal)# switch-ip
(Instant AP)(External Captive Portal)# prevent-frame-overlay
(Instant AP)(External Captive Portal)# out-of-service-page <url>
```



The `out-of-service-page <url>` parameter configures the Instant AP to display a custom captive portal page when the internet uplink is down. This parameter can be configured only through the Instant CLI.

Configuring an SSID or Wired Profile to Use External Captive Portal Authentication

The following procedure describes how to configure external captive portal authentication when adding or editing a guest network profile:

Table 63: *Steps to Configure External Captive Portal on a Guest SSID*

New WebUI	Old WebUI
To configure external captive portal: 1. Navigate to the WLAN wizard or Wired window. ▪ To configure external captive portal authentication for a WLAN SSID, on the **Networks** tab, click **New** to create a new network profile or **edit** to modify an existing profile. ▪ To configure external captive portal authentication for a wired profile, Go to **More** > **Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network, or click **Edit** to select an existing profile. 2. On the **Security** tab, select **External** from the **Splash page type** drop-down list.	To configure external captive portal: 1. Navigate to the **Configuration** > **Networks** page. ▪ To create a new network profile, click **+**. ▪ To modify an existing profile, select the profile and click **edit**. 2. Select the **Security** tab. 3. In the **Splash page type** drop-down list, select **External**. 4. From the **Captive Portal Profile** drop-down list, select a profile. You can select and modify a default profile, or add an already existing profile, or click **+** and create a new profile.

New WebUI	Old WebUI
3. From the **Captive Portal Profile** drop-down list, select a profile. You can select and modify a default profile, or an already existing profile, or click **New** and create a new profile.	

1. Configure the following parameters based on the type of splash page you selected.

Table 64: *External Captive Portal Configuration Parameters*

Parameter	Description
Captive-portal proxy server	If required, configure a captive portal proxy server or a global proxy server to match your browser configuration by specifying the IP address and port number in the **Captive-portal proxy server** text box.
WISPr	Select **Enabled** if you want to enable WISPr authentication. For more information on WISPr authentication, see WISPr Authentication on page 221. **NOTE:** The WISPr authentication is applicable only for the **External** and **Internal-Authenticated** splash pages and is not applicable for wired profiles.
MAC authentication	Select **Enabled** if you want to enable MAC authentication. For information on MAC authentication, see MAC Authentication on page 215.
Delimiter character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the Instant AP will use the delimiter in the MAC authentication request. For example, if you specify colon as the delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. **NOTE:** This option is available only when MAC authentication is enabled.
Uppercase support	Set to **Enabled** to allow the Instant AP to use uppercase letters in MAC address string for MAC authentication. **NOTE:** This option is available only if MAC authentication is enabled.
Authentication server 1 and **Authentication server 2**	To configure an authentication server, select any of the following options: ■ If the server is already configured, select the server from the list. ■ To create new external RADIUS server, select **New**. For more information, see Configuring an External Server for Authentication on page 231.
Reauth interval	Specify a value for the reauthentication interval at which the Instant APs periodically reauthenticate all associated and authenticated clients.
Accounting mode	Select an accounting mode from the **Accounting mode** drop-down list for posting accounting information at the specified **Accounting interval**. When the accounting mode is set to **Authentication**, the accounting starts only after client authentication is successful and stops when the client logs out of the network. If the accounting mode is set to **Association**, the accounting starts when the client associates to the network successfully and stops when the client is disconnected.
Accounting interval	Configure an accounting interval in minutes within the range of 0–60, to allow Instant APs to periodically post accounting information to the RADIUS server.

Table 64: *External Captive Portal Configuration Parameters*

Parameter	Description
Blacklisting	If you are configuring a wireless network profile, select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures.
Max auth failures	If you are configuring a wireless network profile and **Blacklisting** is enabled, specify the maximum number of authentication failures after which users who fail to authenticate must be dynamically blacklisted.
Disable if uplink type is	Select the type of the uplink to exclude.
Encryption	Select **Enabled** to configure encryption settings and specify the encryption parameters.

Click **Next** to continue and then click **Finish** to apply the changes.

The following CLI commands configure security settings for guest users of the WLAN SSID profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# essid <ESSID-name>
(Instant AP)(SSID Profile <name>)# type <Guest>
(Instant AP)(SSID Profile <name>)# captive-portal{<type>[exclude-uplink
<types>]|external[exclude-uplink <types>| profile <name>[exclude-uplink <types>]]}
(Instant AP)(SSID Profile <name>)# captive-portal-proxy-server <IP> <port>
(Instant AP)(SSID Profile <name>)# blacklist
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# max-authentication-failures <number>
(Instant AP)(SSID Profile <name>)# auth-server <server-name>
(Instant Access Point (SSID Profile <name>)# radius-accounting
(Instant Access Point (SSID Profile <name>)# radius-interim-accounting-interval
(Instant Access Point (SSID Profile <name>)# radius-accounting-mode {user-
association|user-authentication}
(Instant AP)(SSID Profile <name>)# wpa-passphrase <WPA_key>
(Instant AP)(SSID Profile <name>)# wep-key <WEP-key> <WEP-index>
```

The following CLI commands configure security settings for guest users of the wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# type <Guest>
(Instant AP)(wired ap profile <name>)# captive-portal{<type>[exclude-uplink
<types>]|external[exclude-uplink <types>| profile <name>[exclude-uplink <types>]]}
(Instant AP)(wired ap profile <name>)# mac-authentication
```

External Captive Portal Redirect Parameters

If the external captive portal redirection is enabled on a network profile, Instant AP sends an HTTP response with the redirect URL to display the splash page and enforce captive portal authentication by clients. The HTTP response from the Instant AP includes the following parameters:

Table 65: *External Captive Portal Redirect Parameters*

Parameter	Example Value	Description
cmd	login	Type of operation
mac	34:02:86:c6:d2:3e	Client MAC address

Table 65: *External Captive Portal Redirect Parameters*

Parameter	Example Value	Description
essid	guest-ecp-109	ESSID
ip	192.0.2.0	Client IP address
apname	9c:1c:12:cb:a2:90	Instant AP host name
apmac	9c:1c:12:cb:a2:90	Instant AP MAC address
vcname	instant-C8:1D:DA"	Virtual controllername
switchip	securelogin.arubanetworks.com	Captive portal domain used for external captive portal authentication
url	http://www.google.com/	original URL

Configuring External Captive Portal Authentication Using ClearPass Guest

You can configure Instant to point to ClearPass Guest as an external captive portal server. With this configuration, the user authentication is performed by matching a string in the server response and that in the RADIUS server (either ClearPass Guest or a different RADIUS server).

Creating a Web Login Page in ClearPass Guest

The ClearPass Guest Visitor Management Appliance provides a simple and personalized UI through which operational staff can quickly and securely manage visitor network access. With ClearPass Guest, the users can have a controlled access to a dedicated visitor management user database. Through a customizable web portal, the administrators can easily create an account, reset a password, or set an expiry time for visitors. Visitors can be registered at reception and provisioned with an individual guest account that defines the visitor profile and the duration of their visit. By defining a web login page on the ClearPass Guest Visitor Management Appliance, you can to provide a customized graphical login page for visitors accessing the network.

For more information on setting up the RADIUS web login page, refer to the *RADIUS Services* section in the *ClearPass Guest Deployment Guide*

Configuring an External RADIUS Server for Captive Portal Authentication

Table 66: *Steps to Configure Uplink Management VLAN*

New WebUI	Old WebUI
To configure Instant to point to ClearPass Guest as an external captive portal server: 1. Select the WLAN SSID for which you want to enable external captive portal authentication with ClearPass Policy Manager. You can also configure the RADIUS server when configuring a new SSID profile. a. Navigate to the **Configuration** > **Networks**	To configure Instant to point to ClearPass Guest as an external captive portal server: 1. Select the WLAN SSID for which you want to enable external captive portal authentication with ClearPass Policy Manager. You can also configure the RADIUS server when configuring a new SSID profile. 2. On the **Security** tab, select **External** from the

New WebUI	Old WebUI
page. b. Select the WLAN SSID profile from the **Networks** list and click **edit**. 2. Select the **Security** tab and select **External** from the **Splash page type** drop-down list. 3. Select **+** from the **Captive portal profile** drop-down list to create a captive portal profile, and configure the following: a. In the **Name** text box, enter the name of the profile . b. In the **Type** drop-down list, select the authentication type. c. In the **IP or hostname** text box, enter the IP address of the ClearPass Guest server. Obtain the ClearPass Guest IP address from your system administrator. d. In the **URL** text box enter **/page_name.php**. This URL must correspond to the **Page Name** configured in the ClearPass Guest RADIUS Web Login page. For example, if the Page Name is **Aruba**, the URL should be **/Aruba.php** in the WebUI. e. Enter the **Port** number (generally should be **80**). The ClearPass Guest server uses this port for HTTP services. f. Click **OK**. 4. To create an external RADIUS server, select **+**from the **Authentication server 1** drop-down list. For information on authentication server configuration parameters, see Configuring an External Server for Authentication on page 231. 5. Click **Next** and until **Finish**. 6. To verify, connect the updated SSID. 7. Open any browser and type any URL. Instant redirects the URL to ClearPass Guest login page. 8. Log in to the network with the username and password specified while configuring the RADIUS server.	**Splash page type** drop-down list. 3. Select **New** from the **Captive portal profile** drop-down list and update the following: a. Enter the IP address of the ClearPass Guest server in the **IP or hostname** text box. Obtain the ClearPass Guest IP address from your system administrator. b. Enter **/page_name.php** in the **URL** text box. This URL must correspond to the **Page Name** configured in the ClearPass Guest RADIUS Web Login page. For example, if the Page Name is **Aruba**, the URL should be **/Aruba.php** in the WebUI. c. Enter the **Port** number (generally should be **80**). The ClearPass Guest server uses this port for HTTP services. d. Click **OK**. 4. To create an external RADIUS server, select **New** from the **Auth server 1** drop-down list. For information on authentication server configuration parameters, see Configuring an External Server for Authentication on page 231. 5. Click **Next** and then click **Finish**. 6. To verify, select the updated SSID in the **Networks** tab of the Instant main window. 7. Open any browser and type any URL. Instant redirects the URL to ClearPass Guest login page. 8. Log in to the network with the username and password specified while configuring the RADIUS server.

Configuring RADIUS Attribute for ClearPass Policy Manager Server Load Balancing

Starting from Instant 6.4.3.4-4.2.1.0, the administrators can configure a RADIUS server IP address as one of the parameters on ClearPass Policy Manager server for external captive portal user authentication.

Configuring a RADIUS server attribute for guest user authentication allows the administrators to balance the load on the ClearPass Policy Manager servers.

When the RADIUS server IP address is configured under **Extra Fields** in the ClearPass Guest login page, the RADIUS server IP parameter is submitted to the server as part of the HTTP or HTTPS POST data when the guest users initiate an HTTP or HTTPS request. The Instant AP intercepts this information to perform the actual RADIUS authentication with the server IP defined in the POST message. For more information on guest registration customization on ClearPass Guest, refer to the *ClearPass Guest User Guide*.

Configuring Facebook Login

Instant supports the Facebook Wi-Fi feature that allows the captive portal clients using a Facebook account to authenticate on an Instant AP. You can configure a guest network to use a customized Facebook page as an external captive portal URL and allow the Instant AP to redirect clients to a Facebook page when it receives an HTTP request. The users can select the appropriate option to authenticate and access the Internet. By configuring the Facebook login feature, businesses can pair their network with the Facebook Wi-Fi service, so that the users logging into Wi-Fi hotspots are presented with a business page, before gaining access to the network.

The Facebook Wi-Fi integration with the Instant AP includes the following procedures:

- Setting up a Facebook Page
- Configuring an SSID
- Configuring the Facebook Portal Page
- Accessing the Portal Page

Setting up a Facebook Page

To enable integration with the Instant AP, ensure that you have a Facebook page created as a local business with a valid location.

- For more information on creating a Facebook page, see the online help available at https://www.facebook.com/help.
- For more information on setting up and using Facebook Wi-Fi service, see https://www.facebook.com/help/126760650808045.

Configuring an SSID

The following procedure describes how to configure guest network profile and enable Facebook login:

Table 67: *Steps to Set Up a Facebook Login*

New WebUI	Old WebUI
To enable Facebook login: 1. Navigate to the **Configuration** > **Networks** page. 2. Under **Networks,** click **+**. 3. Enter a name for the SSID. 4. In the **Primary usage** drop-down list, select **Guest.** 5. Configure other required parameters under **Basic** and **VLAN** tabs. 6. Under **Security**, select **Facebook** from the **Splash page type** drop-down list.	To enable Facebook login: 1. Navigate to **Networks** > **New** to create a new network profile. 2. Enter a name for the SSID. 3. Select **Guest** under **Primary usage**. 4. Configure other required parameters in the **WLAN Settings** and **VLAN** tabs. 5. On the **Security** tab, select **Facebook** from the **Splash page type** drop-down list.

New WebUI	Old WebUI
7. Configure the required settings. 8. Click **Next** until **Finish**. 9. The SSID with the Facebook option is created. After the SSID is created, the Instant AP automatically registers with Facebook. If the Instant AP registration is successful, the **Facebook configuration** link is displayed in the **Security** tab of the WLAN wizard.	6. Click **Next**. The **Access** tab contents are displayed. 7. Click **Finish**. The SSID with the Facebook option is created. After the SSID is created, the Instant AP automatically registers with Facebook. If the Instant AP registration is successful, the **Facebook configuration** link is displayed in the **Security** tab of the WLAN wizard.

The following CLI command configures an account for captive portal authentication:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# captive-portal {<type>[exclude-uplink
<types>]|external [exclude-uplink <types>|profile <name>[exclude-uplink <types>]]}
```

Example

The following example configures a Facebook account for captive portal authentication:

```
(Instant AP)(config)# wlan ssid-profile guestNetwork
(Instant AP)(SSID Profile "guestNetwork")# captive-portal facebook
```

Configuring the Facebook Portal Page

The following procedure describes how to bind the virtual controller with the Facebook portal:

Table 68: *Steps to Bind the VC with the Facebook Portal*

New WebUI	Old WebUI
To bind the VC with the Facebook Portal: 1. Open the SSID with the Facebook option enabled, navigate to the **Security** tab and click the **Facebook configuration** link. The Facebook page is displayed. **NOTE:** The **Facebook configuration** link is displayed only if the Instant AP is successfully registered with Facebook. 2. Log in with your Facebook credentials. The **Facebook Wi-Fi Configuration** page is displayed. 3. Select the Facebook page. 4. Under **Bypass Mode**, select any of the following options: ▪ **Skip Check-in link**—When selected, the users are not presented with your business Facebook page, but are allowed to access the Internet by clicking the **Skip Check-in** link. ▪ **Require Wi-Fi code**—When selected, the users are assigned a Wi-Fi code to gain access to the Facebook page. 5. Customize the session length and terms of service if required.	To bind the VC with the Facebook Portal: 1. Open the SSID with the Facebook option enabled, navigate to the **Security** tab and click the **Facebook configuration** link. The Facebook page is displayed. **NOTE:** The **Facebook configuration** link is displayed only if the Instant AP is successfully registered with Facebook. 2. Log in with your Facebook credentials. The **Facebook Wi-Fi Configuration** page is displayed. 3. Select the Facebook page. 4. Under **Bypass Mode**, select any of the following options: ▪ **Skip Check-in link**—When selected, the users are not presented with your business Facebook page, but are allowed to access the Internet by clicking the **Skip Check-in** link. ▪ **Require Wi-Fi code**—When selected, the users are assigned a Wi-Fi code to gain access to the Facebook page. 5. Customize the session length and terms of service if required.

New WebUI	Old WebUI
6. Click **Save Settings**.	6. Click **Save Settings**.

Accessing the Portal Page

The following procedure describes how to access the Facebook Portal page using the WebUI:

Table 69: *Steps to Access the Facebook Portal Page*

New WebUI	Old WebUI
To access the portal page: 1. Connect to the SSID with the Facebook option enabled. 2. Launch a web browser. The browser opens the Facebook Wi-Fi page. If the Wi-Fi-code based login is enabled, the users are prompted to enter the Wi-FI code. If the **Skip Check-in** link is displayed, click the link to skip checking in to the Facebook business page and proceed to access the Internet. 3. If you want to check in the business page, click **Check In** and provide your credentials. After checking in, click **Continue Browsing** to access the web page that was originally requested.	To access the portal page: 1. Connect to the SSID with the Facebook option enabled. 2. Launch a web browser. The browser opens the Facebook Wi-Fi page. If the Wi-Fi-code based login is enabled, the users are prompted to enter the Wi-FI code. If the **Skip Check-in** link is displayed, click the link to skip checking in to the Facebook business page and proceed to access the Internet. 3. If you want to check in the business page, click **Check In** and provide your credentials. After checking in, click **Continue Browsing** to access the web page that was originally requested.

Configuring Guest Logon Role and Access Rules for Guest Users

For captive portal profile, you can create any the following types of roles:

- A pre-authenticated role—This role is assigned before the captive portal authentication. The user can only access certain destinations with this role.
- A guest role—This role is assigned after user authentication.
- A captive-portal role—This role can be assigned to any network such as Employee, Voice, or Guest. When the user is assigned with this role, a splash page is displayed after opening a browser and the users may need to authenticate.

You can configure up to 128 access rules for guest user roles through the Instant WebUI or the CLI. The following procedure describes how to configure access rules for a guest SSID.

Table 70: *Steps to Configure Access Rules for Guest SSID*

New WebUI	Old WebUI
To configure roles and access rules for the guest network: 1. Navigate to the **Configuration** > **Networks** and select the guest network you want to configure and click **edit**. 2. Select the **Access** tab, select any of the following types of access control from the **Access Rules** drop-down list: ▪ **Unrestricted**—Select this to set	To configure roles and access rules for the guest network: 1. On the **Networks** > **Access** tab, set the slider to any of the following types of access control: ▪ **Unrestricted**—Select this to set unrestricted access to the network. ▪ **Network-based**—Set the slider to **Network-based** to set common rules for all users in a network. The **Allow any to**

New WebUI	Old WebUI
unrestricted access to the network. ■ **Network-based**—Select this to set common rules for all users in a network. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define an access rule: a. Click **+**. b. Select appropriate options in the **New rule** window. c. Click **OK**. ■ **Role-based**—Select this to enable access based on user roles. ■ For role-based access control: ■ Create a user role if required. For more information, see Configuring User Roles. ■ Create access rules for a specific user role. For more information, see Configuring ACL Rules for Network Services on page 260. You can also configure an access rule to enforce captive portal authentication for an SSID with the 802.1X authentication method. For more information, see Configuring Captive Portal Roles for an SSID on page 200. ■ Create a role assignment rule. For more information, see Configuring Derivation Rules on page 282. Instant supports role derivation based on the DHCP option for captive portal authentication. When the captive portal authentication is successful, a new user role is assigned to the guest users based on DHCP option configured for the SSID profile instead of the pre-authenticated role. 3. Click **Finish**.	**all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define an access rule: a. Click **New**. b. Select appropriate options in the **New Rule** window. c. Click **OK**. ■ **Role-based**—Select **Role-based** to enable access based on user roles. ■ For role-based access control: ■ Create a user role if required. For more information, see Configuring User Roles. ■ Create access rules for a specific user role. For more information, see Configuring ACL Rules for Network Services on page 260. You can also configure an access rule to enforce captive portal authentication for an SSID with the 802.1X authentication method. For more information, see Configuring Captive Portal Roles for an SSID on page 200. ■ Create a role assignment rule. For more information, see Configuring Derivation Rules on page 282. Instant supports role derivation based on the DHCP option for captive portal authentication. When the captive portal authentication is successful, a new user role is assigned to the guest users based on DHCP option configured for the SSID profile instead of the pre-authenticated role. 2. Click **Finish**.

The following CLI command configures access control rules for a WLAN SSID:

```
(Instant AP)(config)# wlan access-rule <name>
(Instant AP)(Access Rule <name>)# rule <dest> <mask> <match> {<protocol> <start-port>
<end-port> {permit|deny|src-nat|dst-nat{<IP-address> <port>|<port>}}| app <app>
{permit|deny}| appcategory <appgrp>|webcategory <webgrp> {permit|deny}|webreputation
<webrep> [<option1....option9>]
```

The following CLI command configures access control rules based on the SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-by-ssid
```

The following CLI command configures role assignment rules:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role <attribute>{{equals|not-equals|starts-
with|ends-with|contains|matches-regular-expression}<operator><role>|value-of}
```

The following CLI command configures a pre-authentication role:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-pre-auth <role>
```

The following CLI command configures machine and user authentication roles:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-machine-auth <machine_only> <user_only>
```

The following CLI command configures unrestricted access:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-unrestricted
```

Example

The following example configures access rules for the wireless network:

```
(Instant AP)(config)# wlan access-rule WirelessRule
```

Configuring Captive Portal Roles for an SSID

You can configure an access rule to enforce captive portal authentication for SSIDs that use 802.1X authentication to authenticate clients. You can configure rules to provide access to external or internal captive portal, so that some of the clients using this SSID can derive the captive portal role.

The following conditions apply to the 802.1X and captive portal authentication configuration:

- If a user role does not have captive portal settings configured, the captive portal settings configured for an SSID are applied to the client's profile.
- If the SSID does not have captive portal settings configured, the captive portal settings configured for a user role are applied to the client's profile.
- If captive portal settings are configured for both SSID and user role, the captive portal settings configured for a user role are applied to the client's profile.

You can create a captive portal role for both **Internal** and **External** splash page types.

The following procedure describes how to configure a captive portal role:

Table 71: *Steps to Configure Captive Portal Roles*

New WebUI	Old WebUI
To create a captive portal role: 1. Navigate to the **Configuration** > **Networks** page. 2. Select a guest SSID profile and click **edit** 3. select the **Access** tab, select **Role-based** from the Access Rules drop-down list. 4. Select a role or create a new one if required. 5. In the **Access Rules for <network>** window, click **+** to add a new rule. The **New rule** window is displayed.	To create a captive portal role: 1. Select an SSID profile from the **Networks** tab and click **edit**. The **Edit <WLAN-Profile>** window is displayed. 2. On the **Access** tab, move the slider to **Role-based** access control by using the scroll bar. 3. Select a role or create a new one if required. 4. In the **Access Rules** window, click **New** to add a new rule. The **New Rule** window is displayed.

In the **New Rule** window, specify the parameters.

Table 72: *Captive Portal Rule Configuration Parameters*

Parameter	Description
Rule type	Select **Captive Portal** from the **RuleType** drop-down list.
Splash Page Type	Select any of the following attributes: ■ Select **Internal** to configure a rule for internal captive portal authentication. ■ Select **External** to configure a rule for external captive portal authentication.
Internal	If **Internal** is selected as splash page type, perform the following steps: ■ Under **Splash Page Visuals**, use the editor to specify display text and colors for the initial page that would be displayed to users connecting to the network. The initial page asks for user credentials or email, depending on the splash page type configured. ■ To change the color of the splash page, click the **Splash page** rectangle and select the required color from the **Background Color** palette. ■ To change the welcome text, click the first square box in the splash page, type the required text in the **Welcome** text box, and then click **OK**. Ensure that the welcome text does not exceed 127 characters. ■ To change the policy text, click the second square box in the splash page, type the required text in the **Policy** text box, and click **OK**. Ensure that the policy text does not exceed 255 characters. ■ Specify the URL to which you want to redirect the guest users. ■ To upload a custom logo, click **Upload your own custom logo Image**, browse the image file, and click **upload image**. ■ To preview the captive portal page, click **Preview**.
External	If **External** is selected, perform the following steps: ■ Select a profile from the **Captive portal profile** drop-down list. ■ If you want to edit the profile, click **Edit** and update the following parameters: • **Type**—Select either **Radius Authentication** (to enable user authentication against a RADIUS server) or **Authentication Text** (to specify the authentication text to be returned by the external server after a successful user authentication). • **IP or hostname**— Enter the IP address or the host name of the external splash page server. • **URL**— Enter the URL for the external splash page server. • **Port**—Enter the port number. • **Use https**—Select Enabled to enforce clients to use HTTPS to communicate with the captive portal server. This option is available only if RADIUS Authentication is selected • **Redirect URL**—Specify a redirect URL if you want to redirect the users to another URL. • **Captive Portal failure**—The **Captive Portal failure** drop-down list allows you to configure Internet access for the guest clients when the external

Table 72: *Captive Portal Rule Configuration Parameters*

Parameter	Description
	captive portal server is not available. Select **Deny Internet** to prevent clients from using the network, or **Allow Internet** to allow the guest clients to access Internet when the external captive portal server is not available. • **Automatic URL Whitelisting**—Select **Enabled** or **Disabled** to enable or disable automatic whitelisting of URLs. On selecting the check box for the external captive portal authentication, the URLs allowed for the unauthenticated users to access are automatically whitelisted. The automatic URL whitelisting is disabled by default. • **Server Offload**—Select **Enabled** to enable server offload. The server offload feature ensures that the non-browser client applications are not unnecessarily redirected to the external portal server and thereby reducing the load on the external captive portal server. The **Server Offload** option is **Disabled** by default. • **Prevent frame overlay**—When the **Prevent frame overlay** option is enabled, a frame can display a page only if it is in the same domain as the main page. This option is **Enabled** by default and can be used to prevent the overlay of frames. • **Use VC IP in Redirect URL**—Sends the IP address of the virtual controller in the redirection URL when external captive portal servers are used. This option is disabled by default. • **Auth Text**—Indicates the authentication text returned by the external server after a successful user authentication.

Click **OK**. The **Enforce captive portal** rule is created and listed as an access rule in the **Access Rules** window.

- In the **Role Assignment Rules** window, click **+** to create a role assignment rule based on the user role to which the captive portal access rule is assigned. Click **OK**.
- Click **Finish**.

The client can connect to this SSID after authenticating with username and password. After a successful user login, the captive portal role is assigned to the client.

The following CLI command creates a captive portal role:

```
(Instant AP)(config)# wlan access-rule <Name>
(Instant AP)(Access Rule <Name>)# captive-portal {external [profile <name>]|internal}
```

Configuring Walled Garden Access

On the Internet, a walled garden typically controls access to web content and services. The walled garden access is required when an external captive portal is used. For example, a hotel environment where the unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents.

The users who do not sign up for the Internet service can view the allowed websites (typically hotel property websites). The website names must be DNS-based and support the option to define wildcards. When a user attempts to navigate to other websites that are not in the whitelist of the walled garden

profile, the user is redirected to the login page. Instant AP supports walled garden only for the HTTP requests. For example, if you add yahoo.com in walled garden whitelist and the client sends an HTTPS request (https://yahoo.com), the requested page is not displayed and the users are redirected to the captive portal login page.

In addition, a blacklisted walled garden profile can also be configured to explicitly block the unauthenticated users from accessing some websites.

The following CLI command configures walled garden access:

```
(Instant AP)(config)# wlan walled-garden
(Instant AP)(Walled Garden)# white-list <domain>
(Instant AP)(Walled Garden)# black-list <domain>
```

Disabling Captive Portal Authentication

The following procedure describes how to disable captive portal authentication:

Table 73: *Steps to Configure Uplink Management VLAN*

New WebUI	Old WebUI
To disable captive portal authentication: 1. Navigate to the **Configuration** > **Networks** tab. 2. Select a wireless guest or a wired guest profile and click **Edit**. **NOTE:** You can also customize splash page visuals on the **Security** tab of **New WLAN** (WLAN wizard) and **New Wired Network** (wired profile window) when configuring a new profile. 3. Select the **Security** tab. 4. Select **None** from the **Splash page type** drop-down list. Although the splash page is disabled, you can enable MAC authentication, configure authentication servers, set accounting parameters, blacklist clients based on MAC authentication failures, and configure encryption keys for authorized access. 5. If required, configure the security parameters. 6. Click **Next** and until **Finish** to apply the changes.	To disable captive portal authentication: 1. Select a wireless guest or a wired guest profile. Depending on the network profile selected, the **Edit <WLAN-Profile>** or **Edit Wired Network** window is displayed. **NOTE:** You can also customize splash page visuals on the **Security** tab of **New WLAN** (WLAN wizard) and **New Wired Network** (wired profile window) when configuring a new profile. 2. Navigate to the **Security** tab. 3. Select **None** from the **Splash page type** drop-down list. Although the splash page is disabled, you can enable MAC authentication, configure authentication servers, set accounting parameters, blacklist clients based on MAC authentication failures, and configure encryption keys for authorized access. 4. If required, configure the security parameters. 5. Click **Next** and then click **Finish** to apply the changes.

Configuring Facebook Express Wi-Fi

Aruba Instant APs support Facebook Express Wi-Fi feature that enables users to connect to Facebook Wi-Fi and use internet services. When a user connects to the Facebook Express Wi-Fi SSID, they will be assigned the base role defined in the **facebook-xwf-role** in the **wlan ssid-profile.** In addition to traffic allowed in the base role, the user also inherits access rules defined in the XWF traffic class. On successful authentication with the Facebook server, the user inherits either the FBS or ANY traffic class depending on their data subscription.

Configuring Facebook Express Wi-Fi for a WLAN

Use the following procedure to configure Facebook Express Wi-Fi for a WLAN:

1. Create a user role for Facebook Express Wi-Fi users. This will be the pre-authentication role that is assigned to users connecting to the Facebook Express Wi-Fi SSID. For more information on creating a user role, see Configuring User Roles.
2. Create Facebook Wi-Fi traffic classes using the **wlan traffic-class <name>** command. The following traffic classes must be created:
   - **XWF traffic class** – Defines the traffic allowed to the user before Facebook authentication.
   - **FBS traffic class** – Defines the traffic allowed the user after Facebook authentication.

   In addition to the above mentioned traffic classes, an **ANY** traffic class will be automatically created and assigned for users with an active data subscription. The ANY traffic class allows unrestricted internet access for the user. The ANY traffic class can be assigned a different name using the **wlan traffic-class-any-alias** command. It is recommended that the ANY class is named Internet. For more information on **wlan traffic-class-any-alias** command, see *Aruba Instant 8.x CLI Reference Guide*.

   Configure the following parameters for XWF and FBS traffic classes in the **wlan traffic-class** command:

XWF Traffic Class	FBS Traffic Class
wlan traffic-class XWF index 2 domain *.expresswifi.com domain xwf-static.xx.fbcdn.net domain xwf-scontent.xx.fbcdn.net domain xwf.facebook.com domain xwf.fyi domain h.facebook.com domain graph.expresswifi.com domain *.facebook.com	wlan traffic-class FBS index 1 subnet 31.13.64.32 255.255.255.248 subnet 31.13.65.32 255.255.255.248 subnet 31.13.66.32 255.255.255.248 subnet 31.13.67.32 255.255.255.248 subnet 31.13.68.32 255.255.255.248 subnet 31.13.69.32 255.255.255.248 subnet 31.13.70.32 255.255.255.248 subnet 31.13.71.32 255.255.255.248 subnet 31.13.72.32 255.255.255.248 subnet 31.13.73.32 255.255.255.248 subnet 31.13.74.32 255.255.255.248 subnet 31.13.75.32 255.255.255.248 subnet 31.13.76.32 255.255.255.248 subnet 31.13.77.32 255.255.255.248 subnet 31.13.78.32 255.255.255.248 subnet 31.13.79.32 255.255.255.248 subnet 31.13.80.32 255.255.255.248 subnet 31.13.81.32 255.255.255.248 subnet 31.13.82.32 255.255.255.248 subnet 31.13.83.32 255.255.255.248 subnet 31.13.84.32 255.255.255.248 subnet 31.13.85.32 255.255.255.248 subnet 31.13.86.32 255.255.255.248 subnet 31.13.87.32 255.255.255.248 subnet 31.13.88.32 255.255.255.248 subnet 31.13.89.32 255.255.255.248 subnet 31.13.90.32 255.255.255.248 subnet 31.13.91.32 255.255.255.248 subnet 31.13.92.32 255.255.255.248 subnet 31.13.93.32 255.255.255.248 subnet 31.13.94.32 255.255.255.248 subnet 31.13.95.32 255.255.255.248

XWF Traffic Class	FBS Traffic Class
	subnet 66.220.149.254 255.255.255.255 subnet 69.171.239.13 255.255.255.255 subnet 69.171.250.32 255.255.255.248 subnet 69.171.252.252 255.255.255.255 subnet 69.171.255.13 255.255.255.255 subnet 102.132.96.32 255.255.255.248 subnet 102.132.97.32 255.255.255.248 subnet 102.132.98.32 255.255.255.248 subnet 102.132.99.32 255.255.255.248 subnet 102.132.100.32 255.255.255.248 subnet 102.132.101.32 255.255.255.248 subnet 102.132.102.32 255.255.255.248 subnet 102.132.103.32 255.255.255.248 subnet 102.132.104.32 255.255.255.248 subnet 102.132.105.32 255.255.255.248 subnet 102.132.106.32 255.255.255.248 subnet 102.132.107.32 255.255.255.248 subnet 102.132.108.32 255.255.255.248 subnet 102.132.109.32 255.255.255.248 subnet 102.132.110.32 255.255.255.248 subnet 102.132.111.32 255.255.255.248 subnet 157.240.0.32 255.255.255.248 subnet 157.240.1.32 255.255.255.248 subnet 157.240.2.32 255.255.255.248 subnet 157.240.3.32 255.255.255.248 subnet 157.240.4.32 255.255.255.248 subnet 157.240.5.32 255.255.255.248 subnet 157.240.6.32 255.255.255.248 subnet 157.240.7.32 255.255.255.248 subnet 157.240.8.32 255.255.255.248 subnet 157.240.9.32 255.255.255.248 subnet 157.240.10.32 255.255.255.248 subnet 157.240.11.32 255.255.255.248 subnet 157.240.12.32 255.255.255.248 subnet 157.240.13.32 255.255.255.248 subnet 157.240.14.32 255.255.255.248 subnet 157.240.15.32 255.255.255.248 subnet 157.240.16.32 255.255.255.248 subnet 157.240.17.32 255.255.255.248 subnet 157.240.18.32 255.255.255.248 subnet 157.240.19.32 255.255.255.248 subnet 157.240.20.32 255.255.255.248 subnet 157.240.21.32 255.255.255.248 subnet 157.240.22.32 255.255.255.248 subnet 157.240.23.32 255.255.255.248 subnet 157.240.24.32 255.255.255.248 subnet 157.240.25.32 255.255.255.248 subnet 157.240.26.32 255.255.255.248 subnet 157.240.27.32 255.255.255.248 subnet 157.240.28.32 255.255.255.248 subnet 157.240.29.32 255.255.255.248 subnet 157.240.30.32 255.255.255.248 subnet 157.240.31.32 255.255.255.248 subnet 157.240.192.32 255.255.255.248 subnet 157.240.193.32 255.255.255.248

XWF Traffic Class	FBS Traffic Class
	subnet 157.240.194.32 255.255.255.248 subnet 157.240.195.32 255.255.255.248 subnet 157.240.196.32 255.255.255.248 subnet 157.240.197.32 255.255.255.248 subnet 157.240.198.32 255.255.255.248 subnet 157.240.199.32 255.255.255.248 subnet 157.240.200.32 255.255.255.248 subnet 157.240.201.32 255.255.255.248 subnet 157.240.202.32 255.255.255.248 subnet 157.240.203.32 255.255.255.248 subnet 157.240.204.32 255.255.255.248 subnet 157.240.205.32 255.255.255.248 subnet 157.240.206.32 255.255.255.248 subnet 157.240.207.32 255.255.255.248 subnet 157.240.208.32 255.255.255.248 subnet 157.240.209.32 255.255.255.248 subnet 157.240.210.32 255.255.255.248 subnet 157.240.211.32 255.255.255.248 subnet 157.240.212.32 255.255.255.248 subnet 157.240.213.32 255.255.255.248 subnet 157.240.214.32 255.255.255.248 subnet 157.240.215.32 255.255.255.248 subnet 157.240.216.32 255.255.255.248 subnet 157.240.217.32 255.255.255.248 subnet 157.240.218.32 255.255.255.248 subnet 157.240.219.32 255.255.255.248 subnet 157.240.220.32 255.255.255.248 subnet 157.240.221.32 255.255.255.248 subnet 157.240.222.32 255.255.255.248 subnet 157.240.223.32 255.255.255.248 subnet 173.252.95.252 255.255.255.255 subnet 173.252.127.252 255.255.255.255 subnet 179.60.192.32 255.255.255.248 subnet 179.60.193.32 255.255.255.248 subnet 179.60.194.32 255.255.255.248 subnet 179.60.195.32 255.255.255.248 subnet 185.60.216.32 255.255.255.248 subnet 185.60.217.32 255.255.255.248 subnet 185.60.218.32 255.255.255.248 subnet 185.60.219.32 255.255.255.248

For more information on **wlan traffic-class <name>** command, see *Aruba Instant 8.x CLI Reference Guide*.

3. Create a new WLAN SSID profile or open the SSID settings of an existing WLAN SSID profile using the **wlan ssid-profile <profile-name>** command. Configure the **facebook-xwf-role <role-name>** parameter to enable Facebook Express Wi-Fi on the SSID and assign the user role created in step 1 for users connecting to the SSID. The following is an example configuration of enabling Facebook Express Wi-Fi and assigning the user role **FBClient** to facebook-xwf-role:

```
# wlan ssid-profile Express WiFi
(Instant AP)(SSID Profile "Express WiFi")# facebook-xwf-role FBClient
```

Chapter 14
Authentication and User Management

This chapter provides the following information:

- Overview of Instant AP Users on page 207
- Supported Authentication Methods on page 212
- Supported EAP Authentication Frameworks on page 224
- Configuring Authentication Servers on page 231
- Supported Encryption Types on page 242
- Authentication Survivability on page 243
- 802.1X Authentication on page 212
- 802.1X Supplicant Support on page 250
- MAC Authentication on page 215
- MAC Authentication with 802.1X Authentication on page 217
- MAC Authentication with Captive Portal Authentication on page 220
- WISPr Authentication on page 221
- Blacklisting Clients on page 251
- Authentication Certificates on page 254

Overview of Instant AP Users

The Instant AP users can be classified as follows:

- Administrator—An admin user who creates SSIDs, wired profiles, and DHCP server configuration parameters; and manages the local user database. The admin users can access the virtual controller Management UI.
- Guest administrator—A guest interface management user who manages guest users added in the local user database.
- Administrator with read-only access—The read-only admin user does not have access to the Instant CLI. The WebUI will be displayed in the read-only mode for these users.
- Employee users—Employees who use the enterprise network for official tasks.
- Guest users—Visiting users who temporarily use the enterprise network to access the Internet.

The user access privileges are determined by Instant AP management settings in the AirWave Management client and Aruba Central, and the type of the user. The following table outlines the access privileges defined for the admin user, guest management interface admin, and read-only users.

Table 74: *User Privileges*

User Category	Aruba Central or AMP in Management Mode	Instant AP in Monitor Mode or without AMP or Aruba Central
administrator	Access to local user database only	Complete access to the Instant AP
read-only administrator	No write privileges	No write privileges
guest administrator	Access to local user database only	Access to local user database only

Configuring Instant AP Users

The Instant user database consists of a list of guest and employee users. The addition of a user involves specifying the login credentials for a user. The login credentials for these users are provided outside the Instant system.

A guest user can be a visitor who is temporarily using the enterprise network to access the Internet. However, if you do not want to allow access to the internal network and the Intranet, you can segregate the guest traffic from the enterprise traffic by creating a guest WLAN and specifying the required authentication, encryption, and access rules.

An employee user is the employee who is using the enterprise network for official tasks. You can create Employee WLANs, specify the required authentication, encryption and access rules, and allow the employees to use the enterprise network.



The user database is also used when an Instant AP is configured as an internal RADIUS server.

The local user database of Instant APs can support up to 512 user entries.

The following procedure describes add, edit and delete an Instant AP user using the WebUI.

Table 75: *Managing Instant AP Users*

Old WebUI	New WebUI
Adding a new user: 1. Click the **Security** link located directly above the Search bar in the Instant main window. 2. Click **Users for Internal Server**, to view the contents of the **Users for Internal Server** tab. 3. Enter the user name in the **Username** text box. 4. Enter the password in the **Password** text box and reconfirm. 5. Select the type of network from the **Type** drop-down list. 6. Click **Add** and click **OK.** The users are listed in the **Users** list.	**Adding a new user:** 1. Navigate to the **Configuration** > **Security** page. 2. Expand **Users**. 3. Under **Users** click **+** to add a new user. 4. In the **Add new user** window, update the user name, password, and select the type of user from the **Type** drop-down list. 5. Click **OK**.
Editing User Settings:	**Editing User Settings:**

Old WebUI	New WebUI
1. Select the user you want to modify from the **Users** list in the table. 2. Click **Edit** to modify user settings. 3. Click **OK**.	1. Select the user you want to modify from the **Users** list in the table and click **Edit**. 2. Make the necessary changes to the user profile. 3. Click **OK**. 4. To delete a user,
Deleting a user: 1. Select the user you want to delete from the **Users** list in the table. 2. Click **Delete**. 3. To delete all or multiple users at a time, click **Delete All**. **NOTE:** Deleting a user only removes the user record from the user database, and will not disconnect the online user associated with the user name.	**Deleting a User:** 1. Select the user you want to delete from the **Users** list in the table and click **Delete**. 2. To delete all or multiple users at a time, click **Delete All**. **NOTE:** Deleting a user only removes the user record from the user database, and will not disconnect the online user associated with the user name.

The following CLI snippet allows you to configure an employee user:

```
(Instant AP)(config)# user <username> <password> radius
```

The following CLI snippet allows you to configure a guest user:

```
(Instant AP)(config)# user  <username> <password> portal
```

Configuring Authentication Parameters for Management Users

RADIUS or TACACS authentication servers can be configured to authenticate and authorize the management users of an Instant AP. The authentication servers determine if the user has access to administrative interface. The privilege level for different types of management users is defined on the RADIUS or TACACS server instead of the Instant AP. The Instant APs map the management users to the corresponding privilege level and provide access to the users based on the attributes returned by the RADIUS or TACACS server.

The following procedure describes how to configure authentication parameters for local admin, read-only, and guest management administrator account settings through the WebUI.

Table 76: *Configuring Authentication Parameters for Management Users*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **System** page. 2. Expand **Admin**. 3. Configure the settings defined in the Authentication Parameters for Management Users table below. 4. Click **Save**.	1. Navigate to **System** > **Admin**. 2. Configure the settings defined in the Authentication Parameters for Management Users table below. 3. Click **OK**.

Table 77: *Authentication Parameters for Management Users*

Type of User	Authentication Options	Steps to Follow
Local	**Internal**	Select **Internal** if you want to specify a single set of user credentials. If using an internal authentication server: 1. Specify the **Username** and **Password**. 2. Retype the password to confirm.
	Authentication server	Select the RADIUS or TACACS authentication servers. You can also create a new server by selecting **+** from the **Auth server 1** drop-down list. ■ **Authentication server w/ fallback to internal**— Select this option if you want to use both internal and external servers. When enabled, the authentication switches to **Internal** if there is no response from the RADIUS server (RADIUS server timeout). To use this option, select the authentication servers and configure the user credentials for internal-server-based authentication. ■ **Load balancing**—If two servers are configured, users can use them in the primary or backup mode, or load balancing mode. To enable load balancing, select **Enabled**. For more information on load balancing, see Dynamic Load Balancing between Two Authentication Servers on page 230. ■ **TACACS accounting**—If a TACACS server is selected, click the **TACACS accounting**toggle switch to report management commands, if required.
View Only	**Internal**	Select **Internal** to specify a single set of user credentials. If using an internal authentication server: 1. Specify the **Username** and **Password**. 2. Retype the password to confirm.
	Authentication server	If a RADIUS or TACACS server is configured, select **Authentication server** for authentication.
Guest Registration Only	**Internal**	Select **Internal** to specify a single set of user credentials. If using an internal authentication server: 1. Specify the **Username** and **Password**. 2. Retype the password to confirm.
	Authentication server	If a RADIUS or TACACS server is configured, select **Authentication server** for authentication.

The following CLI snippet allows you to configure a local admin user:

```
(Instant AP)(config)# mgmt-user <username> [password]
```

The following CLI snippet allows you to configure guest management administrator credentials:

```
(Instant AP)(config)# mgmt-user <username> [password] guest-mgmt
```

The following CLI snippet allows you to configure a user with read-only privilege:

```
(Instant AP)(config)# mgmt-user <username> [password] read-only
```

The following CLI snippet allows you to configure management authentication settings:

```
(Instant AP)(config)# mgmt-auth-server <server1>
(Instant AP)(config)# mgmt-auth-server <server2>
(Instant AP)(config)# mgmt-auth-server-load-balancing
(Instant AP)(config)# mgmt-auth-server-local-backup
```

The following CLI snippet allows you to enable TACACS accounting:

```
(Instant AP)(config)# mgmt-accounting command all
```

Blacklisting Unauthorized Users

An unauthorized user can attempt logging in to the Instant AP as an administrator using invalid credentials. Such unauthorized users can be blacklisted and blocked from the network by the administrator. The administrator can configure the count for unsuccessful login attempts, exceeding which the user will be blocked out of the system and the duration for which the user will be blacklisted.

When configured, the unauthorized user's IP address will be blacklisted in the **show mgmt-login-blacklist** table and will be barred from attempting logins to the network for the time period defined in **mgmt-login-blacklist-period**. The blacklist maintained for invalid users can contain up to 256 entries. The blacklist will be cleared when the number of entries exceed 256 or in the event of an AP reboot.

Configuring Blacklist for Unauthorized Users

Two parameters should be configured to blacklist an unauthorized user, the number of unsuccessful login attempts allowed and the time duration the unauthorized user should be blacklisted. This can be configured only through the CLI.

To configure the count for allowed unsuccessful login attempts, before the user is blacklisted, use the following command syntax:

mgmt-login-threshold <1-65535>

The following CLI commands configure the time period for blacklisting the user:

mgmt-login-blacklist-period <10-65535>, the value is measured in seconds.

```
(Instant AP) # configure terminal
(Instant AP) # mgmt-login-threshold <1-65535>
(Instant AP) # mgmt-login-blacklist-period <10-65535>
(Instant AP) #exit
```

The blacklisting feature can be turned off using the **no mgmt-login-threshold** command.

```
(Instant AP) # no mgmt-login-threshold
```

Adding Guest Users through the WebUI

The following procedure describes how to add guest users through the Instant WebUI:

New WebUI	Old WebUI
1. Log in to the WebUI with the guest management interface administrator credentials. The guest management interface is displayed. 2. To add a user, click **+**. The **User** window is displayed.	1. Log in to the WebUI with the guest management interface administrator credentials. The guest management interface is displayed. 2. To add a user, click **New**. The **New Guest User** popup window is displayed.

New WebUI	Old WebUI
3. Specify a **Username** and **Password**. 4. Retype the password to confirm. 5. Click **OK**.	3. Specify a **Username** and **Password**. 4. Retype the password to confirm. 5. Click **OK**.

Supported Authentication Methods

Authentication is a process of identifying a user through a valid username and password or based on the user's MAC addresses. The following authentication methods are supported in Instant:

- 802.1X Authentication
- MAC Authentication
- MAC Authentication with 802.1X Authentication
- MAC Authentication with Captive Portal Authentication
- Captive Portal Authentication
- 802.1X Authentication with Captive Portal Role
- WISPr Authentication
- Enhanced Open Authentication

802.1X Authentication

802.1X is an IEEE standard that provides an authentication framework for WLANs. The 802.1X standard uses the EAP to exchange messages during the authentication process. The authentication protocols that operate inside the 802.1X framework include EAP-TLS, PEAP, and EAP-TTLS. These protocols allow the network to authenticate the client while also allowing the client to authenticate the network. For more information on EAP authentication framework supported by the Instant APs, see Supported EAP Authentication Frameworks on page 224.

The 802.1X authentication method allows anInstant AP to authenticate the identity of a user before providing network access to the user. The RADIUS protocol provides centralized authentication, authorization, and accounting management. For authentication purpose, the wireless client can associate to a NAS or RADIUS client such as a wireless Instant AP. The wireless client can pass data traffic only after a successful 802.1X authentication. ArubaInstant supports the IMSI authentication process for device encryption. The EAP-AKA protocol is used with 802.1X to authenticate client access to a client network. The EAP-AKA makes use of IMSI as a permanent identity in the authentication exchange. It is a unique encryption method that is used to track device movement and protect user privacy.

This section consists of the following procedures:

- Configuring 802.1X Authentication for Wireless Network Profiles on page 213
- Configuring 802.1X Authentication for Wired Profiles on page 214

The Instant network supports internal RADIUS server and external RADIUS server for 802.1X authentication.

The steps involved in 802.1X authentication are as follows:

1. The NAS requests authentication credentials from a wireless client.
2. The wireless client sends authentication credentials to the NAS.
3. The NAS sends these credentials to a RADIUS server.

4. The RADIUS server checks the user identity and authenticates the client if the user details are available in its database. The RADIUS server sends an **Access-Accept** message to the NAS. If the RADIUS server cannot identify the user, it stops the authentication process and sends an **Access-Reject** message to the NAS. The NAS forwards this message to the client and the client must re-authenticate with appropriate credentials.
5. After the client is authenticated, the RADIUS server forwards the encryption key to the NAS. The encryption key is used for encrypting or decrypting traffic sent to and from the client.

In the 802.1X termination-disabled mode, if the identity in the **EAP-ID-Resp** message is longer than or equal to 248 octets and the identity contains **@FQDN** at the end, then the **EAP-ID-Resp** message is not dropped. The RADIUS User-Name attribute contains the truncated-string (up to 127 octets) from the original identify before the last **@FQDN** followed by the last **@FQDN**.



The NAS acts as a gateway to guard access to a protected resource. A client connecting to the wireless network first connects to the NAS.

Configuring 802.1X Authentication for Wireless Network Profiles

The following procedure describes how to configure 802.1X authentication for a wireless network profile in the WebUI or the CLI.

Table 78: *Configuring 802.1X Authentication for Wireless Network Profiles*

New WebUI	Old WebUI
1. In the **Configuration** > **Networks** page, click **+** to create a new WLAN network profile or select an existing profile for which you want to enable 802.1X authentication and click **edit**. 2. Ensure that all required WLAN and VLAN attributes are defined, and then click **Next**. 3. Under **Security** tab, specify the following parameters for the **Enterprise** security level: 4. Select any of the following options from the **Key management** drop-down list. ▪ **WPA2 Enterprise** ▪ **WPA Enterprise** ▪ **Both (WPA2 & WPA)** ▪ **Dynamic WEP with 802.1x**. If you do not want to use a session key from the RADIUS server to derive pairwise unicast keys, select the **Use Session Key for LEAP** check-box. 5. To terminate the EAP portion of 802.1X authentication on the Instant AP instead of the RADIUS server, toggle the **EAP Offload** switch. 6. By default, for 802.1X authentication, the client conducts an EAP exchange with the RADIUS server, and the Instant AP acts as a relay for this exchange. When **EAP Offload** is enabled, the Instant AP by itself acts as an authentication server	1. On the **Networks** tab, click **New** to create a new WLAN network profile or select an existing profile for which you want to enable 802.1X authentication and click **edit**. 2. In the **Edit <profile-name>** or the **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**. 3. On the **Security** tab, specify the following parameters for the **Enterprise** security level: 4. Select any of the following options from the **Key management** drop-down list. ▪ **WPA2 Enterprise** ▪ **WPA Enterprise** ▪ **Both (WPA2 & WPA)** ▪ **Dynamic WEP with 802.1x**. If you do not want to use a session key from the RADIUS server to derive pairwise unicast keys, select the **Session Key for LEAP** check-box. 5. To terminate the EAP portion of 802.1X authentication on the Instant AP instead of the RADIUS server, set **EAP Offload** to **Enabled**. 6. By default, for 802.1X authentication, the client conducts an EAP exchange with the RADIUS server, and the Instant AP acts as a relay for this exchange. When **EAP Offload** is enabled, the Instant AP by

New WebUI	Old WebUI
and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server. 7. Specify the type of authentication server to use and configure other required parameters. You can also configure two different authentication servers to function as primary and backup servers when **EAP Offload** is enabled. For more information on RADIUS authentication configuration parameters, see External RADIUS Server on page 231. 8. Click **Next** to define access rules, and then click **Finish** to apply the changes.	itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server. 7. Specify the type of authentication server to use and configure other required parameters. You can also configure two different authentication servers to function as primary and backup servers when **EAP Offload** is enabled. For more information on RADIUS authentication configuration parameters, see External RADIUS Server on page 231. 8. Click **Next** to define access rules, and then click **Finish** to apply the changes.

The following CLI commands configures 802.1X authentication for a wireless network:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# type {<Employee>|<Voice>}
(Instant AP)(SSID Profile <name>)# opmode {wpa2-aes|wpa-tkip|wpa-tkip,wpa2-
aes|dynamic-wep}
(Instant AP)(SSID Profile <name>)# leap-use-session-key
(Instant AP)(SSID Profile <name>)# termination
(Instant AP)(SSID Profile <name>)# auth-server <server1>
(Instant AP)(SSID Profile <name>)# auth-server <server2>
(Instant AP)(SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant AP)(SSID Profile <name>)# auth-survivability
(Instant AP)(SSID Profile <name>)# exit
(Instant AP)(config)# auth-survivability cache-time-out <hours>
```

Configuring 802.1X Authentication for Wired Profiles

The following procedure describes how to configure 802.1X authentication for a wired profile in the WebUI or the CLI.

Table 79: *Configuring 802.1X Authentication for Wired Profiles*

New WebUI	Old WebUI
1. Go to the **Configuration** > **Networks** page. 2. Click **+** under the **Networks** window to create a new network or select an existing profile for which you want to enable 802.1X authentication and then click **+**. 3. Under the **Basic** tab ensure that the required Wired and VLAN attributes are defined, and then click **Next**. 4. In the **Security** tab, toggle the **802.1X authentication** switch to enable. 5. Specify the type of authentication server to use and configure other required parameters. For more information on configuration parameters, see In the Old WebUI on page 165. 6. Click **Next** to define access rules and then click **Finish** to apply the changes.	1. Click the **Wired** link under **More** in the main window. The **Wired** window is displayed. 2. Click **New** under **Wired Networks** to create a new network or select an existing profile for which you want to enable 802.1X authentication and then click **Edit**. 3. In the **New Wired Network** or the **Edit Wired Network** window, ensure that all the required Wired and VLAN attributes are defined, and then click **Next**. 4. On the **Security** tab, select **Enabled** from the **802.1X authentication** drop-down list. 5. Specify the type of authentication server to use and configure other required parameters. For more information on configuration parameters, see In the Old WebUI on page 165.

New WebUI	Old WebUI
7. Assign the profile to an Ethernet port. For more information, see Assigning a Profile to Ethernet Ports on page 170.	6. Click **Next** to define access rules, and then click **Finish** to apply the changes. 7. Assign the profile to an Ethernet port. For more information, see Assigning a Profile to Ethernet Ports on page 170.

The following CLI commands configures 802.1X authentication for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# type {<employee>|<guest>}
(Instant AP)(wired ap profile <name>)# dot1x
(Instant AP)(wired ap profile <name>)# auth-server <server1>
(Instant AP)(wired ap profile <name>)# auth-server <server2>
(Instant AP)(wired ap profile <name>)# server-load-balancing
(Instant AP)(wired ap profile <name>)# radius-reauth-interval <Minutes>
```

MAC Authentication

MAC authentication is used for authenticating devices based on their physical MAC addresses. MAC authentication requires that the MAC address of a machine matches a manually defined list of addresses. This authentication method is not recommended for scalable networks and the networks that require stringent security settings.

MAC authentication can be used alone or it can be combined with other forms of authentication such as WEP authentication. However, it is recommended that you do not use the MAC-based authentication. The following MAC authentication combinations can be configured for a wired or wireless network profile.

- Configuring MAC Authentication for Wireless Network Profiles on page 215
- Configuring MAC Authentication for Wired Network Profiles on page 216

Configuring MAC Authentication for Wireless Network Profiles

The following procedure describes how to configure MAC authentication for a wired profile in the WebUI.

Table 80: *Configuring MAC Authentication for WIreless Network Profiles*

New WebUI	Old WebUI
1. In the **Configuration** > **Networks** page, click **+** to create a new network profile or select an existing profile for which you want to enable MAC authentication and click **Edit**. 2. Ensure that all required WLAN and VLAN attributes are defined, and then click **Next**. 3. In the **Security** tab, toggle the **MAC authentication** switch for the **Personal** or the **Open** security level. 4. In the **Authentication server 1** drop-down list, specify the type of authentication server to use. 5. To allow the Instant AP to use a delimiter in the MAC authentication request, specify a character (for example, colon or dash) as a delimiter for the	1. On the **Networks** tab, click **New** to create a new network profile or select an existing profile for which you want to enable MAC authentication and click **edit**. 2. In the **Edit <profile-name>** or the **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**. 3. On the **Security** tab, select **Enabled** from the **MAC authentication** drop-down list for the **Personal** or the **Open** security level. 4. In the **Authentication server 1** drop-down list, specify the type of authentication server to use. 5. If an internal authentication server is used, perform the following steps to allow MAC-address-

New WebUI	Old WebUI
MAC address string in the **Delimiter character** text box. For example, if you specify colon as the delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. 6. To allow the Instant AP to use uppercase letters in the MAC address string, toggle the **Uppercase support** switch to enable. **NOTE:** The **Delimiter character** and **Uppercase support** parameters are displayed only when MAC authentication is enabled. 7. Configure other parameters as required. 8. Click **Next** to define access rules, and then click **Finish** to apply the changes.	based authentication: ■ Click the **Users** link beside the **Internal server** parameter. The **Users** window is displayed. ■ Specify the client MAC address as the username and password. ■ Specify the type of the user (employee or guest). ■ Click **Add**. ■ Repeat the steps to add more users. ■ Click **OK**. 6. To allow the Instant AP to use a delimiter in the MAC authentication request, specify a character (for example, colon or dash) as a delimiter for the MAC address string in the **Delimiter character** text box. For example, if you specify colon as the delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. 7. To allow the Instant AP to use uppercase letters in the MAC address string, set **Uppercase support** to **Enabled**. **NOTE:** The **Delimiter character** and **Uppercase support** parameters are displayed only when MAC authentication is enabled. 8. Configure other parameters as required. 9. Click **Next** to define access rules, and then click **Finish** to apply the changes.

The following CLI commands configure MAC-address based authentication with external server:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# type {<Employee>|<Voice>|<Guest>}
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# mac-authentication-delimiter <delim>
(Instant AP)(SSID Profile <name>)# mac-authentication-upper-case
(Instant AP)(SSID Profile <name>)# external-server
(Instant AP)(SSID Profile <name>)# auth-server <server-name1>
(Instant AP)(SSID Profile <name>)# auth-server <server-name2>
(Instant AP)(SSID Profile <name>)# server-load-balancing
(Instant AP)(SSID Profile <name>)# radius-reauth-interval <minutes>
```

The following CLI command adds users for MAC authentication based on internal authentication server:

```
(Instant AP)(config)# user <username> [<password>] [portal|radius]
```

Configuring MAC Authentication for Wired Network Profiles

The following procedure describes how to configure MAC authentication for a wired profile in the WebUI or the CLI.

Table 81: *Configuring MAC Authentication for WIred Profiles*

New WebUI	Old WebUI
1. In the **Configuration** > **Networks** page, click **+** to create a new network profile or select an existing profile for which you want to enable MAC authentication and click **Edit**. 2. Ensure that all required wired and VLAN attributes are defined, and then click **Next**. 3. Under **Security** tab, toggle the **MAC authentication** switch to enable. 4. In the **Authentication server 1** drop-down list, specify the type of authentication server to use. 5. Configure other parameters as required. 6. Click **Next** to define access rules, and then click **Finish** to apply the changes.	1. Click the **Wired** link under **More** in the main window. The **Wired** window is displayed. 2. Click **New** under **Wired Networks** to create a new network or select an existing profile for which you want to enable MAC authentication and then click **Edit**. 3. In the **New Wired Network** or the **Edit Wired Network** window, ensure that all the required wired and VLAN attributes are defined, and then click **Next**. 4. Under **Security** tab, select **Enabled** from the **MAC authentication** drop-down list. 5. In the **Authentication server 1** drop-down list, specify the type of authentication server to use. 6. If an internal authentication server is used, perform the following steps to allow MAC-address-based authentication: ▪ Click the **Users** link beside **Internal server**. The **Users** window is displayed. ▪ Specify the client MAC address as the username and password. ▪ Specify the type of the user (employee or guest). ▪ Click **Add**. ▪ Repeat the steps to add more users. ▪ Click **OK**. 7. Configure other parameters as required. 8. Click **Next** to define access rules, and then click **Finish** to apply the changes. 9. Click **Next** to define access rules, and then click **Finish** to apply the changes.

The following CLI commands configure MAC-address-based authentication with external server:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# type {<employee>|<guest>}
(Instant AP)(wired ap profile <name>)# mac-authentication
(Instant AP)(wired ap profile <name>)# auth-server <server-1>
(Instant AP)(wired ap profile <name>)# auth-server <server-2>
(Instant AP)(wired ap profile <name>)# server-load-balancing
(Instant AP)(wired ap profile <name>)# radius-reauth-interval <Minutes>
```

The following CLI command adds users for MAC authentication based on internal authentication server:

```
(Instant AP)(config)# user <username> [<password>] [portal|radius]
```

MAC Authentication with 802.1X Authentication

MAC Authentication with 802.1X Authentication method has the following features:

- MAC authentication precedes 802.1X authentication—The administrators can enable MAC authentication for 802.1X authentication. MAC authentication shares all the authentication server configurations with 802.1X authentication. If a wireless or wired client connects to the network, MAC authentication is performed first. If MAC authentication fails, 802.1X authentication does not trigger. If MAC authentication is successful, 802.1X authentication is attempted. If 802.1X authentication is successful, the client is assigned an 802.1X authentication role. If 802.1X authentication fails, the client is assigned a **deny-all** role or **mac-auth-only** role.
- MAC authentication only role—Allows you to create a **mac-auth-only** role to allow role-based access rules when MAC authentication is enabled for 802.1X authentication. The **mac-auth-only** role is assigned to a client when the MAC authentication is successful and 802.1X authentication fails. If 802.1X authentication is successful, the **mac-auth-only** role is overwritten by the final role. The **mac-auth-only** role is primarily used for wired clients.
- L2 authentication fall-through—Allows you to enable the **l2-authentication-fallthrough** mode. When this option is enabled, the 802.1X authentication is allowed even if the MAC authentication fails. If this option is disabled, 802.1X authentication is not allowed. The **l2-authentication-fallthrough** mode is disabled by default.
- For more information on configuring anInstant AP to use MAC as well as 802.1X authentication, see 802.1X Authentication on page 212.

This section consists of the following procedures:

- Configuring MAC and 802.1X Authentications for Wireless Network Profiles
- Configuring MAC and 802.1X Authentications for Wireless Network Profiles

Configuring MAC and 802.1X Authentications for Wireless Network Profiles

Table 82: *Configuring MAC and 802.1X Authentication for Wireless Network Profiles*

New WebUI	Old WebUI
1. In the **Configuration** > **Networks** section, click **+** to create a new network profile or select an existing profile for which you want to enable MAC and 802.1X authentications and click **Edit**. 2. Ensure that all required WLAN and VLAN attributes are defined, and then click **Next**. 3. Under **Security** tab, select **Enterprise** from the **Security Level** drop-down list. Ensure that the required parameters for MAC authentication and 802.1X authentication are configured. 4. Select the **Perform MAC authentication before 802.1X** check box to use 802.1X authentication only when the MAC authentication is successful. 5. Select the **MAC authentication fail-thru** check box to use 802.1X authentication even when the MAC authentication fails. 6. Click **Next** and until **Finish** to apply the changes.	1. On the **Networks** tab, click **New** to create a new network profile or select an existing profile for which you want to enable MAC and 802.1X authentications and click **edit**. 2. In the **Edit <profile-name>** or the **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**. 3. On the **Security** tab, move the slider to the **Enterprise** security level. Ensure that the required parameters for MAC authentication and 802.1X authentication are configured. 4. Select the **Perform MAC authentication before 802.1X** check box to use 802.1X authentication only when the MAC authentication is successful. 5. Select the **MAC authentication fail-thru** check box to use 802.1X authentication even when the MAC authentication fails. 6. Click **Next** and then click **Finish** to apply the changes.

The following CLI commands configure MAC and 802.1X Authentications for a Wireless Network profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# type {<Employee>|<Voice>|<Guest>}
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# l2-auth-failthrough
(Instant AP)(SSID Profile <name>)# auth-server <server-name1>
(Instant AP)(SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant AP)(SSID Profile <name>)# auth-survivability
(Instant AP)(SSID Profile <name>)# exit
(Instant AP)(config)# auth-survivability cache-time-out <hours>
```

Configuring MAC and 802.1X Authentications for Wired Network Profiles

The following procedure describes how to configure MAC and 802.1X authentications for a wired profile in the WebUI.

Table 83: *Configuring MAC and 802.1X Authentication for Wired Profiles*

New WebUI	Old WebUI
1. In the **Configuration** > **Networks** section, click **+** to create a new network profile or select an existing profile for which you want to enable MAC and 802.1X authentications and click **Edit**. 2. Ensure that all required WLAN and VLAN attributes are defined, and then click **Next**. 3. Under **Security** tab, perform the following steps: a. Toggle the **MAC authentication** switch to enable. b. Toggle the **802.1X authentication** switch to enable. c. Toggle the **MAC authentication fail-thru** switch to enable. 4. In the **Authentication server 1** drop-down list, specify the type of authentication server to use and configure other required parameters. For more information on configuration parameters, see In the Old WebUI on page 165. 5. Click **Next** to define access rules, and then click **Finish** to apply the changes.	1. Click the **Wired** link under **More** in the main window. The **Wired** window is displayed. 2. Click **New** under **Wired Networks** to create a new network or select an existing profile for which you want to enable MAC authentication and then click **Edit**. 3. In the **New Wired Network** or the **Edit Wired Network** window, ensure that all the required wired and VLAN attributes are defined, and then click **Next**. 4. On the **Security** tab, perform the following steps: a. Select **Enabled** from the **MAC authentication** drop-down list. b. Select **Enabled** from the **802.1X authentication** drop-down list. c. Select **Enabled** from the **MAC authentication fail-thru** drop-down list. 5. In the **Authentication server 1** drop-down list, specify the type of authentication server to use and configure other required parameters. For more information on configuration parameters, see In the Old WebUI on page 165. 6. Click **Next** to define access rules, and then click **Finish** to apply the changes.

The following CLI commands enable MAC and 802.1X authentications for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile "<name>")# type {<employee>|<guest>}
(Instant AP)(wired ap profile "<name>")# mac-authentication
(Instant AP)(wired ap profile "<name>")# dot1x
(Instant AP)(wired ap profile "<name>")# l2-auth-failthrough
(Instant AP)(wired ap profile "<name>")# auth-server <name>
(Instant AP)(wired ap profile "<name>")# server-load-balancing
(Instant AP)(wired ap profile "<name>")# radius-reauth-interval <Minutes>
```

MAC Authentication with Captive Portal Authentication

You can enforce MAC authentication for captive portal clients. The following configuration conditions apply to MAC and captive portal authentication method:

- If the captive portal splash page type is **Internal-Authenticated** or **External-RADIUS Server**, MAC authentication reuses the server configurations.
- If the captive portal splash page type is **Internal-Acknowledged** or **External-Authentication Text** and MAC authentication is enabled, a server configuration page is displayed.

Configuring MAC Authentication with Captive Portal Authentication

The following procedure describes how to configure the MAC authentication with captive portal authentication for a network profile using the WebUI.

Table 84: *Configuring MAC Authentication with Captive Portal Authentication*

New WebUI	Old WebUI
1. In the **Configuration** > **Networks** section, click **+** to create a new network profile or select an existing profile for which you configure internal captive portal authentication for a WLAN SSID or a wired profile and click **Edit**. **NOTE:** To enable MAC authentication with captive portal authentication on a new WLAN SSID or wired profile, click the **Security** tab on the **New WLAN** window and the **New Wired Network** window. 2. Select the **Security** tab and specify the following parameters: a. Toggle the **MAC authentication** switch to enable MAC authentication for captive portal users. If the MAC authentication fails, the captive portal authentication role is assigned to the client. b. In case of a wired profile for employee access, toggle the **802.1X authentication** switch to enable. This is in addition to enabling MAC authentication. c. In case of a wired profile for guess access, select a profile from the **Captive portal profile** drop-down list. This is in addition to enabling MAC authentication. d. To enforce MAC authentication, go to the **Access** tab, select **Role-based** from the **Access Rules** drop-down list, and toggle the **Enforce MAC auth only role** switch to enable. 3. Click **Next** and then click **Finish** to apply the changes. **NOTE:** The **Enforce MAC auth only role** parameter is	1. Select an existing wireless or wired profile for which you want to enable MAC with captive portal authentication. Depending on the network profile selected, the **Edit <WLAN-Profile>** or the **Edit Wired Network** window is displayed. **NOTE:** To enable MAC authentication with captive portal authentication on a new WLAN SSID or wired profile, click the **Security** tab on the **New WLAN** window and the **New Wired Network** window. 2. On the **Security** tab, specify the following parameters: a. Select **Enabled** from the **MAC authentication** drop-down list to enable MAC authentication for captive portal users. If the MAC authentication fails, the captive portal authentication role is assigned to the client. b. In case of a wired profile, select the **802.1X authentication** check box in addition to **MAC authentication**. c. To enforce MAC authentication, click the **Access** tab and select **Enforce MAC auth only role** check box. 3. Click **Next** and then click **Finish** to apply the changes.

New WebUI	Old WebUI
not supported on a WLAN profile for employee access.	

The following CLI commands configure MAC authentication with captive portal authentication for a wireless profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# type <guest>
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# captive-portal {<type> [exclude-uplink
<types>]|external [Profile <name>] [exclude-uplink <types>]}
(Instant AP)(SSID Profile <name>)# set-role-mac-auth <mac-only>
```

The following CLI commands configure MAC authentication with captive portal authentication for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# type <guest>
(Instant AP)(wired ap profile <name>)# mac-authentication
(Instant AP)(wired ap profile <name>)# captive-portal <type>
(Instant AP)(wired ap profile <name>)# captive-portal {<type> [exclude-uplink
<types>]|external [Profile <name>] [exclude-uplink <types>]}
(Instant AP)(wired ap profile <name>)# set-role-mac-auth <mac-only>
```

Captive Portal Authentication

Captive portal authentication is used for authenticating guest users. For more information on captive portal authentication, see Captive Portal for Guest Access

802.1X Authentication with Captive Portal Role

This authentication mechanism allows you to configure different captive portal settings for clients on the same SSID. For example, you can configure an 802.1X SSID and create a role for captive portal access, so that some of the clients using the SSID derive the captive portal role. You can configure rules to indicate access to external or internal captive portal, or none. For more information on configuring captive portal roles for an SSID with 802.1X authentication, see Configuring Captive Portal Roles for an SSID on page 200.

WISPr Authentication

WISPr authentication allows the smart clients to authenticate on the network when they roam between WISP even if the wireless hotspot uses an ISP with whom the client may not have an account.

If a hotspot is configured to use WISPr authentication in a specific ISP and a client attempts to access the Internet at that hotspot, the WISPr AAA server configured for the ISP authenticates the client directly and allows the client to access the network. If the client only has an account with a *partner* ISP, the WISPr AAA server forwards the client's credentials to the partner ISP's WISPr AAA server for authentication. When the client is authenticated on the partner ISP, it is also authenticated on the hotspot's own ISP as per their service agreements. The Instant AP assigns the default WISPr user role to the client when the client's ISP sends an authentication message to the Instant AP.

Configuring WISPr Authentication

Instant supports the following smart clients:

- iPass
- Boingo

These smart clients enable client authentication and roaming between hotspots by embedding iPass Generic Interface Specification *redirect*, *authentication*, and *logoff* messages within HTML messages that are sent to the Instant AP.



WISPr authentication is supported only for the **Internal - Authenticated** and **External** captive portal authentication. Select the **Internal – Authenticated** or the **External** option from the **Splash page type** drop-down list to configure WISPr authentication for a WLAN profile.

The following procedure describes how to configure WISPr authentication using the WebUI.

Table 85: *Configuring WISPr Authentication*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **System** page. 2. Click **Show advanced options** at the bottom of the page. 3. Expand **WISPr**. 4. In the **ISO country code** text box enter the ISO Country Code for the WISPr Location ID. 5. In the **E.164 country code** text box enter the E.164 Country Code for the WISPr Location ID. 6. In the **E.164 area code** text box enter the E.164 Area Code for the WISPr Location ID. 7. In the **SSID/Zone** text box enter the SSID or the zone name for the WISPr Location ID. 8. In the **Operator name** text box enter the operator name of the hotspot. 9. In the **Location name** text box enter the name of the Hotspot location. If no name is defined, the name of the Instant AP to which the user is associated is used. 10. Click **Save** to apply the changes.	1. Click the **System** link located directly above the Search bar in the Instant main window. The **System** window is displayed. 2. Click **Show advanced options**. 3. Click **WISPr** tab. The **WISPr** tab contents are displayed. 4. Enter the ISO Country Code for the WISPr Location ID in the **ISO country code** text box. 5. Enter the E.164 Area Code for the WISPr Location ID in the **E.164 area code** text box. 6. Enter the operator name of the hotspot in the **Operator name** text box. 7. Enter the E.164 Country Code for the WISPr Location ID in the **E.164 country code** text box. 8. Enter the SSID or the zone name for the WISPr Location ID in the **SSID/Zone** text box. 9. Enter the name of the Hotspot location in the **Location name** text box. If no name is defined, the name of the Instant AP to which the user is associated is used. 10. Click **OK** to apply the changes.

The WISPr RADIUS attributes and configuration parameters are specific to the RADIUS server used by your ISP for the WISPr authentication. Contact your ISP to determine these values. You can find a list of ISO and ITU country and area codes at the ISO and ITU websites (www.iso.org and http://www.itu.int).



A Boingo smart client uses a NAS identifier in the <CarrierID>_<VenueID> format for location identification. To support Boingo clients, ensure that you configure the NAS identifier parameter in the RADIUS server profile for the WISPr server.

The following CLI commands configure WISPr authentication:

```
(Instant AP)(config)# wlan wispr-profile
(Instant AP)(WISPr)# wispr-location-id-ac
(Instant AP)(WISPr)# wispr-location-id-cc
(Instant AP)(WISPr)# wispr-location-id-isocc
(Instant AP)(WISPr)# wispr-location-id-network
(Instant AP)(WISPr)# wispr-location-name-location
(Instant AP)(WISPr)# wispr-location-name-operator-name
```

Enhanced Open Authentication

Enhanced open provides improved data encryption in open Wi-Fi networks and protects data from sniffing. Enhanced open replaces open system as the default option. With enhanced open, the client and WLAN perform Diffie-Hellman key exchange during the access procedure and use the resulting pairwise key with a 4-way handshake.

Aruba Instant supports the following Enhanced Open authentication types:

- Enhanced Open without PMK caching
- Enhanced Open with PMK caching
- Enhanced Open transition mode

Enhanced Open Without PMK Caching

In the Enhanced Open opmode without PMK caching, the 802.11 beacon, probe response frame, and authentication request or response frame are generic. However, 802.11 association request or response are specific for enhanced open that does not include PMK caching.

Aruba Instant advertises support for enhanced open by using an AKM suite selector in all beacons and probe response frames. Besides, PMF is set to required (MFPR=1). Authentication request and authentication response use open authentication.

A client that wishes to perform data encryption in an open Wi-Fi network using enhanced open, indicates enhanced open AKM in the 802.11 association request with PMF is required (MFPR=1). The DHPE contains group and the Diffie-Hellman public Key from the client. Instant supports Diffie-Hellman 256-bit Elliptic Curve groups 19, 20, and 21.

Instant includes the enhanced open AKM and DHPE in the 802.11 association response after agreeing to enhanced open with PME is required (MFPR=1). The DHPE contains group and the Diffie-Hellman public key from Instant. If Instant does not support the group indicated in the received 802.11 association request, it responds with an 802.11 association response having the status code 77. A status code 77 indicates unsupported finite cyclic group.

After completing the 802.11 association, PMK and its associated PMKID are created. Instant initiates a 4-way handshake with the client using the generated PMK. The result of the 4-way handshake is the encryption key to protect bulk unicast data and broadcast data between the client and Instant.

Enhanced Open With PMK Caching

If enhanced open has been established earlier, a client that wishes to perform enhanced open with PMK caching includes a PMKID in its 802.11 association request in addition to the enhanced open AKM, DHPE, and PMF is required(MFPR=1). If Aruba Instant has cached the PMK identified by that PMKID, it includes the PMKID in its 802.11 association response but does not include the DHPE. If Instant has not cached the PMK identified by that PMKID, it ignores the PMKID and proceeds with enhanced open association by including a DHPE. The 4-way handshake is initiated subsequently.

Enhanced Open Transition Mode

The enhanced open transition mode enables a seamless transition from open unencrypted WLAN connections without adversely impacting the end user experience. It provides the ability for enhanced open and non-enhanced open clients to connect to the same open system virtual AP.

Two different SSIDs are created for each configured 802.11 open system virtual AP, one for enhanced open authentication and another for open networks. Both SSIDs operate either in the same band and channel or the band and channel of the other SSID (the enhanced open transition mode information element includes the band and channel information). Aruba Instant always uses the same band and channel.

802.11 beacon and probe response frames of the open BSS include an enhanced open transition mode information element to encapsulate BSSID and SSID of the enhanced open BSS.

802.11 beacon and probe response frames from the enhanced open BSS include an enhanced open transition mode information element to encapsulate the BSSID and SSID of the open BSS. Besides, the beacon frame from the enhanced open BSS has zero length SSID and indicates enhanced open in robust security network element.

In enhanced open transition mode, Aruba Instant uses more virtual APs than configured . The number of virtual APs pushed depends on multizone parameters, if configured (maximum SSIDs per zone). During enhanced open transition mode, depending on the available VAP slots, Instant will either push both open and enhanced open virtual APs or only enhanced-open virtual APs. There will be no impact on other virtual APs configured. An additional enhanced-open virtual AP will be pushed to an AP only if it has an available extra slot.

During transition, if there are many enhanced-open enabled virtual APs, based on the availability of slots, the AP will choose to transition all enhanced-open virtual APs or configure them as enhanced-open-only virtual APs. That is, if there are 2 enhanced-open virtual APs and 4 available slots, the AP will create 2 enhanced-open-only virtual APs and 2 open virtual APs. If the available slots are 3, the AP will create 2 enhanced-open-only virtual APs and no open virtual APs.

Configuring Enhanced Open

The following procedure describes how to enable enhanced open security using the New WebUI:

1. Navigate to the WLAN wizard (To add a new profile, go to **Configuration > Networks** and click **+**. To modify an existing profile, go to **Configuration > Networks** , select a WLAN SSID from the list of networks to edit.
2. Click the **Security** tab.
3. Select **Open** from the **Security Level** drop-down list. The authentication options applicable to the Open network are displayed.
4. The **Enhanced Open** toggle switch is disabled by default. Slide the toggle switch to the right-side to enable the enhanced open function.

The following CLI commands enable enhanced open:

```
(Instant AP)(config)# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile "<profile_name>")# opmode enhanced-open
```

The following CLI commands disable enhanced open:

```
(Instant AP)(config)# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile "<profile_name>")# no opmode
```

The following CLI commands enable opmode transition:

```
(Instant AP)(config)# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile "<profile_name>")# opmode-transition
```

The following CLI commands disable opmode transition:

```
(Instant AP)(config)# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile "<profile_name>")# opmode-transition-disable
```

Supported EAP Authentication Frameworks

The following EAP authentication frameworks are supported in the Instant network:

- EAP-TLS—The EAP-TLS method supports the termination of EAP-TLS security using the internal RADIUS server . The EAP-TLS requires both server and CA certificates installed on the Instant AP. The client certificate is verified on the virtual controller (the client certificate must be signed by a known CA) before the username is verified on the authentication server.
- EAP-TTLS —The EAP-TTLS method uses server-side certificates to set up authentication between clients and servers. However, the actual authentication is performed using passwords.
- EAP-PEAP—EAP-PEAP is an 802.1X authentication method that uses server-side public key certificates to authenticate clients with server. The PEAP authentication creates an encrypted SSL/TLS tunnel between the client and the authentication server. Exchange of information is encrypted and stored in the tunnel ensuring the user credentials are kept secure.
- LEAP—LEAP uses dynamic WEP keys for authentication between the client and authentication server.

To use the Instant AP's internal database for user authentication, add the usernames and passwords of the users to be authenticated.



Aruba does not recommend the use of LEAP authentication, because it does not provide any resistance to network attacks.

Authentication Termination on Instant AP

Instant APs support EAP termination for enterprise WLAN SSIDs. The EAP termination can reduce the number of exchange packets between the Instant AP and the authentication servers. Instant allows EAP termination for PEAP-GTC and PEAP-MS-CHAV2. PEAP-GTC termination allows authorization against a LDAP server and external RADIUS server while PEAP-MS-CHAV2 allows authorization against an external RADIUS server.

This allows the users to run PEAP-GTC termination with their username and password to a local Microsoft Active Directory server with LDAP authentication.

- EAP-GTC—This EAP method permits the transfer of unencrypted usernames and passwords from the client to the server. The main uses for EAP-GTC are procuring one-time token cards such as SecureID and using LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the Instant AP to an external authentication server for user data backup.
- EAP-MSCHAPv2—This EAP method is widely supported by Microsoft clients. A RADIUS server must be used as the back-end authentication server.

Supported Authentication Servers

Instant supports the following server types for client authentication:

- Internal RADIUS Server on page 225
- External RADIUS Server on page 226
- TACACS Servers on page 230

Instant supports load balancing between two authentication servers to maximize efficiency by switching between the configured authentication servers without the intervention of the administrator. To know more, read Dynamic Load Balancing between Two Authentication Servers.

Internal RADIUS Server

Each Instant AP has an instance of free RADIUS server operating locally. When you enable the internal RADIUS server option for the network, the client on the Instant AP sends a RADIUS packet to the local IP

address. The internal RADIUS server listens and replies to the RADIUS packet. Instant serves as a RADIUS server for 802.1X authentication. However, the internal RADIUS server can also be configured as a backup RADIUS server for an external RADIUS server.

External RADIUS Server

In the external RADIUS server, the IP address of the virtual controller is configured as the NAS IP address. Instant RADIUS is implemented on the virtual controller and this eliminates the need to configure multiple NAS clients for every Instant AP on the RADIUS server for client authentication. Instant RADIUS dynamically forwards all the authentication requests from a NAS to a remote RADIUS server. The RADIUS server responds to the authentication request with an **Access-Accept** or **Access-Reject** message, and the clients are allowed or denied access to the network depending on the response from the RADIUS server. When you enable an external RADIUS server for the network, the client on the Instant AP sends a RADIUS packet to the local IP address. The external RADIUS server then responds to the RADIUS packet.

Instant supports the following external authentication servers:

- RADIUS
- LDAP
- ClearPass Policy Manager Server for AirGroup CoA

To use an LDAP server for user authentication, configure the LDAP server on the virtual controller, and configure user IDs and passwords. To use a RADIUS server for user authentication, configure the RADIUS server on the virtual controller.

RADIUS Server Authentication with VSA

An external RADIUS server authenticates network users and returns to the Instant AP the VSA that contains the name of the network role for the user. The authenticated user is placed into the management role specified by the VSA.

Instant supports the following VSAs for user role and VLAN derivation rules:

- AP-Group
- AP-Name
- ARAP-Features
- ARAP-Security
- ARAP-Security-Data
- ARAP-Zone-Access
- Acct-Authentic
- Acct-Delay-Time
- Acct-Input-Gigawords
- Acct-Input-Octets
- Acct-Input-Packets
- Acct-Interim-Interval
- Acct-Link-Count
- Acct-Multi-Session-Id
- Acct-Output-Gigawords
- Acct-Output-Octets
- Acct-Output-Packets

- Acct-Session-Id
- Acct-Session-Time
- Acct-Status-Type
- Acct-Terminate-Cause
- Acct-Tunnel-Packets-Lost
- Add-Port-To-IP-Address
- Aruba-AP-Group
- Aruba-AP-IP-Address
- Aruba-AS-Credential-Hash
- Aruba-AS-User-Name
- Aruba-Admin-Path
- Aruba-Admin-Role
- Aruba-AirGroup-Device-Type
- Aruba-AirGroup-Shared-Group
- Aruba-AirGroup-Shared-Role
- Aruba-AirGroup-Shared-User
- Aruba-AirGroup-User-Name
- Aruba-AirGroup-Version
- Aruba-Auth-SurvMethod
- Aruba-Auth-Survivability
- Aruba-CPPM-Role
- Aruba-Calea-Server-Ip
- Aruba-Device-Type
- Aruba-Essid-Name
- Aruba-Framed-IPv6-Address
- Aruba-Location-Id
- Aruba-Mdps-Device-Iccid
- Aruba-Mdps-Device-Imei
- Aruba-Mdps-Device-Name
- Aruba-Mdps-Device-Product
- Aruba-Mdps-Device-Profile
- Aruba-Mdps-Device-Serial
- Aruba-Mdps-Device-Udid
- Aruba-Mdps-Device-Version
- Aruba-Mdps-Max-Devices
- Aruba-Mdps-Provisioning-Settings
- Aruba-Named-User-Vlan
- Aruba-Network-SSO-Token
- Aruba-No-DHCP-Fingerprint
- Aruba-Port-Bounce-Host
- Aruba-Port-Id
- Aruba-Priv-Admin-User
- Aruba-Template-User

- Aruba-User-Group
- Aruba-User-Role
- Aruba-User-Vlan
- Aruba-WorkSpace-App-Name
- Authentication-Sub-Type
- Authentication-Type
- CHAP-Challenge
- Callback-Id
- Callback-Number
- Chargeable-User-Identity
- Cisco AV-Pair
- Class
- Connect-Info
- Connect-Rate
- Crypt-Password
- DB-Entry-State
- Digest-Response
- Domain-Name
- EAP-Message
- Error-Cause
- Event-Timestamp
- Exec-Program
- Exec-Program-Wait
- Expiration
- Fall-Through
- Filter-Id
- Framed-AppleTalk-Link
- Framed-AppleTalk-Network
- Framed-AppleTalk-Zone
- Framed-Compression
- Framed-IP-Address
- Framed-IP-Netmask
- Framed-IPX-Network
- Framed-IPv6-Pool
- Framed-IPv6-Prefix
- Framed-IPv6-Route
- Framed-Interface-Id
- Framed-MTU
- Framed-Protocol
- Framed-Route
- Framed-Routing
- Full-Name
- Group

- Group-Name
- Hint
- Huntgroup-Name
- Idle-Timeout
- Location-Capable
- Location-Data
- Location-Information
- Login-IP-Host
- Login-IPv6-Host
- Login-LAT-Node
- Login-LAT-Port
- Login-LAT-Service
- Login-Service
- Login-TCP-Port
- Menu
- Message-Auth
- NAS-IPv6-Address
- NAS-Port-Type
- Operator-Name
- Password
- Password-Retry
- Port-Limit
- Prefix
- Prompt
- Rad-Authenticator
- Rad-Code
- Rad-Id
- Rad-Length
- Reply-Message
- Requested-Location-Info
- Revoke-Text
- Server-Group
- Server-Name
- Service-Type
- Session-Timeout
- Simultaneous-Use
- State
- Strip-User-Name
- Suffix
- Termination-Action
- Termination-Menu
- Tunnel-Assignment-Id
- Tunnel-Client-Auth-Id

- Tunnel-Client-Endpoint
- Tunnel-Connection-Id
- Tunnel-Medium-Type
- Tunnel-Preference
- Tunnel-Private-Group-Id
- Tunnel-Server-Auth-Id
- Tunnel-Server-Endpoint
- Tunnel-Type
- User-Category
- User-Name
- User-Vlan
- Vendor-Specific
- fw_mode
- dhcp-option
- dot1x-authentication-type
- mac-address
- mac-address-and-dhcp-options

TACACS Servers

You can now configure a TACACS server as the authentication server to authenticate and authorize all types of management users, and account user sessions. When configured, the TACACS server allows a remote access server to communicate with an authentication server to determine if the user has access to the network. The Instant AP users can create several TACACS server profiles and associate these profiles to the user accounts to enable authentication of the management users.

TACACS supports the following types of authentication:

- ASCII
- PAP
- CHAP
- ARAP
- MS-CHAP



The TACACS server cannot be attributed to any SSID or wired profile in general as the authentication server and is configured only for the Instant AP management users.

Dynamic Load Balancing between Two Authentication Servers

Two authentication servers can be configured to serve as a primary and backup RADIUS server and enable load balancing between these servers. Load balancing of authentication servers ensures that the authentication load is split across multiple authentication servers and enables the Instant APs to perform load balancing of authentication requests destined to authentication servers such as RADIUS or LDAP.

The load balancing in Instant AP is performed based on outstanding authentication sessions. If there are no outstanding sessions and if the rate of authentication is low, only primary server will be used. The secondary is used only if there are outstanding authentication sessions on the primary server. With

this, the load balance can be performed across RADIUS servers of asymmetric capacity without the need to obtain inputs about the server capabilities from the administrators.

Configuring Authentication Servers

This section describes the following procedures:

- Configuring an External Server for Authentication on page 231
- Enabling RADIUS Communication over TLS (RadSec) on page 237
- Configuring Dynamic RADIUS Proxy Parameters on page 239

External RADIUS Server

In the external RADIUS server, the IP address of the virtual controller is configured as the NAS IP address. Instant RADIUS is implemented on the virtual controller and this eliminates the need to configure multiple NAS clients for every Instant AP on the RADIUS server for client authentication. Instant RADIUS dynamically forwards all the authentication requests from a NAS to a remote RADIUS server. The RADIUS server responds to the authentication request with an **Access-Accept** or **Access-Reject** message, and the clients are allowed or denied access to the network depending on the response from the RADIUS server. When you enable an external RADIUS server for the network, the client on the Instant AP sends a RADIUS packet to the local IP address. The external RADIUS server then responds to the RADIUS packet.

Instant supports the following external authentication servers:

- RADIUS
- LDAP
- ClearPass Policy Manager Server for AirGroup CoA

To use an LDAP server for user authentication, configure the LDAP server on the virtual controller, and configure user IDs and passwords. To use a RADIUS server for user authentication, configure the RADIUS server on the virtual controller.

Configuring an External Server for Authentication

The following procedure describes how to configure RADIUS, TACACS, LDAP, and ClearPass Policy Manager servers using the WebUI.

Table 86: *Configuring an External Server for Authentication*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **Security** page. 2. Expand **Authentication Servers**. 3. To create a new server, click **+**. The **New Authentication Server** window for specifying details for the new server is displayed. 4. Configure parameters based on the type of sever. ▪ **RADIUS**—To configure a RADIUS server, specify the attributes described in the RADIUS Server Configuration Parameters table below. To assign the RADIUS authentication server to a network profile, select the newly added server	1. Navigate to **Security** > **Authentication Servers**. The **Security** window is displayed. 2. To create a new server, click **New**. A window for specifying details for the new server is displayed. 3. Configure parameters based on the type of sever. ▪ **RADIUS**—To configure a RADIUS server, specify the attributes described in the RADIUS Server Configuration Parameters table below. To assign the RADIUS authentication server to a network profile, select the newly added server when configuring security settings for a wireless or wired network profile.

New WebUI	Old WebUI
when configuring security settings for a wireless or wired network profile. **NOTE:** You can also add an external RADIUS server by selecting the **New** option when configuring a WLAN or wired profile. For more information, see Points to Remember on page 145 and In the Old WebUI on page 165. ▪ **LDAP**—To configure an LDAP server, select the **LDAP** option and configure the attributes described in the LDAP Server Configuration Parameters table below. ▪ **TACACS**—To configure TACACS server, select the **TACACS** option and configure the attributes described in the TACACS Server Configuration parameters table below. **NOTE:** You can also add TACACS server by selecting the **New** option when configuring authentication parameters for management users. For more information, see Configuring Authentication Parameters for Management Users on page 209. ▪ **CoA only** for AirGroup CoA—To configure a ClearPass Policy Manager server used for AirGroup CoA, select the **CoA only** check box and configure the attributes defined in the ClearPass Policy Manager Server Configuration Parameters for AirGroup CoA table below. The RADIUS server is automatically selected. **NOTE:** The ClearPass Policy Manager server acts as a RADIUS server and asynchronously provides the AirGroup parameters for the client device including shared user, role, and location. 5. Click **OK**.	**NOTE:** You can also add an external RADIUS server by selecting the **New** option when configuring a WLAN or wired profile. For more information, see Points to Remember on page 145 and In the Old WebUI on page 165. ▪ **LDAP**—To configure an LDAP server, select the **LDAP** option and configure the attributes described in the LDAP Server Configuration Parameters table below. ▪ **TACACS**—To configure TACACS server, select the **TACACS** option and configure the attributes described in the TACACS Server Configuration parameters table below. **NOTE:** You can also add TACACS server by selecting the **New** option when configuring authentication parameters for management users. For more information, see Configuring Authentication Parameters for Management Users on page 209. ▪ **CoA only** for AirGroup CoA—To configure a ClearPass Policy Manager server used for AirGroup CoA, select the **CoA only** check box and configure the attributes defined in the ClearPass Policy Manager Server Configuration Parameters for AirGroup CoA table below. The RADIUS server is automatically selected. **NOTE:** The ClearPass Policy Manager server acts as a RADIUS server and asynchronously provides the AirGroup parameters for the client device including shared user, role, and location. 4. Click **OK**.

Table 87: *RADIUS Server Configuration Parameters*

Parameter	Description
Name	Enter a name for the server.
IP address	Enter the host name or the IP address of the external RADIUS server. **NOTE:** The hose name value will be accepted only if the **RadSec** parameter is enabled.

Table 87: *RADIUS Server Configuration Parameters*

Parameter	Description
RadSec	Set **RadSec** to **Enabled** to enable secure communication between the RADIUS server and Instant AP by creating a TLS tunnel between the Instant AP and the server. If **RadSec** is enabled, the following configuration options are displayed: ▪ **RadSec port**—Communication port number for RadSec TLS connection. By default, the port number is set to 2083. ▪ RFC 3576 ▪ RFC 5997 ▪ NAS IP address ▪ NAS identifier ▪ Service type framed user For more information on RadSec configuration, see Enabling RADIUS Communication over TLS (RadSec) on page 237.
Auth port	Enter the authorization port number of the external RADIUS server within the range of 1–65,535. The default port number is 1812.
Accounting port	Enter the accounting port number within the range of 1–65,535. This port is used for sending accounting records to the RADIUS server. The default port number is 1813.
Shared key	Enter a shared key for communicating with the external RADIUS server.
Retype key	Re-enter the shared key.
Timeout	Specify a timeout value in seconds. The value determines the timeout for one RADIUS request. The Instant AP retries to send the request several times (as configured in the **Retry count**) before the user gets disconnected. For example, if the **Timeout** is 5 seconds, **Retry counter** is 3, user is disconnected after 20 seconds. The default value is 5 seconds.
Retry count	Specify a number between 1 and 5. Indicates the maximum number of authentication requests that are sent to the server group, and the default value is 3 requests.
RFC 3576	Select **Enabled** to allow the Instant APs to process RFC 3576-compliant CoA and disconnect messages from the RADIUS server. Disconnect messages cause a user session to be terminated immediately, whereas the CoA messages modify session authorization attributes such as data filters.
RFC 5997	This helps to detect the server status of the RADIUS server. Every time there is an authentication or accounting request timeout, the Instant AP will send a status request enquiry to get the actual status of the RADIUS server before confirming the status of the server to be DOWN. ▪ **Authentication**—Select this check-box to ensure the Instant AP sends a status-server request to determine the actual state of the authentication server before marking the server as unavailable. ▪ **Accounting**—Select this check-box to ensure the Instant AP sends a status-server request to determine the actual state of the accounting server before marking the server as unavailable. **NOTE:** You can choose to select either the Authentication or Accounting check-boxes or select both check-boxes to support RFC5997.
NAS IP address	Allows you to configure an arbitrary IP address to be used as RADIUS attribute 4, NAS IP Address, without changing source IP Address in the IP header of the RADIUS packet.

Table 87: *RADIUS Server Configuration Parameters*

Parameter	Description
	NOTE: If you do not enter the IP address, the virtual controller IP address is used by default when **Dynamic RADIUS Proxy** is enabled.
NAS Identifier	Allows you to configure strings for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.
Dead Time	Specify a dead time for authentication server in minutes. When two or more authentication servers are configured on the Instant AP and a server is unavailable, the dead time configuration determines the duration for which the authentication server would be available if the server is marked as unavailable.
Dynamic RADIUS proxy parameters	Specify the following dynamic RADIUS proxy parameters: ■ **DRP IP**—IP address to be used as source IP for RADIUS packets. ■ **DRP Mask**—Subnet mask of the DRP IP address. ■ **DRP VLAN**—VLAN in which the RADIUS packets are sent. ■ **DRP Gateway**—Gateway IP address of the DRP VLAN. For more information on dynamic RADIUS proxy parameters and configuration procedure, see Configuring Dynamic RADIUS Proxy Parameters on page 239.
Service type framed user	Sets the service type value to frame for the following authentication methods: ■ **802.1X**—Changes the service type to frame for 802.1X authentication. ■ **Captive Portal**—Changes the service type to frame for Captive Portal authentication. ■ **MAC**—Changes the service type to frame for MAC authentication.

Table 88: *LDAP Server Configuration Parameters*

Parameter	Description
Name	Enter a name for the server.
IP address	Enter the IP address of the LDAP server.
Auth port	Enter the authorization port number of the LDAP server. The default port number is 389. **NOTE:** Secure LDAP over SSL is currently not supported on Instant APs. Changing the authentication port to 636 will not enable secure LDAP over SSL.
Admin-DN	Enter a DN for the admin user with read/search privileges across all the entries in the LDAP database (the user need not have write privileges, but the user must be able to search the database, and read attributes of other users in the database).
Admin password	Enter a password for administrator.
Base-DN	Enter a DN for the node that contains the entire user database.

Table 88: *LDAP Server Configuration Parameters*

Parameter	Description
Filter	Specify the filter to apply when searching for a user in the LDAP database. The default filter string is **(objectclass=*)**.
Key Attribute	Specify the attribute to use as a key while searching for the LDAP server. For Active Directory, the value is **sAMAccountName**
Timeout	Enter a value between 1 and 30 seconds. The default value is 5.
Retry count	Enter a value between 1 and 5. The default value is 3.
Dead Time	Specify a dead time for the authentication server in minutes within the range of 1–1440 minutes. The default dead time interval is 5 minutes. When two or more authentication servers are configured on the Instant AP and a server is unavailable, the dead time configuration determines the duration for which the authentication server would be available if the server is marked as unavailable.

Table 89: *TACACS Configuration Parameters*

Parameter	Description
Name	Enter a name for the server.
IP address	Enter the IP address of the TACACS server.
Auth Port	Enter a TCPIP port used by the server. The default port number is 49.
Shared Key	Enter a secret key of your choice to authenticate communication between the TACACS+ client and the server.
Retype Key	Re-enter the shared key.
Timeout	Enter a number between 1 and 30 seconds to indicate the timeout period for TACACS+ requests. The default value is 20 seconds.
Retry Count	Enter a number between 1 and 5 to indicate the maximum number of authentication attempts. The default value is 3.
Dead time	Specify a dead time in minutes within the range of 1–1440 minutes. The default dead time interval is 5 minutes.
Session authorization	Enables or disables session authorization. When enabled, the optional authorization session is turned on for the admin users. By default, session authorization is disabled.

Table 90: *ClearPass Policy Manager Server Configuration Parameters for AirGroup CoA*

Parameter	Description
Name	Enter a name of the server.
IP address	Enter the host name or IP address of the server.

Parameter	Description
Air Group CoA port	Enter a port number for sending AirGroup CoA on a port different from the standard CoA port. The default value is 5999.
Shared key	Enter a shared key for communicating with the external RADIUS server.
Retype key	Re-enter the shared key.

The following CLI commands configure a RADIUS server with DRP parameters:

```
(Instant AP)(config)# wlan auth-server <profile-name>
(Instant AP)(Auth Server <profile-name>)# ip <host>
(Instant AP)(Auth Server <profile-name>)# key <key>
(Instant AP)(Auth Server <profile-name>)# port <port>
(Instant AP)(Auth Server <profile-name>)# acctport <port>
(Instant AP)(Auth Server <profile-name>)# nas-id <NAS-ID>
(Instant AP)(Auth Server <profile-name>)# nas-ip <NAS-IP-address>
(Instant AP)(Auth Server <profile-name>)# timeout <seconds>
(Instant AP)(Auth Server <profile-name>)# retry-count <number>
(Instant AP)(Auth Server <profile-name>)# rfc3576
(Instant AP)(Auth Server <profile-name>)# rfc5997 {auth-only|acct-only}
(Instant AP)(Auth Server <profile-name>)# deadtime <minutes>
(Instant AP)(Auth Server <profile-name>)# drp-ip <IP-address>  <mask> vlan  <vlan>
gateway <gateway-IP-address)
```

The following CLI commands enable RadSec:

```
(Instant AP)(config)# wlan auth-server <profile-name>
(Instant AP)(Auth Server "name")# ip <host>
(Instant AP)(Auth Server "name")# radsec [port <port>]
(Instant AP)(Auth Server "name")# rfc3576
(Instant AP)(Auth Server "name")# rfc5997 {auth-only|acct-only}
(Instant AP)(Auth Server "name")# nas-id <id>
(Instant AP)(Auth Server "name")# nas-ip <ip>
```

The following CLI commands configure an LDAP server:

```
(Instant AP)(config)# wlan ldap-server <profile-name>
(Instant AP)(LDAP Server <profile-name>)# ip <IP-address>
(Instant AP)(LDAP Server <profile-name>)# port <port>
(Instant AP)(LDAP Server <profile-name>)# admin-dn <name>
(Instant AP)(LDAP Server <profile-name>)# admin-password <password>
(Instant AP)(LDAP Server <profile-name>)# base-dn <name>
(Instant AP)(LDAP Server <profile-name>)# filter <filter>
(Instant AP)(LDAP Server <profile-name>)# key-attribute <key>
(Instant AP)(LDAP Server <profile-name>)# timeout <seconds>
(Instant AP)(LDAP Server <profile-name>)# retry-count <number>
(Instant AP)(LDAP Server <profile-name>)# deadtime <minutes>
```

The following CLI commands configure a TACACS+ server:

```
(Instant AP)(config)# wlan tacacs-server <profile-name>
(Instant AP)(TACACS Server <profile-name>)# ip <IP-address>
(Instant AP)(TACACS Server <profile-name>)# port <port>
(Instant AP)(TACACS Server <profile-name>)# key <key>
(Instant AP)(TACACS Server <profile-name>)# timeout <seconds>
(Instant AP)(TACACS Server <profile-name>)# retry-count <number>
(Instant AP)(TACACS Server <profile-name>)# deadtime <minutes>
```

The following CLI commands configure a ClearPass Policy Manager server used for AirGroup CoA:

```
(Instant AP)(config)# wlan auth-server <profile-name>
(Instant AP)(Auth Server <profile-name>)# ip <host>
```

```
(Instant AP)(Auth Server <profile-name>)# key <key>
(Instant AP)(Auth Server <profile-name>)# cppm-rfc3576-port <port>
(Instant AP)(Auth Server <profile-name>)# cppm-rfc3576-only
```

Customizing the RADIUS Attributes

Starting from Aruba Instant 8.3.0.0, the users can now configure RADIUS modifier profile to customize the attributes that are included, excluded and modified in the RADIUS request before it is sent to the authentication server. The RADIUS modifier profile can be configured and applied to either Access-Request or Accounting-Request or both on a RADIUS authentication server.

This profile can contain up to 64 RADIUS attributes with static values that are used either to add or update in the request and another 64 RADIUS attributes to be excluded from the Requests.

Two new parameters have been added in the RADIUS authentication-server profile :

- l auth-modifier: When assigned, it references to a RADIUS modifier profile which is applied to all Access-Requests sending to this RADIUS authentication-server.
- l acct-modifier: When assigned, it references to a RADIUS modifier profile which is applied to all Accounting-Requests sending to this RADIUS authentication-server.

Enabling RADIUS Communication over TLS (RadSec)

You can configure an Instant AP to use TLS tunnel and to enable secure communication between the RADIUS server and Instant AP. Enabling RADIUS communication over TLS increases the level of security for authentication that is carried out across the cloud network. When configured, this feature ensures that the RadSec protocol is used for safely transmitting the authentication and accounting data between the Instant AP and the RadSec server.

The following conditions apply to RadSec configuration:

- When the TLS tunnel is established, RADIUS packets will go through the tunnel.
- By default, the TCP port 2083 is assigned for RadSec. Separate ports are not used for authentication, accounting, and dynamic authorization changes.
- Instant supports dynamic CoA (RFC 3576) over RadSec and the RADIUS server uses an existing TLS connection opened by the Instant AP to send the request.
- By default, the Instant AP uses its device certificate to establish a TLS connection with RadSec server. You can also upload your custom certificates on to Instant AP.For more information on uploading certificates, see Authentication Certificates on page 254.

Configuring a RadSec Server

The following procedure describes how to configure a RadSec using the WebUI.

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **Security** page. 2. Expand **Authentication Servers**. 3. To create a new server, click **+**. The **New Authentication Server** window for specifying details for the new server is displayed. 4. Select the **RADIUS** server type and configure the following parameters: a. Enter the name of the server. b. Enter the host name or the IP address of the	1. Navigate to **Security** > **Authentication Servers**. 2. To create a new server, click **New**. The **New Authentication Server** window for specifying details for the new server is displayed. 3. Select the **RADIUS** server type and configure the following parameters: a. Enter the name of the server. b. Enter the host name or the IP address of the server.

New WebUI	Old WebUI
server. c. Toggle the **RadSec** switch to enable RadSec. d. Ensure that the port defined for RadSec is correct in the **RadSec port** text box. By default, the port number is set to 2083. e. To allow the Instant APs to process RFC 3576-compliant CoA and disconnect messages from the RADIUS server, select the **Dynamic Authorization** toggle switch. Disconnect messages cause a user session to be terminated immediately, whereas the CoA messages modify session authorization attributes such as data filters. f. If **Dynamic Authorization** is enabled, specify an AirGroup CoA port, if required. g. Enter the NAS IP address. h. Specify the NAS identifier to configure strings for RADIUS attribute 32 and to send it with RADIUS requests to the RADIUS server. 5. Click **OK**.	c. Select **Enabled** to enable RadSec. d. Ensure that the port defined for RadSec is correct. By default, the port number is set to 2083. e. To allow the Instant APs to process RFC 3576-compliant CoA and disconnect messages from the RADIUS server, set **RFC 3576** to **Enabled**. Disconnect messages cause a user session to be terminated immediately, whereas the CoA messages modify session authorization attributes such as data filters. f. If **RFC 3576** is enabled, specify an AirGroup CoA port if required. g. Enter the NAS IP address. h. Specify the NAS identifier to configure strings for RADIUS attribute 32 and to send it with RADIUS requests to the RADIUS server. 4. Click **OK**.

The following CLI command configures the RadSec server:

```
(Instant AP)(config)# wlan auth-server <profile-name>
(Instant AP)# ip <host>
(Instant AP)(Auth Server "name")# radsec [port <port>]
(Instant AP)(Auth Server "name")# rfc3576
(Instant AP)(Auth Server "name")# nas-id <id>
(Instant AP)(Auth Server "name")# nas-ip <ip>
```

Associating the RadSec Server Profile with a Network Profile

The following procedure associates the server profile with a network profile using the WebUI.

New WebUI	Old WebUI
NOTE: Access the WLAN wizard or the Wired Settings window (Go to the **Configuration** > **Networks** page, select a WLAN or a wired profile and click **edit**). You can also associate the authentication servers when creating a new WLAN or wired profile. 1. Select the **Security** tab. 2. If you are configuring the authentication server for a WLAN SSID profile, move the slider to **Enterprise** security level and select an authentication type from the **Key management** drop-down list. 3. For a wired profile, enable the **MAC authentication** or **802.1X authentication** toggle	1. Access the WLAN wizard or the Wired Settings window. a. To open the WLAN wizard, select an existing SSID on the **Networks** tab, and click **edit**. b. To open the wired settings window, click **More** > **Wired**. In the **Wired** window, select a profile and click **Edit**. **NOTE:** You can also associate the authentication servers when creating a new WLAN or wired profile. 2. Click the **Security** tab.

New WebUI	Old WebUI
switch. 4. From the **Auth server 1** drop-down list, select the server on which RadSec is enabled. You can also create a new server with Radsec enabled by clicking **+**. 5. Click **Next** and until **Finish**. 6. To assign the RADIUS authentication server to a network profile, select the newly added server when configuring security settings for a WLAN or wired network profile.	3. If you are configuring the authentication server for a WLAN SSID profile, move the slider to **Enterprise** security level and select an authentication type from the **Key management** drop-down list. 4. For a wired profile, set **MAC authentication** or **802.1X authentication** to **Enabled**. 5. From the **Auth server 1** drop-down list, select the server name on which RadSec is enabled. You can also create a new server with Radsec enabled by selecting **New**. 6. Click **Next** and then click **Finish**. 7. To assign the RADIUS authentication server to a network profile, select the newly added server when configuring security settings for a WLAN or wired network profile.

The following CLI command associates an authentication server to a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# auth-server <server-name>
```

The following CLI command associates an authentication server to a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# auth-server <name>
```

Configuring Dynamic RADIUS Proxy Parameters

The RADIUS server can be deployed at different locations and VLANs. In most cases, a centralized RADIUS or local server is used to authenticate users. However, some user networks can use a local RADIUS server for employee authentication and a centralized RADIUS-based captive portal server for guest authentication. To ensure that the RADIUS traffic is routed to the required RADIUS server, the dynamic RADIUS proxy feature must be enabled.



In a multi-AP cluster, DRP does not work with Radsec. Member APs will directly establish TLS connection with the Radsec server, and not through the Conductor AP.

If the Instant AP clients need to authenticate to the RADIUS servers through a different IP address and VLAN, ensure that the following steps are completed:

1. Enable dynamic RADIUS proxy.
2. Configure dynamic RADIUS proxy IP, VLAN, netmask, and gateway for each authentication server.
3. Associate the authentication servers to SSID or a wired profile to which the clients connect.

After completing the configuration steps mentioned above, you can authenticate the SSID users against the configured dynamic RADIUS proxy parameters.

Enabling Dynamic RADIUS Proxy

The following procedure describes how to enable RADIUS server support using the WebUI.

Table 91: *Enabling Dynamic RADIUS Proxy*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **System** page. 2. Expand **General**. 3. Toggle the **Dynamic RADIUS Proxy** switch to enable. 4. Click **Save**.	1. In the Instant main window, click the **System** link. The **System** window is displayed. 2. In the **General** tab of the **System** window, select the **RADIUS** check box for **Dynamic Proxy**. 3. Click **OK**.
NOTE: When dynamic RADIUS proxy is enabled, the virtual controller network uses the IP Address of the virtual controller for communication with external RADIUS servers. Ensure that the virtual controller IP Address is set as a NAS IP when configuring RADIUS server attributes with dynamic RADIUS proxy enabled. For more information on configuring RADIUS server attributes, see External RADIUS Server on page 231. In case of VPN deployments, the tunnel IP received when establishing a VPN connection is used as the NAS IP. In such cases, the virtual controller IP need not be configured for the external RADIUS servers.	

The following CLI command enables the dynamic RADIUS proxy feature:

```
(Instant AP)(config)# dynamic-radius-proxy
```

Configuring Dynamic RADIUS Proxy Parameters

The following procedure describes how to configure DRP parameters for the authentication server by using the WebUI.

Table 92: *Configuring Dynamic RADIUS Proxy Parameters*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **Security** page. 2. Expand **Authentication Servers**. 3. To create a new server, click **+** and configure the required RADIUS server parameters as described in Table 87. 4. Ensure that the following dynamic RADIUS proxy parameters are configured: a. **DRP IP**—IP address to be used as source IP for RADIUS packets. b. **DRP Mask**—Subnet mask of the DRP IP address. c. **DRP Vlan**—VLAN in which the RADIUS packets are sent. d. **DRP Gateway**—Gateway IP address of the DRP VLAN. 5. Click **OK**.	1. Go to **Security** > **Authentication Servers**. 2. To create a new server, click **New** and configure the required RADIUS server parameters as described in Table 87. 3. Ensure that the following dynamic RADIUS proxy parameters are configured: a. **DRP IP**—IP address to be used as source IP for RADIUS packets. b. **DRP Mask**—Subnet mask of the DRP IP address. c. **DRP VLAN**—VLAN in which the RADIUS packets are sent. d. **DRP Gateway**—Gateway IP address of the DRP VLAN. 4. Click **OK**.

The following CLI commands configures a dynamic RADIUS proxy parameters:

```
(Instant AP)(config)# wlan auth-server <profile-name>
(Instant AP)(Auth Server <profile-name>)# ip <IP-address>
(Instant AP)(Auth Server <profile-name>)# key <key>
```

```
(Instant AP)(Auth Server <profile-name>)# port <port>
(Instant AP)(Auth Server <profile-name>)# acctport <port>
(Instant AP)(Auth Server <profile-name>)# nas-id <NAS-ID>
(Instant AP)(Auth Server <profile-name>)# nas-ip <NAS-IP-address>
(Instant AP)(Auth Server <profile-name>)# timeout <seconds>
(Instant AP)(Auth Server <profile-name>)# retry-count <number>
(Instant AP)(Auth Server <profile-name>)# deadtime <minutes>
(Instant AP)(Auth Server <profile-name>)# drp-ip  <IP-address>  <mask> vlan  <vlan>
gateway <gateway-IP-address>
```

Associate DRP Server Profile to a Network Profile

The following procedure describes how to associate the DRP server profiles with a network profile by using the WebUI:

Table 93: *Associating DRP Server profile to a Network Profile*

New WebUI	Old WebUI
1. Access the WLAN wizard or the Wired Settings window (Go to the **Configuration** > **Networks**, select a WLAN or a wired profile and click **Edit**). **NOTE:** You can also associate the authentication servers when creating a new WLAN or wired profile. 2. Select the **Security** tab. 3. If you are configuring the authentication server for a WLAN SSID profile, move the slider to **Enterprise** security level and select an authentication type from the **Key management** drop-down list. 4. For a wired profile, enable the **MAC authentication** or **802.1X authentication** toggle switch. 5. From the **Auth server 1** drop-down list, select the server name on which dynamic RADIUS proxy parameters are enabled. You can also create a new server with dynamic RADIUS proxy parameters enabled by selecting **+**. 6. Click **Next** and until **Finish**. 7. To assign the RADIUS authentication server to a network profile, select the newly added server when configuring security settings for a WLAN or wired network profile.	1. Access the WLAN wizard or the Wired Settings window. a. To open the WLAN wizard, select an existing SSID on the **Networks** tab, and click **edit**. b. To open the wired settings window, click **More** > **Wired**. In the **Wired** window, select a profile and click **Edit**. **NOTE:** You can also associate the authentication servers when creating a new WLAN or wired profile. 2. Click the **Security** tab. 3. If you are configuring the authentication server for a WLAN SSID profile, move the slider to **Enterprise** security level and select an authentication type from the **Key management** drop-down list. 4. For a wired profile, set **MAC authentication** or **802.1X authentication** to **Enabled**. 5. From the **Auth server 1** drop-down list, select the server name on which dynamic RADIUS proxy parameters are enabled. You can also create a new server with dynamic RADIUS proxy parameters enabled by selecting **New**. 6. Click **Next** and then click **Finish**. 7. To assign the RADIUS authentication server to a network profile, select the newly added server when configuring security settings for a WLAN or wired network profile.
NOTE: You can also add an external RADIUS server by selecting New for Authentication Server when configuring a WLAN or wired profile. For more information, see Points to Remember on page 145 and In the Old WebUI on page 165.	

The following CLI commands associates an authentication server to a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# auth-server <server-name>
```

The following CLI commands associates an authentication server to a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# auth-server <name>
```

Supported Encryption Types

Encryption is the process of converting data into a cryptic format or code when it is transmitted on a network. Encryption prevents unauthorized use of the data.

Instant supports the following types of encryption:

- **WEP**—WEP is an authentication method where all users share the same key. WEP is not as secure as other encryption types such as TKIP.
- **TKIP**—TKIP uses the same encryption algorithm as WEP. However, TKIP is more secure and has an additional message integrity check.
- **AES**—The AES encryption algorithm is a widely supported encryption type for all wireless networks that contain any confidential data. AES in Wi-Fi leverages 802.1X or PSKs to generate per-station keys for all devices. AES provides a high level of security like IPsec clients.



WEP and TKIP are limited to WLAN connection speed of 54 Mbps. The 802.11n connection supports only AES encryption. Aruba recommends AES encryption. Ensure that all devices that do not support AES are upgraded or replaced with the devices that support AES encryption.

WPA and WPA2

WPA is created based on the draft of 802.11i, which allowed users to create more secure WLANs. WPA2 encompasses the full implementation of the 802.11i standard. WPA2 is a superset that encompasses the full WPA feature set.

The following table summarizes the differences between the two certifications:

Table 94: *WPA and WPA2 Features*

Certification	Authentication	Encryption
WPA	■ PSK ■ IEEE 802.1X with EAP	TKIP with message integrity check
WPA2	■ PSK ■ IEEE 802.1X with EAP	AES—Counter Mode with Cipher Block Chaining Message Authentication Code

WPA and WPA2 can be further classified as follows:

- **Personal**—Personal is also called PSK. In this type, a unique key is shared with each client in the network. Users have to use this key to securely log in to the network. The key remains the same until it is changed by authorized personnel. You can also configure key change intervals .

- **Enterprise**—Enterprise is more secure than WPA Personal. In this type, every client automatically receives a unique encryption key after securely logging in to the network. This key is automatically updated at regular intervals. WPA uses TKIP and WPA2 uses the AES algorithm.

Recommended Authentication and Encryption Combinations

The following table summarizes the recommendations for authentication and encryption combinations for the Wi-Fi networks.

Table 95: *Recommended Authentication and Encryption Combinations*

Network Type	Authentication	Encryption
Employee	802.1X	AES
Guest Network	Captive portal	None
Voice Network or Handheld devices	802.1X or PSK as supported by the device	AES if possible, TKIP or WEP if necessary (combine with security settings assigned for a user role).

Supported Encryption types for Instant AP Authentication

Instant supports the following encryption types to authenticate wired Instant APs for 802.1X supplicants, Mesh and Wi-Fi uplink stations.

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

Authentication Survivability

The authentication survivability feature supports a survivable authentication framework against any remote link failures when working with external authentication servers. When enabled, this feature allows the Instant APs to authenticate the previously connected clients against the cached credentials if the connection to the authentication server is temporarily lost. This feature is now available for WLAN SSIDs with open, personal (MPSK-AES) and enterprise security levels.

Instant supports the following authentication standards for authentication survivability:

- **EAP-MSCHAPv2**: The PEAP, also known as Protected EAP, is a protocol that encapsulates EAP within a potentially encrypted and authenticated TLS tunnel.
- **EAP-TLS**: EAP-TLS is an IETF open standard that uses the TLS protocol.
- **MAC Authentication**: MAC-based authentication is a standard that authenticates devices based on their physical media access control (MAC) address.

When the authentication survivability feature is enabled, the following authentication process is used:

1. Upon successful authentication, the associated Instant AP caches the authentication credentials of the connected clients for the configured duration. The cache expiry duration for authentication survivability can be set within the range of 1–99 hours, with 24 hours being the default cache

timeout duration.

2. If the client roams or tries to reconnect to the Instant AP and the remote link fails due to the unavailability of the authentication server, the Instant AP uses the cached credentials in the internal authentication server to authenticate the user. However, if the client tries to reconnect after the cache expiry, the authentication fails.
3. When the authentication server is available and if the client tries to reconnect, the Instant AP detects the availability of server and allows the client to authenticate to the server. Upon successful authentication, the Instant AP cache details are refreshed.

Starting from Aruba Instant 8.4.0.0, access credentials, user roles, and other key attributes are cached when clients are authenticated by an external authentication server.

Below are the cached RADIUS attributes:

- ARUBA_NAMED_VLAN
- ARUBA_NO_DHCP_FINGERPRINT
- ARUBA_ROLE
- ARUBA_VLAN
- MS_TUNNEL_MEDIUM_TYPE
- MS_TUNNEL_PRIVATE_GROUP_ID
- MS_TUNNEL_TYPE
- PW_SESSION_TIMEOUT
- PW_USER_NAME

Important Points to Remember

- Any client connected through ClearPass Policy Manager and authenticated through Instant AP remains authenticated with the Instant AP even if the client is removed from the ClearPass Policy Manager server during the ClearPass Policy Manager downtime.
- Do not make any changes to the authentication survivability cache timeout duration when the authentication server is down.
- For EAP-PEAP authentication, ensure that the ClearPass Policy Manager 6.0.2 or later version is used for authentication. For EAP-TLS authentication, any external or third-party server can be used.
- For EAP-TLS authentication, ensure that the server and CA certificates from the authentication servers are uploaded on the Instant AP. For more information, see Authentication Certificates on page 254.
- Authentication cache will be lost if the Instant AP on which the user credentials are cached, is rebooted.
- EAP-PEAP authentication survivability is supported on Aruba CPPM Server version 6.0.2 or later versions.

Limitations

Authentication survivability is not supported under the following conditions:

1. When EAP Termination is enabled.
2. When the RadSec server is used as an authentication server.
3. When the internal server is used as a secondary authentication server.

Enabling Authentication Survivability

The following procedure describes how to enable authentication survivability for a wireless network profile through the WebUI:

Table 96: *Enabling Authentication Survivability*

New WebUI	Old WebUI
1. In the **Configuration** > **Networks** page, a. Click **+** to create a new WLAN SSID profile, or b. Select an existing profile for which you want to enable authentication survivability and click **edit**. 2. Ensure that the required WLAN and VLAN attributes are defined under **Basic** and **VLAN** tabs. 3. Under **Security** tab, select **Open, Personal (MPSK-AES)** or **Enterprise** in **Security Level** list box. 4. Select an existing authentication server or create a new server by clicking **+**. 5. To enable authentication survivability, toggle the **Authentication survivability** switch. On enabling this, the Instant AP authenticates the previously connected clients using EAP-PEAP, EAP-TLS, and MAC authentication when connection to the external authentication server is temporarily lost. 6. In the **Cache timeout (global)** text box, specify the cache timeout duration, after which the cached details of the previously authenticated clients expire. You can specify a value within the range of 1–99 hours and the default cache timeout duration is 24 hours. 7. Click **Next** and until **Finish** to apply the changes.	1. On the **Networks** tab, click **New** to create a new WLAN SSID profile or select an existing profile for which you want to enable authentication survivability and click **edit**. 2. In the **Edit <profile-name>** or the **New WLAN** window, ensure that the required WLAN and VLAN attributes are defined, and then click **Next**. 3. On the **Security** tab, under **Open, Personal (MPSK-AES)** or **Enterprise** security settings, select an existing authentication server or create a new server by clicking **New**. 4. To enable authentication survivability, select **Enabled** from the **Authentication survivability** drop-down list. On enabling this, the Instant AP authenticates the previously connected clients using EAP-PEAP, EAP-TLS and MAC authentication when connection to the external authentication server is temporarily lost. 5. In the **Cache timeout (global)** text box, specify the cache timeout duration, after which the cached details of the previously authenticated clients expire. You can specify a value within the range of 1–99 hours and the default cache timeout duration is 24 hours. 6. Click **Next** and then click **Finish** to apply the changes.

The following CLI commands configures authentication survivability for a wireless network:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# type {<Employee>|<Voice>|<Guest>}
(Instant AP)(SSID Profile <name>)# auth-server <server-name1>
(Instant AP)(SSID Profile <name>)# auth-survivability
(Instant AP)(SSID Profile <name>)# exit
(Instant AP)(config)# auth-survivability cache-time-out <hours>
```

The following CLI command shows the cache expiry duration:

```
(Instant AP)# show auth-survivability time-out
```

The following CLI command shows information on **auth-survivability** cached by the Instant AP:

```
(Instant AP)# show auth-survivability cached-info
```

The following CLI command shows logs for debugging:

```
(Instant AP)# show auth-survivability debug-log
```

Priority for Local Cache Authentication

Priority for Local Cache Authentication for wireless networks is based on the Authentication Survivability framework of Aruba Instant. When Priority for Local Cache Authentication is enabled, the Instant AP first attempts to authenticate clients with the local cache data maintained for authentication survivability and uses the RADIUS server to authenticate only those clients whose data is not available in the local cache. This feature can be used only if Authentication Survivability is enabled.

Configuring Priority for Local Cache Authentication

Priority for Local Cache Authentication is only available for clients authenticated through MAC and 802.1x authentication.

The following procedure describes how to prioritize local cache for authentication using the New WebUI:

1. Select the network for which you want to enable local authentication in the **Configuration> Networks** page and click **edit**.
2. Navigate to the **Security** Tab.
3. Enable **Authentication Survivability**.
4. Toggle the **Priority for Local Cache Authentication** button to enable or disable the feature.
5. Click **Next** to configure Access settings for the WLAN network and click **Finish**.

The following CLI commands enables Priority for Local Cache Authentication for an WLAN SSID profile using the CLI:

```
(Instant AP)(config)# wlan ssid-profile <profile name>
(Instant AP)(SSID Profile "<profile name>")# auth-survivability
(Instant AP)(SSID Profile "<profile name>")# priority-use-local-cache-auth
```

The following CLI commands disables Priority for Local Cache Authentication for an WLAN SSID profile:

```
(Instant AP)(config)# wlan ssid-profile <profile name>
(Instant AP)(SSID Profile "<profile name>")# no priority-use-local-cache-auth
```

WPA3 Security

Aruba Instant supports WPA3 security improvements that include:

- **Simultaneous Authentication of Equals (SAE)**—Replaces WPA2-PSK with password-based authentication that is resistant to dictionary attacks.
- **WPA3-Enterprise 192-Bit Mode**—Brings Suite-B 192-bit security suite that is aligned with Commercial National Security Algorithm (CNSA) for enterprise network. SAE-based keys are not based on PSK and are therefore pairwise and unique between clients and the AP. Suite B restricts the deployment to one of two options:
  - 128-bit security
  - 192-bit security without the ability to mix-and-match ciphers, Diffie-Hellman groups, hash functions, and signature modes

SAE

SAE replaces the less-secure WPA2-PSK authentication. Instead of using the PSK as the PMK, SAE arrives at a PMK, by mapping the PSK to an element of a finite cyclic group, PassWord Element (PWE), doing FCG operations on it, and exchanging it with the peer.

Aruba Instant supports:

- SAE without PMK caching
- SAE with PMK caching
- SAE or WPA2-PSK mixed mode

SAE Without PMK Caching

Instant advertises support for SAE by using an AKM suite selector for SAE in all beacons and probe response frames. Besides, PMF is set to required (MFPR=1).

A client that wishes to perform SAE sends an 802.11 authentication request with authentication algorithm set to value 3 (SAE). This frame contains a well-formed commit message, that is, authentication transaction sequence set to 1, an FCG, commit-scalar, and commit-element.

Instant supports group 19, a 256-bit Elliptic Curve group. Instant responds with an 802.11 authentication containing its own commit message.

Instant and the client compute the PMK and send the confirm message to each other using an authentication frame with authentication transaction sequence set to 2.

The client sends an association request with the AKM suite set to SAE and Instant sends an association response.

Instant initiates a 4-way key handshake with the client to derive the PTK.

SAE With PMK Caching

If SAE has been established earlier, a client that wishes to perform SAE with PMK caching sends an authentication frame with authentication algorithm set to open. Instant sends an authentication response and the client sends a reassociation request with AKM set to SAE and includes the previously derived PMKID.

Instant checks if the PMKID is valid and sends an association response with the status code success.

Instant initiates a 4-way key handshake with the client to derive the PTK.

SAE or WPA2-PSK Mixed Mode

SAE or WPA2-PSK mixed mode allows both SAE clients and clients that can only perform WPA2-PSK to connect to the same BSSID. In this mode, the beacon or probe responses contain a AKM list which contains both PSK (00-0F-AC:2) and SAE (00-0F-AC:8). Clients that support SAE send an authentication frame with SAE payload and connect to the BSSID.

Clients that support only WPA2-PSK send an authentication frame with authentication algorithm set to open.

Instant initiates a 4-way key handshake similar to WPA2.

WPA3-Enterprise

WPA3-Enterprise enforces top secret security standards for an enterprise Wi-Fi in comparison to secret security standards. Top secret security standards includes:

- Deriving at least 384-bit PMK/MSK using Suite B compatible EAP-TLS.
- Securing pairwise data between STA and authenticator using AES-GCM-256.
- Securing group addressed data between STA and authenticator using AES-GCM-256.
- Securing group addressed management frames using BIP-GMAC-256



WPA3-Enterprise compatible 802.1X authentication occurs between STA and CPPM.

WPA3-Enterprise 192-bit Mode requires a compatible EAP server (such as Aruba ClearPass Policy Manager 6.8+) and requires EAP-TLS.

WPA3-Enterprise advertises or negotiates the following capabilities in beacons, probes response, or 802.11 association:

- AKM Suite Selector as 00-0F-AC:12
- Pairwise Cipher Suite Selector as 00-0F-AC:9
- Group data cipher suite selector as 00-0F-AC:9
- Group management cipher suite (MFP) selector as 00-0F-AC:12

If WPA3-Enterprise is enabled, STA is successfully associated only if it uses one of the four suite selectors for AKM selection, pairwise data protection, group data protection, and group management protection. If a STA mismatches any one of the four suite selectors, the STA association fails.

WPA3 Opmodes

Aruba Instant supports the WPA3-AES-CCM-128, WPA3-CNSA, WPA3-AES-CCM-256, and WPA3-SAE-AES opmodes.

The WPA3 opmodes are effective only on the 300 Series, 303 Series, 310 Series, 320 Series, 330 Series, 340 Series, AP-365, AP-367, 370 Series, 510 Series, 530 Series, and 550 Series access points. Other access points will reject these opmodes.

Before using the WPA3-SAE-AES opmode, disable opmode-transition and configure a WPA hexkey or WPA passphrase as a pre-shared key. Use the WPA3 with SAE and PSK mode for SAE mixed mode operation during transition. The opmode-transition is not applicable to WPA3-AES-CCM-128 and WPA3-CNSA opmodes.

WPA2-PSK-AES virtual APs will be not be automatically upgraded to WPA3-SAE-AES virtual APs. Hence, WPA2-PSK-AES virtual APs will not automatically work in mixed mode. Configure a WPA3-SAE-AES virtual AP with opmode-transition for the virtual AP to operate in mixed mode.

Configuring WPA3

To support WPA3, configure the **opmode** and **opmode-transition** parameters under the **wlan ssid-profile** command.

The **opmode-transition** parameter is enabled by default and provides backward compatibility for authentication and WPA3-SAE-AES opmode. Use the **opmode-transition** parameter as a fallback option if a client faces connectivity issues on the enhanced open authentication or WPA3-SAE-AES transition mode virtual APs.

The following CLI commands disable opmode transition:

```
(Instant AP)(config)# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile "<profile_name>")# opmode-transition-disable
```

The following CLI commands enable opmode transition:

```
(Instant AP)(config)# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile "<profile_name>")# opmode-transition
```

The following procedure describes how to configure WPA3 for Enterprise with 192-bit mode using the New WebUI:

1. Navigate to the WLAN wizard (To add a new profile, go to **Configuration > Networks** and click **+**. To modify an existing profile, go to **Configuration > Networks** , select a WLAN SSID from the list of networks to edit.
2. Click the **Security** tab.
3. Select **Enterprise** from the **Security Level** drop-down list. The authentication options applicable to the Enterprise network are displayed.
4. Select one of the following from the **Key Management** drop-down list:
   a. **WPA3-Enterprise (CNSA)**—WPA3 with AES GCM-256 encryption using CNSA (192 bit).
   b. **WPA3-Enterprise (CCM 128)**—WPA3 with AES CCM encryption and dynamic keys using 802.1X.
   c. **WPA3-Enterprise (CCM 256)**—WPA3 with AES GCM-256 encryption.
5. Click **Next** and the click **Finish**.

The following CLI commands configure WPA3 opmode for Enterprise security:

```
(Instant AP)(config)# wlan ssid-profile wpa3_mode
(Instant AP)(SSID Profile "wpa3_mode")# opmode wpa3-aes-ccm-128
(Instant AP)(SSID Profile "wpa3_mode")# opmode wpa3-cnsa
```

The following procedure describes how to configure WPA3 opmode for Personal security using the New WebUI:

1. Navigate to the WLAN wizard (To add a new profile, go to **Configuration > Networks** and click **+**. To modify an existing profile, go to **Configuration > Networks**, select a WLAN SSID from the list of networks to edit.
2. Click the **Security** tab.
3. Select **Personal** from the **Security Level** drop-down list. The authentication options applicable to the Personal network are displayed.
4. Select **WPA3 Personal** from the **Key Management** drop-down list.
5. Click **Next** and the click **Finish**.

The following CLI commands configure WPA3 opmode for Personal security:

```
(Instant AP)(config)# wlan ssid-profile wpa3_mode
(Instant AP)(SSID Profile "wpa3_mode")# opmode wpa3-sae-aes
```



Using the WPA3-SAE-AES opmode requires a pre-shared key. Configure either a WPA hexkey or WPA passphrase as a pre-shared key.

The following CLI commands disable WPA3 opmode:

```
(Instant AP)(config)# wlan ssid-profile wpa3_mode
(Instant AP)(SSID Profile "wpa3_mode")# no opmode
```

Fast BSS Transition Support for WPA3

Aruba Instant supports Fast BSS Transition (802.1r) for the following WPA3 modes in both tunnel-forwarding and decrypt-tunnel modes for all APs which support WPA3:

- WPA3-Personal – SAE
- WPA3-Personal – SAE/WPA2-PSK Mixed mode
- WPA3-Enterprise Basic option

- WPA3-Enterprise 192-bit Security option
- WPA3-Enterprise non-CNSA mode with GCMP-256 Cipher Suite

802.1X Supplicant Support

The 802.1X authentication protocol prevents the unauthorized clients from gaining access to the network through publicly accessible ports. If the ports to which the Instant APs are connected, are configured to use the 802.1X authentication method, ensure that you configure the Instant APs to function as an 802.1X client or supplicant. If your network requires all wired devices to authenticate using PEAP or TLS protocol, you need to configure the Instant AP uplink ports for 802.1X authentication, so that the switch grants access to the Instant AP only after completing the authentication as a valid client.

To enable the 802.1X supplicant support on an Instant AP, ensure that the 802.1X authentication parameters are configured on all Instant APs in the cluster and are stored securely in the Instant AP flash.



The 802.1X supplicant support feature is not supported with mesh and Wi-Fi uplink.

Configuring an Instant AP for 802.1X Supplicant Support

The following procedure describes how to enable 802.1X supplicant support, configure 802.1X authentication parameters on every Instant AP using the WebUI:

Table 97: *Configuring 802.1X Supplicant Support*

New WebUI	Old WebUI
To use PEAP protocol-based 802.1X authentication method, complete the following steps: 1. In the **Configuration** > **Access Points** page, select the Instant AP on which you want to set the variables for 802.1X authentication, and click **Edit**. 2. In the **Edit Access Point <access point>** page, expand the **Uplink**. 3. Under **PEAP User**, enter a username, password, and retype the password for confirmation. The Instant AP username and password are stored in Instant AP flash. When the Instant AP boots, the */tmp/ap1xuser* and */tmp/ap1xpassword* files are created based on these two variables. **NOTE:** The default inner authentication protocol for PEAP is MS-CHAPV2.	To use PEAP protocol-based 802.1X authentication method, complete the following steps: 1. In the **Access Points** tab, click the Instant AP on which you want to set the variables for 802.1X authentication, and then click the **edit** link. 2. In the **Edit Access Point** window, click the **Uplink** tab. 3. Under **PEAP user**, enter the username, password, and retype the password for confirmation. The Instant AP username and password are stored in Instant AP flash. When the Instant AP boots, the */tmp/ap1xuser* and */tmp/ap1xpassword* files are created based on these two variables. **NOTE:** The default inner authentication protocol for PEAP is MS-CHAPV2.
To upload server certificates for validating the authentication server credentials, complete the following steps: 1. Expand **Upload Certificate**. 2. Specify the URL from where you want to upload the certificates and select the type of certificate. 3. Click **Upload Certificate**.	To upload server certificates for validating the authentication server credentials, complete the following steps: 1. Click **Upload New Certificate**. 2. Specify the URL from where you want to upload the certificates and select the type of certificate. 3. Click **OK**.

New WebUI	Old WebUI
To configure 802.1X authentication on uplink ports of an Instant AP, complete the following steps: 1. Go to **Configuration** > **System** page. 2. Click **Show advanced options** at the bottom of the page and expand **Uplink**. 3. Under **AP1X**, select **PEAP** or **TLS** in the **AP1X type** drop-down list. 4. If you want to validate the server credentials using server certificate, toggle the **Validate server** switch to enable. Ensure that the server certificates for validating server credentials are uploaded to Instant AP database. 5. Click **Save**. 6. Reboot the Instant AP. **NOTE:** The user certificate must be in the PEM format and include both the user certificate and the private key. If the certificate pair is encrypted, you must obtain the associated private key.	To configure 802.1X authentication on uplink ports of an Instant AP, complete the following steps: 1. Go to **System** > **Show advanced options** > **Uplink**. 2. Click **AP1X**. 3. Select **PEAP** or **TLS** in the **AP1X type** drop-down list. 4. If you want to validate the server credentials using server certificate, select the **Validate server** check box. Ensure that the server certificates for validating server credentials are uploaded to Instant AP database. 5. Click **OK**. 6. Reboot the Instant AP. **NOTE:** The user certificate must be in the PEM format and include both the user certificate and the private key. If the certificate pair is encrypted, you must obtain the associated private key.

The following CLI command sets username and password variable used by the PEAP protocol-based 802.1X authentication:

```
(Instant AP)# ap1x-peap-user <ap1xuser> <password>
```

The following CLI command sets the PEAP 802.1X authentication type:

```
(Instant AP)(config)# ap1x peap [validate-server]
```

The following CLI command sets TLS 802.1X authentication type:

```
(Instant AP)(config)# ap1x  tls <user> [validate-server]
```

The following CLI command uploads user or CA certificates for PEAP or TLS authentication:

```
(Instant AP)# copy tftp <addr> <file> ap1x {ca|cert <password>}  format pem
```

The following CLI commands download user or server certificates from a TFTP, FTP, or web server:

```
(Instant AP)# download ap1x <url> format pem [psk <psk>]
(Instant AP)# download ap1xca <url> format pem
```

The following CLI command shows the certificate details:

```
(Instant AP)# show ap1xcert
```

The following CLI commands verify the configuration, use any of the following commands:

```
(Instant AP)# show ap1x config
(Instant AP)# show ap1x debug-logs
(Instant AP)# show ap1x status
```

Blacklisting Clients

The client blacklisting denies connection to the blacklisted clients. When a client is blacklisted, it is not allowed to associate with an Instant AP in the network. If a client is connected to the network when it is blacklisted, a deauthentication message is sent to force client disconnection.

This section describes the following procedures:

- Blacklisting Clients Manually on page 252
- Blacklisting Clients Dynamically on page 252

Blacklisting Clients Manually

Manual blacklisting adds the MAC address of a client to the blacklist. These clients are added into a permanent blacklist. These blacklisted clients are not allowed to connect to the network unless they are removed from the blacklist.

The following procedure describes how to add a client to the blacklist manually using the WebUI.

Table 98: *Blacklisting Clients Manually*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **Security** page. 2. Expand **Blacklisting**. 3. Under **Manual Blacklisting**, click **+**. 4. Enter the MAC address of the client to be blacklisted in the **MAC address to add** text box. **NOTE:** For the blacklisting to take effect on the MAC address, you must enable blacklisting in the SSID profile. For more information, see Blacklisting on page 141. 5. Click **OK**. The **Blacklisted Since** column in the **Manual Blacklist** window displays the time at which the current blacklisting has started for the client. 6. To delete a client from the manual blacklist, select the MAC Address of the client under the **Manual Blacklist** window and click **Delete**. 7. Click **Save**.	1. Click the **Security** link located directly above the Search bar in the Instant main window. 2. Click the **Blacklisting** tab. 3. Under **Manual Blacklisting**, click **New**. 4. Enter the MAC address of the client to be blacklisted in the **MAC address to add** text box. **NOTE:** For the blacklisting to take effect on the MAC address, you must enable blacklisting in the SSID profile. For more information, see Blacklisting on page 141. 5. Click **OK**. The **Blacklisted Since** column in the **Manual Blacklist** window displays the time at which the current blacklisting has started for the client. 6. To delete a client from the manual blacklist, select the MAC Address of the client under the **Manual Blacklist** window, and then click **Delete**.

The following CLI command blacklists a client:

```
(Instant AP)(config)# blacklist-client <MAC-Address>
```

The following CLI commands enable blacklisting in the SSID profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# blacklisting
```

The following CLI command shows the blacklisted clients:

```
(Instant AP)# show blacklist-client
Blacklisted Clients
-------------------
MAC                Reason        Timestamp  Remaining time(sec)  AP name
---                ------        ---------  -------------------  -------
00:1c:b3:09:85:15  user-defined  17:21:29   Permanent            -
```

Blacklisting Clients Dynamically

The clients can be blacklisted dynamically when they exceed the authentication failure threshold or when a blacklisting rule is triggered as part of the authentication process. Users can be blacklisted by the following methods:

- **Authentication Failure Blacklisting** - When a client takes time to authenticate and exceeds the configured failure threshold, it is automatically blacklisted by an Instant AP.
- **Session Firewall-Based Blacklisting** - In session firewall-based blacklisting, an ACL rule is used to enable the option for dynamic blacklisting. When the ACL rule is triggered, it sends out blacklist information and the client is blacklisted.

Configuring Blacklist Duration

The following procedure describes how to set the blacklist duration using the WebUI.

Table 99: *Configuring Blacklist Duration*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **Security** page. 2. Expand **Blacklisting**. 3. Expand **Dynamic Blacklisting.** 4. In the **Auth failure blacklist time** field enter the duration after which the clients must be blacklisted. 5. In the **PEF rule blacklisted time** field enter the duration after which the clients can be blacklisted due to an ACL rule trigger. 6. Click **Save**. **NOTE:** To enable session-firewall-based blacklisting, click **+** in the **Configuration** > **Networks** tab, navigate to the **Basic > VLAN > Security > Access** window, click **+** under **Access Rules for <network>** and click the **Blacklist** check box in the **New rule** window.	1. Click the **Security** link located directly above the Search bar in the Instant main window. 2. Click the **Blacklisting** tab. 3. Under **Dynamic Blacklisting**: 4. For **Auth failure blacklist time**, the duration in seconds after which the clients that exceed the authentication failure threshold must be blacklisted. 5. For **PEF rule blacklisted time**, enter the duration in seconds after which the clients can be blacklisted due to an ACL rule trigger. 6. Click **OK**. **NOTE:** To enable session-firewall-based blacklisting, click **New** in the **Networks** tab and navigate to **WLAN Settings > VLAN > Security > Access** window, and click the **Blacklist** check box of the corresponding ACL rule.
NOTE: You can configure a maximum number of authentication failures by the clients, after which a client must be blacklisted. For more information on configuring maximum authentication failure attempts, see Points to Remember on page 145.	

The following CLI commands dynamically blacklists clients:

```
(Instant AP)(config)# auth-failure-blacklist-time <seconds>
(Instant AP)(config)# blacklist-time <seconds>
```

The following CLI commands enable blacklisting in the SSID profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# blacklisting
```

The following CLI commands show the blacklisted clients:

```
(Instant AP)# show blacklist-client config
Blacklist Time               :60
Auth Failure Blacklist Time  :60
Manually Blacklisted Clients
----------------------------
```

```
MAC  Time
---  ----
Dynamically Blacklisted Clients
-------------------------------
MAC  Reason  Timestamp  Remaining time(sec)  AP IP
---  ------  ---------  -------------------  -----
Dyn Blacklist Count  :0
```

Authentication Certificates

A certificate is a digital file that certifies the identity of the organization or products of the organization. It is also used to establish your credentials for any web transactions. It contains the organization name, a serial number, expiration date, a copy of the certificate-holder's public key, and the digital signature of the certificate-issuing authority so that a recipient can ensure that the certificate is real.

There is a default server certificate installed in the controller to demonstrate the authentication of the controller for Captive Portal and WebUI management access. However, this certificate does not guarantee security in production networks. Aruba strongly recommends that you replace the default certificate with a custom certificate issued for your site or domain by a trusted CA.

Instant supports the following certificate types in either PEM or DER format:

- Public Certificate
- Server Certificate
- Trusted CA Certificate
- Client Certificate

Uploading Public Certificates

Public certificates must be bundled with the intermediate certificate, root certificate, and the private key issued by the certificate authority to be supported by the Instant AP. The system will reject the public certificate if it is not bundled with the supporting certificates and the private key. Use the following procedure to bundle public certificates for Instant APs:

1. Open the certificate file using a text editor.
2. Copy and paste the Intermediate certificate, root certificate, and the private key below the certificate in the following order:
   a. Certificate
   b. Intermediate certificate
   c. Root certificate
   d. Private key
3. Save the certificate file.



Ensure that there are no blank spaces or blank lines in the certificate file.

Installing Certificates on the Instant AP

Starting from Aruba Instant 8.7.0.0, certificates must be imported and assigned to an application to take effect. This allows you to install and use third party certificates for specific applications. This feature is currently available only in Instant networks that are managed locally and is not supported in Central, or AirWave deployments.

Certificates can be assigned to applications using the new WebUI or CLI. The old WebUI does not allow application assignment. Applications can be configured with one or more certificates, if required. In cluster configurations, certificate import and assignment can be carried out only on the master AP.



Central and AirWave deployments will continue to use the legacy method of installing certificates.

Since Central does not support this feature, ensure that the **wlan cert-assignment-profile** and the installed certificates are removed on the AP before connecting it to Central. The AP might fail to provision if the application assignment and certificates are not removed.

This section contains the following procedures:

- Managing Certificates in the WebUI on page 255
- Managing Certificates in the CLI on page 256
- Loading Certificates Through AirWave on page 256

Managing Certificates in the WebUI

The following procedures describe how to import, assign and remove certificates on the Instant AP using the WebUI.

Table 100: *Loading Certificates in the WebUI*

New WebUI	Old WebUI
To import certificates to the Instant AP: 1. Navigate to the **Maintenance** > **Certificates** page. 2. To upload a certificate, click **Upload New Certificate**. The **New Certificate** window is displayed. 3. Click **Browse** and select the appropriate certificate file you want to upload. 4. Enter a name for the certificate in the **Certificate name** text box. 5. Select the certificate type from the **Certificate type** drop-down list. You can select any of the following certificate types: a. **Public—**Public key certificate b. **Server—**Server certificate c. **Trusted CA**— CA certificate to validate the identity of the client. d. **Client—**Client certificate 6. Select the certificate format from the **Certificate format** drop-down list. 7. If you have selected **Public**, **Server**, or **Client** as the **Certificate Type**, enter a passphrase in **Passphrase** and confirm the passphrase in the **Retype Passphrase** field. If the certificate does not include a passphrase, there is no passphrase required. 8. Click **Upload Certificate** to complete the	1. Click the **Maintenance** link located directly above the Search bar in the Instant main window. 2. Click the **Certificates** tab. The **Certificates** tab contents are displayed. 3. To upload a certificate, click **Upload New Certificate**. The **New Certificate** window is displayed. 4. Browse and select the file to upload. Select any of the following types of certificates from the **Certificate type** drop-down list: a. **CA**—CA certificate to validate the identity of the client. b. **Auth Server**—The authentication server certificate to verify the identity of the server to the client. c. **Captive portal server**—Captive portal server certificate to verify the identity of internal captive portal server to the client. d. **RadSec**—The RadSec server certificate to verify the identity of the server to the client. e. **RadSec CA**—The RadSec CA certificate for mutual authentication between the Instant AP clients and the TLS server. f. **WebUI**—Customized certificate for WebUI management. 5. Select the certificate format from the **Certificate**

<table>
<tr><th>New WebUI</th><th>Old WebUI</th></tr>
<tr><td>certificate upload.</td><td rowspan="3">format drop-down list.
6. If you have selected Auth Server, Captive portal server, WebUI, or RadSec as the type of certificate, enter a passphrase in Passphrase and retype the passphrase. If the certificate does not include a passphrase, there is no passphrase required.
7. Click Browse and select the appropriate certificate file, and click Upload Certificate. The Certificate Successfully Installed message is displayed.</td></tr>
<tr><td>To assign certificate for an application:
1. Navigate to the Maintenance > Certificates page.
2. Click on Certificate Usage.
3. Click on add icon to assign certificates to an application. The New Certificate Assignment window is displayed.
4. Select the application you want to assign a certificate from the Application drop-down list.
5. Select the certificate type from the Certificate type drop-down list.
6. Select the certificate name from the Certificate name drop-down list.
7. Click OK to assign the certificate to the application.</td></tr>
<tr><td>To delete a certificate assigned to an application:
1. Navigate to the Maintenance > Certificates page.
2. Click on Certificate Usage.
3. Select the certificate assignment you want to delete and click on delete.
4. Click OK to delete the certificate assignment.</td></tr>
<tr><td colspan="2">NOTE:
The Instant AP database can have only one authentication server certificate and one captive portal server certificate at any point in time.
When a Captive Portal server certificate is uploaded with the WebUI option selected, the default management certificate on the Instant WebUI is also replaced by the Captive portal server certificate.
Certificates cannot be removed if they are assigned to an application. Therefore, ensure that you disassociate the certificate from an application before removing it.</td></tr>
</table>

Managing Certificates in the CLI

The following CLI command imports a certificate to the AP:

```
(Instant AP)#crypto pki-import
```

The following CLI command assigns certificates for an application:

```
(Instant AP)(config)#wlan cert-assignment-profile
```

The following CLI command removes a certificates on an AP:

```
(Instant AP)#crypto pki-remove
```

The following CLI command shows certificates installed on the AP:

```
(Instant AP)#show cert assignment
```

Loading Certificates Through AirWave

You can manage certificates using AirWave. The AMP directly provisions the certificates and performs basic certificate verification (such as certificate type, format, version, serial number, and so on) before accepting the certificate and uploading to an Instant AP network. The AMP packages the text of the certificate into an HTTPS message and sends it to the virtual controller. After the virtual controller receives this message, it draws the certificate content from the message, converts it to the right format, and saves it on the RADIUS server.

To load a certificate in AirWave:

1. Navigate to **Device Setup > Certificates** and then click **Add** to add a new certificate. The **Certificate** window is displayed.
2. Enter the certificate **Name**, and click **Choose File** to browse and upload the certificate.
3. Select the appropriate **Format** that matches the certificate filename.
4. Select **Server Cert** for certificate **Type**, and provide the passphrase if you want to upload a server certificate.
5. Select either **Intermediate CA** or **Trusted CA** certificate **Type**, if you want to upload a CA certificate.
6. After you upload the certificate, navigate to **Groups,** click the Instant **Group** and then select **Basic**. The Group name is displayed only if you have entered the **Organization** name in the WebUI. For more information, see Configuring Organization String on page 442 for further information.

   The **Virtual Controller Certificate** section displays the certificates (CA cert and Server).
7. Click **Save** to apply the changes only to AirWave. Click **Save and Apply** to apply the changes to the Instant AP.
8. To clear the certificate options, click **Revert**.

Loading Customized Certificates from AirWave

AirWave also provides users with the option of uploading customized certificates on the Instant AP. The customized certificate is uploaded on AirWave and then pushed to the Instant AP from the AirWave UI.

- Before uploading the new customized certificate, ensure that you uninstall any existing customized certificates on the Instant AP:

```
(Instant AP)# clear-cert-airwaveca
```

- Upload the customized certificate to AirWave and push it to the Instant AP. Refer to Loading Certificates Through AirWave on page 256
- Once the new customized certficate is uploaded to the Instant AP, verify the certfication installation using the following command:

```
(Instant AP)# show ap checksum
```

Perform these steps after you have verified that the new customized certificate is successfully installed on the Instant AP:

1. Delete PSK configuration from the Instant AP using the following command:

   ```
   (Instant AP)(config)# no ams-key
   ```
2. Add a DNS server and link the AMP IP address with the domain name of the new customized certificate.

3. Configure the AMP IP address

```
(Instant AP)(config)# ams-ip <domain_name>
```

4. In the AirWave UI, navigate to **AMP Setup** > **General** > **Aruba Instant Options** > **Change SSL Change** and click **Change**. Ensure you delete the ams-key for **cert-only mode** or **cert and psk mode**.
5. Add the Instant AP to AMP again.

Automatic Update of CA Certificate Bundle

Starting from Instant 8.7.0.0, the CA certificate bundle on the AP is updated automatically when a new version of CA certificate bundle is available on Activate. In addition to automatic update, a new CLI command is introduced to manually trigger the update. The CA certificate bundle update can only be triggered using the CLI.



The CA certificate bundle download will be triggered automatically if the SSL handshake between the AP and Activate or Aruba Central fails because of certificate error.

The following CLI command triggers the CA certificate bundle upgrade on the AP:

```
(Instant AP)# ca-bundle update
```

The following CLI command displays the version details of CA certificate bundle on the AP:

```
(Instant AP)# show ca-bundle version
```

The following CLI command displays the upgrade status of the CA certificate bundle:

```
(Instant AP)# show ca-bundle upgrade status
```

The following CLI command resets the CA certificate bundle to the factory default version:

```
(Instant AP)# ca-bundle reset
```

Chapter 15
Roles and Policies

This chapter describes the procedures for configuring user roles, role assignment, and firewall policies.

- Firewall Policies on page 259
- Content Filtering on page 273
- Configuring User Roles on page 277
- Configuring Derivation Rules on page 282
- Using Advanced Expressions in Role and VLAN Derivation Rules on page 290

Firewall Policies

Instant firewall provides identity-based controls to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for wired and wireless networks. Using Instant firewall, you can enforce network access policies that define access to the network, areas of the network that users may access, and the performance thresholds of various applications.

Instant supports a role-based stateful firewall. Instant firewall recognizes flows in a network and keeps track of the state of sessions. Instant firewall manages packets according to the first rule that matches the packet. The firewall logs on the Instant APs are generated as syslog messages.

ACL Rules

You can use ACL rules to either permit or deny data packets passing through the Instant AP. You can also limit packets or bandwidth available to a set of user roles by defining access rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses.

You can create access rules to allow or block data packets that match the criteria defined in an access rule. You can create rules for either inbound traffic or outbound traffic. Inbound rules explicitly allow or block the inbound network traffic that matches the criteria in the rule. Outbound rules explicitly allow or block the network traffic that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to an IP address through the firewall.

The Instant AP clients are associated with user roles, that determine the client's network privileges and the frequency at which clients re-authenticate.

Instant supports the following types of ACLs:

- ACLs that permit or deny traffic based on the source IP address of the packet.
- ACLs that permit or deny traffic based on the source or destination IP address, and the source or destination port number.
- ACLs that permit or deny traffic based on network services, application, application categories, web categories, and security ratings.



- You can configure up to 512 access control entries in an ACL for a user role.
- The maximum configurable universal role is 2048.

Configuring ACL Rules for Network Services

This section describes the procedure for configuring ACLs to control access to network services.

- For information on configuring access rules based on application and application categories, see Configuring ACL Rules for Application and Application Categories on page 384.
- For information on configuring access rules based on web categories and web reputation, see Configuring Web Policy Enforcement Service on page 387.

The following procedure describes how to configure ACL rules for a user roles using the WebUI.

Table 101: *Configuring ACL Rules for User Roles*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Security** > **Roles**. The **Roles** tab contents are displayed. Alternatively, you can configure access rules for a wired or wireless client through the WLAN wizard or the Wired Profile window. a. To configure access rules for a wired or wireless client, go to **Configuration** > **Networks** tab. Click **+** to create a new network or select the network profile to modify an existing profile. b. Go to the **Access** tab. 2. Select the role for which you want to configure access rules. 3. In the **Access rules** section, click **+** to add a new rule. The **New rule** window is displayed. 4. Ensure that the rule type is set to **Access Control**. 5. To configure a rule to control access to network services, select **Network** under the **Service** category and specify the parameters described in the Access Rule Configuration Parameters table below. 6. Click **OK** in the **New Rule** window and then click **Save**.	1. Navigate to **Security** > **Roles**. The **Roles** tab contents are displayed. Alternatively, you can configure access rules for a wired or wireless client through the WLAN wizard or the Wired Profile window. ▪ To configure access rules through the Wired Profile window: a. Navigate to **More** > **Wired**. b. Click **Edit** and then **Edit Wired Network**. c. Click **Access**. ▪ To configure access rules through WLAN wizard: a. Navigate to **Network > WLAN SSID**. b. Click **Edit** and then **Edit WLAN**. 2. Click **Access**. 3. Select the role for which you want to configure access rules. 4. In the **Access rules** section, click **New** to add a new rule. The **New Rule** window is displayed. 5. Ensure that the rule type is set to **Access Control**. 6. To configure a rule to control access to network services, select **Network** under the **Service** category and specify the parameters described in the Access Rule Configuration Parameters table below. 7. Click **OK** in the **New Rule** window and then click

New WebUI	Old WebUI
	OK in the **Roles** tab.

NOTE:

- The maximum roles configurable on an Instant AP is 64.
- The maximum ACL entries supported is 2048.
- The maximum ACL entries for each role is 512.

Table 102: *Access Rule Configuration Parameters*

Service Category	Description
Network	Select a service from the list of available services. You can allow or deny access to any or all of the services based on your requirement: ■ **any**—Access is allowed or denied to all services. ■ **custom**—Available protocols are **TCP**, **UDP**, **ethernet**, and **Other**. If you select the **TCP** or **UDP** protocol, enter appropriate port numbers. If you select the **Other** option, enter the appropriate ID. If you select the **ethernet** option, specify the ethernet type. **NOTE:** If TCP and UDP use the same port, ensure that you configure separate access rules to permit or deny access.
Action	Select any of following actions: ■ Select **Allow** to allow access to users based on the access rule. ■ Select **Deny** to deny access to users based on the access rule. ■ Select **Destination-NAT** to allow making changes to the destination IP address. ■ Select **Source-NAT** to allow making changes to the source IP address. • **Default**: All client traffic is directed to the default VLAN. • **Tunnel**: The traffic from the Network Assigned clients is directed to the VPN tunnel. • **VLAN**: Specify the non-default VLAN ID to which the guest traffic needs to be redirected to.
Destination	Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements. ■ **to all destinations**— Access is allowed or denied to all destinations. ■ **to a particular server**—Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server. ■ **except to a particular server**—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. ■ **to a network**—Access is allowed or denied to a network. After selecting this option, specify the IP address and netmask for the destination network. ■ **except to a network**—Access is allowed or denied to networks other than the

Table 102: *Access Rule Configuration Parameters*

Service Category	Description
	specified network. After selecting this option, specify the IP address and netmask of the destination network. ▪ **to domain name**—Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the **Domain Name** text box.
Log	Select the **Log** check box if you want a log entry to be created when this rule is triggered. Instant supports firewall-based logging. Firewall logs on the Instant APs are generated as security logs.
Blacklist	Select the **Blacklist** check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as **Auth failure blacklist time** on the Blacklisting tab of the **Security** window. For more information, see Blacklisting Clients on page 251.
Disable scanning	Select **Disable scanning** check box to disable ARM scanning when this rule is triggered. The selection of **Disable scanning** applies only if ARM scanning is enabled. For more information, see Configuring Radio Settings on page 377.
DSCP tag	Select the **DSCP tag** check box to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0–63. To assign a higher priority, specify a higher value.
802.1p priority	Select the **802.1p priority** check box to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value. **NOTE:** This parameter is applicable only for VLAN tagged frames.

The following CLI commands configure access rules:

```
(Instant AP)(config)# wlan access-rule <access-rule-name>
(Instant AP)(Access Rule <Name>)#rule <dest> <mask> <match/invert> {<protocol> <start-port> <end-port> {permit|deny|src-nat [vlan <vlan_id>|tunnel]|dst-nat{<IP-address> <port>|<port>}}[<option1....option9>]
```

Example

```
(Instant AP)(config)# wlan access-rule employee
(Instant AP)(Access Rule "employee")# rule 10.17.88.59 255.255.255.255 match 6 4343 4343 log
(Instant AP)(Access Rule "employee")# rule 192.0.2.8 255.255.255.255 invert 6 110 110 permit
(Instant AP)(Access Rule "employee")# rule 192.0.2.2 255.255.255.0 192.0.2.7 255.255.255.0 match tcp 21 21 deny
(Instant AP)(Access Rule "employee")# rule 192.0.2.2  255.255.255.0 192.0.2.7 255.255.255.0 match udp 21 21 deny
(Instant AP)(Access Rule "employee")# rule 192.0.2.2 255.255.255.0 match 6 631 631 permit
(Instant AP)(Access Rule "employee")# rule 192.0.2.8 255.255.255.255 invert 6 21 21 deny
(Instant AP)(Access Rule "employee")# rule 192.0.2.1 255.255.255.0 invert 17 67 69 deny
```

Configuring Extended ACLs

Starting from Instant 8.5.0.0, Instant APs support extended ACLs to configure firewall policies. Extended ACLs allow you to configure firewall policies based on the source IP and ethertype of the data packet. Extended ACLs can be configured only through the CLI.

The extended ACL types supported with Instant are:

- Session ACLs – These ACLs permit or deny traffic based on source and destination IP address, port number, or IP protocol.
- Ethertype ACLs – These ACLs permit or deny traffic based on the ethertype field in the frame header for non-IP packets.

Extended ACLs have the following limitations:

- Extended ACLs do not support IPv6.
- Extended ACLs are not supported with downloadable and pre-auth roles.

To enforce firewall policies using extended ACLs, configure the extended ACL and then attach it to the start of the **access-rule** command. When an extended ACL is added to the **access-rule**, the rules of the access list is applied first followed by the rules defined in the access-rule command.

Configuring an Extended ACL

The following CLI commands configure a session ACL using **wlan access-list session** command and create firewall policies based on source and destination IP:

```
(Instant AP)(config) # wlan access-list session <acl-name>
(Instant AP)(Session-ACL "<acl-name>") #rule <src> <smask> <dest> <mask> <match>
{<protocol> <start-port> <end-port> {permit|deny|src-nat [vlan <vlan id>|tunnel
<tunnel ip>]|dst-nat{<IP-address> <port>| <port>}| app <app> {permit| deny}|
appcategory <appgrp>| webcategory <webgrp> {permit| deny}| webreputation <webrep>}
[<opt1....opt11>]
```

The following CLI commands configure an ethertype using **wlan access-list eth** command and create firewall policies based on ethernet type:

```
(Instant AP)(config)# wlan access-list eth <name>
(Instant AP)(Eth-ACL "<name>")#rule {any | <eth-type>} {permit | deny}
```



Session and Ethertype ACLs allow upto 256 access control entries in a single ACL.

Attaching Extended ACLs to the Access Rule

A session ACL or ethertype ACL is added to the access-rule using the **access-list session <acl-name>** and **access-list eth <acl-name>** parameters of the **access-rule** command.

The following CLI commands configure extended ACLs to the access rule using **access-rule** command:

```
(Instant AP)(config)# wlan access-rule WirelessRule
(Instant AP)(Access Rule "WirelessRule")# access-list session <acl-name>
(Instant AP)(Access Rule "WirelessRule")# access-list eth <acl-name>
```

Configuring NAT Rules

NAT is the process of modifying network address information when packets pass through a routing device. The routing device acts as an agent between the public (the Internet) and the private (local network), which allows translation of private network IP addresses to a public address space.

Instant supports the NAT mechanism to allow a routing device to use the translation tables for mapping the private addresses into a single IP address. When packets are sent from this address, they appear to

originate from the routing device. Similarly, if packets are sent to the private IP address, the destination address is translated as per the information stored in the translation tables of the routing device.

Configuring a Source-NAT Access Rule

The source-NAT action in access rules allows the user to override the routing profile entries. For example, when a routing profile is configured to use 0.0.0.0/0, the client traffic in L3 mode access on an SSID destined to the corporate network is sent to the tunnel. When an access rule is configured with **Source-NAT** action, the users can specify the service, protocol, or destination to which the source-NAT is applied.

You can also configure source-based routing to allow client traffic on one SSID to reach the Internet through the corporate network, while the other SSID can be used as an alternate uplink. The following procedure describes how to create an access rule to perform source-NAT by using the WebUI.

Table 103: *Configuring Access Rule to Perform Source-NAT*

New WebUI	Old WebUI
1. Navigate to the WLAN wizard or the Wired settings window: ▪ To configure access rules for a wired or wireless client, go to **Configuration** > **Networks** page. Click **+** to create a new network or select the network profile to modify an existing profile and click **Edit**. 2. Select the **Access** tab. 3. To configure access rules for the network, select the **Network-based** in the **Access Rules** list box. To configure access rules for user roles, select **Role-based**. 4. To create an access rule for the network, click **+**. To create an access rule for a user role, select the user role in the **Roles** window and then click **+** in the **Access Rules for <network>** window. The **New rule** window is displayed. 5. In the **New rule** window, perform the following steps: a. Select **Access control** from the **Rule type** drop-down list. b. Select **Source-NAT** from the **Action** drop-down list, to allow for making changes to the source IP address. c. Select a Service from the list of available services in the **Network** drop down list box. ▪ **Default**: All client traffic by default will be directed to the native vlan. ▪ **Tunnel**: All network-based traffic will be directed to the VPN tunnel.	1. Navigate to the WLAN wizard or the Wired settings window: ▪ To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or click **edit** to modify an existing profile. ▪ To configure access rules for a wired profile, **More** > **Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile. 2. Click the **Access** tab. 3. To configure access rules for the network, move the slider to the **Network-based** access control type. To configure access rules for user roles, move the slider to the **Role-based** access control type. 4. To create a new rule for the network, click **New**. To create an access rule for a user role, select the user role and then click **New**. The **New Rule** window is displayed. 5. In the **New Rule** window, perform the following steps: a. Select **Access control** from the **Rule type** drop-down list. b. Select **Source-NAT** from the **Action** drop-down list, to allow for making changes to the source IP address. c. Select a service from the list of available services.

New WebUI	Old WebUI
▪ **VLAN**: All client based traffic will be directed to the specified uplink VLAN using the IP address of the interface that Instant AP has on that VLAN. If the interface is not found, this option has no effect. d. Select the required option from the **Destination** drop-down list. e. If required, enable other parameters such as **Log**, **Blacklist**, **Disable scanning**, **DSCP tag**,**Time Range** and **802.1p priority**. f. Click **OK**. 6. Click **Finish**.	▪ **Default**: All client traffic by default will be directed to the native vlan. ▪ **Tunnel**: All network-based traffic will be directed to the VPN tunnel. ▪ **VLAN**: All client based traffic will be directed to the specified uplink VLAN using the IP address of the interface that Instant AP has on that VLAN. If the interface is not found, this option has no effect. d. Select the required option from the **Destination** drop-down list. e. If required, enable other parameters such as **Log**, **Blacklist**, **Disable scanning**, **DSCP tag**, and **802.1p priority**. f. Click **OK**. 6. Click **Finish**.

The following CLI commands configure source-NAT access rule:

```
(Instant AP)(config)# wlan access-rule <access_rule>
(Instant AP)(Access Rule "<access_rule>")# rule <dest> <mask> <match> <protocol>
<sport> <eport> src-nat [vlan <vlan_id>|tunnel]
```

Configuring Policy-Based Corporate Access

To allow different forwarding policies for different SSIDs, you can configure policy-based corporate access. The configuration overrides the routing profile configuration and allows any destination or service to be configured to have direct access to the Internet (bypassing VPN tunnel) based on the ACL rule definition. When policy-based corporate access is enabled, the virtual controller performs source-NAT by using its uplink IP address.

To configure policy-based corporate access:

1. Ensure that an L3 subnet with netmask, gateway, VLAN, and IP address is configured. For more information on configuring L3 subnet, see Configuring Layer-3 Mobility on page 484.
2. Ensure that the source IP address is associated with the IP address configured for the L3 subnet.
3. Create an access rule for the SSID profile with Source-NAT action as described in Configuring a Source-NAT Access Rule on page 264. The source-NAT pool is configured and corporate access entry is created.

Configuring a Destination NAT Access Rule

Instant supports configuration of the destination NAT rule, which can be used to redirect traffic to the specified IP address and destination port. The destination NAT configuration is supported only in the bridge mode without VPN.

The following procedure describes how to configure a destination NAT access rule by using the WebUI:

Table 104: *Configuring Destination NAT Access Rule*

New WebUI	Old WebUI
1. Navigate to the WLAN wizard or the Wired settings window: ▪ To configure access rules for a wired or wireless client, go to **Configuration** > **Networks** tab. Click **+** to create a new network or select the network profile to modify an existing profile and click **Edit**. 2. Select the **Access** tab. 3. To configure access rules for the network, select the **Network-based** in the **Access Rules** list box. To configure access rules for user roles, select **Role-based**. 4. To create an access rule for the network, click **+**. To create an access rule for a user role, select the user role in the **Roles** window and then click **+** in the **Access Rules for <network>** window. The **New rule** window is displayed. 5. In the **New rule** window, perform the following steps: a. Select **Access control** from the **Rule type** drop-down list. b. Select **destination-NAT** from the **Action** drop-down list, to allow for making changes to the source IP address. c. Specify the IP address and port details. d. Select a Service from the list of available services in the **Network** drop down list box. e. Select the required option from the **Destination** drop-down list. f. If required, enable other parameters such as **Log**, **Blacklist**, **Disable scanning**, **DSCP tag**, **Time Range** and **802.1p priority**. g. Click **OK**. 6. Click **Finish**.	1. Navigate to the WLAN wizard or the Wired settings window: ▪ To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or click **edit** to modify an existing profile. ▪ To configure access rules for a wired profile, **More > Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile. 2. Click the **Access** tab. 3. To configure access rules for the network, move the slider to the **Network-based** access control type. To configure access rules for user roles, move the slider to the **Role-based** access control type. 4. To create a new rule for the network, click **New**. To create an access rule for a user role, select the user role and then click **New**. The **New Rule** window is displayed. 5. In the **New Rule** window, perform the following steps: a. Select **Access control** from the **Rule type** drop-down list. b. Select **destination-NAT** from the **Action** drop-down list, to allow for making changes to the source IP address. c. Specify the IP address and port details. d. Select a service from the list of available services. e. Select the required option from the **Destination** drop-down list. f. If required, enable other parameters such as **Log**, **Blacklist**, **Disable scanning**, **DSCP tag**, and **802.1p priority**. g. Click **OK**. 6. Click **Finish**.

The following CLI commands configure destination NAT access rule:

```
(Instant AP)(config)# wlan access-rule <access_rule>
```

```
(Instant AP)(Access Rule "<access_rule>")# rule <dest> <mask> <match> <protocol>
<sport>       <eport>  dst-nat ip <IP-address> [<port>]
```

Configuring ALG Protocols

The following procedure describes how to enable or disable protocols for ALG using the WebUI:

Table 105: *Configuring ALG Protocols*

New WebUI	Old WebUI
1. Go to **Configuration** > **Security**. 2. Expand **Firewall Settings**. 3. Under **Application Layer Gateway Algorithms**, the **SIP**, **VOCERA**, **Alcatel NOE**, and **Cisco Skinny** protocols are enabled by default. To disable a specific protocol, toggle the corresponding switch to disable. 4. Click **Save**.	1. Click the **Security** link located directly above the Search bar on the Instant main window. 2. Click the **Firewall Settings** tab. 3. Select **Enabled** from the corresponding drop-down lists to enable SIP, VOCERA, Alcatel NOE, and Cisco Skinny protocols. 4. Click **OK**.
NOTE: When the protocols for ALG are set to **Disabled**, the changes are not applied until the existing user sessions expire. Reboot the Instant AP and the client, or wait for a few minutes to view the changes.	

The following CLI commands configure protocols for ALG:

```
(Instant AP)(config)# alg
(Instant AP)(ALG)# sccp-disable
(Instant AP)(ALG)# no sip-disable
(Instant AP)(ALG)# no ua-disable
(Instant AP)(ALG)# no vocera-disable
```

The following CLI command shows the ALG configuration:

```
(Instant AP)# show alg
```

Configuring Firewall Settings for Protection from ARP Attacks

The following procedure describes how to configure firewall settings to protect the network against ARP attacks using the WebUI:

Table 106: *Configuring Firewall Settings for protection against ARP Attacks*

New WebUI	Old WebUI
1. Go to **Configuration** > **Security**. 2. Expand **Firewall Settings**. 3. To configure protection against security attacks, under **Protection against wired attacks** select the following check boxes: ▪ Toggle the **Drop bad ARP** switch to enable the Instant AP to drop the fake ARP packets.	1. Click the **Security** link located directly above the search bar on the Instant main window. 2. Click the **Firewall Settings** tab. The contents of the **Firewall Settings** tab are displayed. 3. To configure protection against security attacks, select the following check boxes: ▪ Select **Enable** from the **Drop bad ARP** drop-down list to enable the Instant AP to

New WebUI	Old WebUI
▪ Toggle the **Fix malformed DHCP** switch to enable the Instant AP to fix the malformed DHCP packets. ▪ Toggle the **ARP poison check** switch to enable the Instant AP to trigger alerts about ARP poisoning that may have been caused by rogue Instant APs. ARP poisoning detection triggers alerts when a known client on the Instant AP spoofs the base MAC address of the Instant AP. 4. Click **Save**.	drop the fake ARP packets. ▪ Select **Enable** from the **Fix malformed DHCP** drop-down list to enable the Instant AP to fix the malformed DHCP packets. ▪ Select **Enable** from the **ARP poison check** drop-down list to enable the Instant AP to trigger alerts about ARP poisoning that may have been caused by rogue Instant APs. ARP poisoning detection triggers alerts when a known client on the Instant AP spoofs the base MAC address of the Instant AP. 4. Click **OK**.

The following CLI commands configure firewall settings to prevent attacks:

```
(Instant AP)(config)# attack
(Instant AP)(ATTACK)# drop-bad-arp-enable
(Instant AP)(ATTACK)# fix-dhcp-enable
(Instant AP)(ATTACK)# no
(Instant AP)(ATTACK)# poison-check-enable
```

The following CLI command shows the configuration status:

```
(Instant AP)# show attack config
Current Attack
--------------
Attack        Status
------        ------
drop-bad-arp  Enabled
fix-dhcp      Enabled
poison-check  Enabled
```

The following CLI command shows the attack statistics:

```
(Instant AP)# show attack stats
attack counters
---------------------------------------
Counter                                 Value
-------                                 -------
arp packet counter                      0
drop bad arp packet counter             0
dhcp response packet counter            0
fixed bad dhcp packet counter           0
send arp attack alert counter           0
send dhcp attack alert counter          0
arp poison check counter                0
garp send check counter                 0
```

Auto Topology Rules

Auto Topology is a feature that automatically adds ACL rules into the firewall. This ensures that any kind of control-plane messages required for the automatic cluster formation are never blocked. By default, this feature is enabled. However, this feature can be disabled when customers prefer full control on the

security policy rather than accepting automatic ACL rules. This feature governs all the ACLs and impacts all the traffic that is hit by the ACLs.

Configuring Firewall Settings to Disable Auto Topology Rules

You can disable the rules by configuring firewall settings in the Instant AP.

In order to deny auto topology communication outside the Instant AP subnet, the inbound firewall settings must be enabled.

When the inbound firewall settings are enabled:

- ACEs must be configured to block auto topology messages, as there is no default rule at the top of predefined ACLs.
- ACEs must be configured to override the guest VLAN auto-expanded ACEs. In other words, the user defined ACEs take higher precedence over guest VLAN ACEs.

For more information on inbound firewall settings, see Managing Inbound Traffic on page 269



The priority of a particular ACE is determined based on the order in which it is programmed. Ensure that you do not accidentally override the guest VLAN ACEs.

The following procedure describes how to change the status of auto topology rules by using the WebUI:

Table 107: *Configuring the Status of Auto Topology Rules*

New WebUI	Old WebUI
1. Go to **Configuration** > **Security**. 2. Expand **Firewall Settings**. 3. Under **Firewall**, The **Auto topology rules** setting is enabled by default. To disable this setting, toggle the switch. 4. Click **Save**.	1. Click the **Security** located directly above the Search bar in the Instant main window. 2. Go to the **Firewall Settings** tab. 3. In **Firewall** section, select **Disabled** from the **Auto topology rules** drop-down list. 4. Click **OK**.

The following CLI commands disable auto topology rules:

```
(Instant AP)(config)# firewall
(Instant AP)(firewall)# disable-auto-topology-rules
```

The following CLI command shows the configuration status:

```
(Instant AP) # show firewall
```

Managing Inbound Traffic

Instant now supports an enhanced inbound firewall by allowing the configuration of firewall rules and management subnets, and restricting corporate access through an uplink switch.

To allow flexibility in firewall configuration, Instant supports the following features:

- Inbound firewall rules
- Configurable management subnets
- Restricted corporate access

Configuring Inbound Firewall Rules

You can now configure firewall rules for the inbound traffic coming through the uplink ports of an Instant AP. The rules defined for the inbound traffic are applied if the destination is not a user connected to the Instant AP. If the destination already has a user role assigned, the user role overrides the actions or options specified in the inbound firewall configuration. However, if a deny rule is defined for the inbound traffic, it is applied irrespective of the destination and user role. Unlike the ACL rules in a WLAN SSID or a wired profile, the inbound firewall rules can be configured based on the source subnet.



- For all subnets, a deny rule is created by default as the last rule. If at least one rule is configured, the deny all rule is applied to the upstream traffic by default.
- Management access to the Instant AP is allowed irrespective of the inbound firewall rule. For more information on configuring restricted management access, see Configuring Management Subnets on page 272.
- The inbound firewall is not applied to traffic coming through the GRE tunnel.

The following procedure describes how to configure inbound firewall rules through the WebUI:

Table 108: *Configuring Inbound Firewall Rules*

New WebUI	Old WebUI
1. Navigate to the **Configuration > Security** page. 2. Expand **Inbound Firewall**. 3. Under **Inbound Firewall Rules**, click **+**. 4. Configure the parameters described in the Inbound Firewall Rule Configuration Parameters table below. 5. Click **OK** in the **New Rule** window and then click **Save**.	1. Navigate to **Security** > **Inbound Firewall**. 2. Under **Inbound Firewall Rules**, click **New**. 3. Configure the parameters described in the Inbound Firewall Rule Configuration Parameters table below. 4. Click **OK** in the **New Rule** window and then click **OK** in the **Inbound Firewall** tab.

Table 109: *Inbound Firewall Rule Configuration Parameters*

Parameter	Description
Action	Select any of following actions: ■ Select **Allow** to allow to access users based on the access rule. ■ Select **Deny** to deny access to users based on the access rule. ■ Select **Destination-NAT** to allow making changes to the destination IP address and the port. ■ Select **Source-NAT** to allow making changes to the source IP address. The destination NAT and source NAT actions apply only to the network services rules.
Service	Select a service from the list of available services. You can allow or deny access to any or all of the services based on your requirement: ■ **any**—Access is allowed or denied to all services. ■ **custom**—Available options are **TCP**, **UDP**, and **Other**. If you select the **TCP** or **UDP** options, enter appropriate port numbers. If the **Other** option is selected, ensure that

Table 109: *Inbound Firewall Rule Configuration Parameters*

Parameter	Description
	an appropriate ID is entered.
Source	Select any of the following options: ■ **from all sources**—Traffic from all sources is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. ■ **from a host**—Traffic from a particular host is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address of the host. ■ **from a network**—Traffic from a particular network is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address and netmask of the source network.
Destination	Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements. ■ **to all destinations**—Traffic for all destinations is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. ■ **to a particular server**—Traffic to a specific server is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address of the destination server. ■ **except to a particular server**—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. ■ **to a network**—Traffic to the specified network is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address and netmask for the destination network. ■ **except to a network**—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. ■ **to domain name**—Traffic to the specified domain is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the domain name in the **Domain Name** text box.
Log	Select the **Log** check box if you want a log entry to be created when this rule is triggered. Instant supports firewall-based logging function. Firewall logs on the Instant APs are generated as security logs.
Blacklist	Select the **Blacklist** check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified in the **Auth failure blacklist time** on the **Blacklisting** tab of the **Security** window. For more information, see Blacklisting Clients on page 251.
Disable scanning	Select **Disable scanning** check box to disable ARM scanning when this rule is triggered. The selection of **Disable scanning** applies only if ARM scanning is enabled. For more information, see Configuring Radio Settings on page 377.

Table 109: *Inbound Firewall Rule Configuration Parameters*

Parameter	Description
DSCP tag	Select the **DSCP tag** check box to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0–63. To assign a higher priority, specify a higher value.
802.1p priority	Select the **802.1p priority** check box to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value.

The following CLI commands configure inbound firewall rules:

```
(Instant AP)(config)# inbound-firewall
(Instant AP)(inbound-firewall)# rule <subnet> <smask> <dest> <mask> <protocol> <sport>
<eport> {permit|deny|src-nat|dst-nat <IP-address> <port>} [<option1....option9>]
```

Configuring Management Subnets

You can configure subnets to ensure that the Instant AP management is carried out only from these subnets. When the management subnets are configured, access through Telnet, SSH, and UI is restricted to these subnets only.

The following procedure describes how to configure management subnets by using the WebUI:

Table 110: *Configuring Management Subnets*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **Security** page. 2. Expand **Inbound Firewall**. 3. To add a new management subnet: ▪ Under **Management Subnets**, click **+**. The **Add new management subnet** window is displayed. ▪ Enter the subnet IP address in **Subnet**. ▪ Enter the subnet mask in **Mask**. ▪ Click **OK**. 4. To add multiple subnets, repeat step 3. 5. Click **Save**.	1. Navigate to the **Security** > **Inbound Firewall** tab. 2. To add a new management subnet: ▪ In the **Add new management subnet** section, enter the subnet address in **Subnet**. ▪ Enter the subnet mask in **Mask**. ▪ Click **Add**. 3. To add multiple subnets, repeat step 2. 4. Click **OK**.

The following CLI command configures a management subnet:

```
(Instant AP)(config) # restricted-mgmt-access <subnet-IP-address> <subnet-mask>
```

Configuring Restricted Access to Corporate Network

You can configure restricted corporate access to block unauthorized users from accessing the corporate network. When restricted corporate access is enabled, corporate access is blocked from the uplink port of master Instant AP, including clients connected to a slave Instant AP.

The following procedure describes how to configure restricted corporate access by using the WebUI:

Table 111: *Configuring Firewall Settings for protection against ARP Attacks*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **Security** page. 2. Expand **Inbound Firewall** tab. 3. Select **Enabled** from the **Restrict Corporate Access** drop-down list. 4. Click **Save**.	1. Click the **Security** link located directly above the search bar on the Instant main window. Navigate to the **Security** > **Inbound Firewall** tab. 2. Select **Enabled** from the **Restrict Corporate Access** drop-down list. 3. Click **OK**.

The following CLI command configures restricted management access:

```
(Instant AP)(config) # restrict-corp-access
```

Content Filtering

The content filtering feature allows you to route DNS requests and create content filtering policies.

With content filter, you can achieve the following:

- Block certain categories of websites based on your organization policy. For example, if you block the **web-based-email** category, clients who are assigned this policy will not be able to visit email-based websites such as mail.yahoo.com.
- Prevent known malware hosts from accessing your wireless network.
- Improve employee productivity by limiting access to certain websites.
- Reduce bandwidth consumption significantly.



Regardless of whether content filtering is disabled or enabled, the DNS requests to http://instant.arubanetworks.com are always resolved internally on Instant.

The content filtering configuration applies to all Instant APs in the network and the service is enabled or disabled globally across the wireless or wired network profiles.

Enabling Content Filtering

This section describes the following procedures:

- Enabling Content Filtering for a Wireless Profile on page 273
- Enabling Content Filtering for a Wired Profile on page 274

Enabling Content Filtering for a Wireless Profile

The following procedure describes how to enable content filtering for a wireless SSID in the WebUI.

Table 112: *Configuring Content Filtering for a Wireless Profile*

New WebUI	Old WebUI
1. Select a wireless profile in the **Configuration** > **Networks** section and click **Edit**. The window for editing the WLAN SSID profile is displayed. 2. Click **Show advanced options** at the bottom of the window.	1. Select a wireless profile in the **Network** tab and then click the **edit** link. The window for editing the WLAN SSID profile is displayed. 2. Click **Show advanced options**. 3. Under **Miscellaneous**, select **Enabled** from

New WebUI	Old WebUI
3. Under **Miscellaneous**, toggle the **Content filtering** switch to enable. 4. Click **Next** to continue.	**Content Filtering** drop-down list, and click **Next** to continue.

You can also enable content filtering while adding a new WLAN profile. For more information, see Configuring WLAN Settings for an SSID Profile on page 131.

The following CLI commands enable content filtering on a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# content-filtering
```

Enabling Content Filtering for a Wired Profile

The following procedure describes how to enable content filtering for a wired profile using the WebUI.

Table 113: *Configuring Content Filtering for a Wired Profile*

New WebUI	Old WebUI
1. Select a wired profile in the **Configuration** > **Networks** section and click **Edit**. The window for editing the wired profile is displayed. 2. Click **Show advanced options** at the bottom of the window. 3. Under **Miscellaneous**, toggle the **Content filtering** switch to enable. 4. Click **Next** to continue.	1. Click the **Wired** link under **More** in the Instant main window. The **Wired** window is displayed. 2. In the **Wired** window, select the wired profile to modify. 3. Click **Edit**. The **Edit Wired Network** window is displayed. 4. In the **Wired Settings** tab, select **Enabled** from the **Content Filtering** drop-down list, and click **Next** to continue.

The following CLI commands enable content filtering for a wired profile:

```
(Instant AP)(config)# wired-port-profile test
(Instant AP)(wired ap profile <name>)# content-filtering
```

Configuring Enterprise Domains

The enterprise domain names list displays the DNS domain names that are valid on the enterprise network. This list is used to determine how client DNS requests must be routed.

The following procedure describes how to configure an enterprise domain through the WebUI.

Table 114: *Configuring Enterprise Domains*

New WebUI	Old WebUI
1. Go to **Configuration** > **Tunnelling** . 2. Expand **Enterprise Domains**. 3. Click **+** and enter a new domain name. 4. Click **OK** . 5. Click **Save**.	1. Click the **Tunnelling** link under **More** in the Instant main window. 2. In the **Tunnelling** window, select **Enterprise Domains**. 3. Click **New** and enter a new domain name. 4. Click **OK** . 5. Click **Finish**.
NOTE: To delete a domain, select the domain and click **Delete**. This will remove the domain name from the list.	

The following CLI commands configure an enterprise domain:

```
(Instant AP)(config)# internal-domains
(Instant AP)(domain)# domain-name <name>
```

Configuring URL Filtering Policies

The following procedure describes how to configure URL filtering policies to block certain categories of websites based on your organization specifications by defining ACL rules either through the WebUI.

Table 115: *Configuring URL Filtering Policies*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Security**. 2. Expand **Roles**. 3. In the **Roles** window, select any WLAN SSID or wired profile role, and click **+** in the **Access Rules for <network>** section. The **New rule** window is displayed. 4. Select **Access Control** from the **Rule type** drop-down list. 5. To set an access policy based on the web category: a. Under **Service** section, select **Web category** and expand the drop-down list that contains the web categories. b. Select the categories to which you want to deny or allow access. You can also search for a web category and select the required option. c. From the **Action** drop-down list, select **Allow** or **Deny** as required. 6. To filter access based on the security ratings of the website: a. Select **Web reputation** under **Service**. b. Move the slider to the required security rating level. c. From the **Action** drop-down list, select **Allow** or **Deny** as required. 7. To set a bandwidth limit based on web category or web reputation score, select the **Application Throttling** check box and specify the downstream and upstream rates in Kbps. For example, you can set a higher bandwidth for trusted sites and a low bandwidth rate for high-risk sites. 8. Click **OK** to save the rules. 9. Click **Save** to save the changes to the role for which you defined ACL rules.	1. Navigate to **Security** > **Roles**. 2. In the **Roles** window, select any WLAN SSID or wired profile role, and click **New** in the **Access Rules for <network>** section. The **New Rule** window is displayed. 3. Select **Access Control** from the **Rule Type** drop-down list. 4. To set an access policy based on the web category: a. Under **Service** section, select **Web category** and expand the drop-down list that contains the web categories. b. Select the categories to which you want to deny or allow access. You can also search for a web category and select the required option. c. From the **Action** drop-down list, select **Allow** or **Deny** as required. d. Click **OK**. 5. To filter access based on the security ratings of the website: a. Select **Web reputation** under **Service** section. b. Move the slider to the required security rating level. c. From the **Action** drop-down list, select **Allow** or **Deny** as required. 6. To set a bandwidth limit based on web category or web reputation score, select the **Application Throttling** check box and specify the downstream and upstream rates in Kbps. For example, you can set a higher bandwidth for trusted sites and a low bandwidth rate for high-risk sites. 7. Click **OK** to save the rules. 8. Click **OK** in the **Roles** tab to save the changes to the role for which you defined ACL rules.

The following CLI commands control access based on web categories and security ratings:

```
(Instant AP)(config)# wlan access-rule <access_rule>
```

```
(Instant AP)(Access Rule "<access-rule>")# rule <dest> <mask> <match> webcategory
<webgrp> {permit| deny}[<option1....option9>]
(Instant AP)(Access Rule "<access-rule>")# rule <dest> <mask> <match> webreputation
<webrep> {permit|deny}[<option1....option9>]
```

Creating Custom Error Page for Web Access Blocked by AppRF Policies

You can create a list of URLs to which the users are redirected when they access blocked websites. You can define an access rule to use these redirect URLs and assign the rule to a user role in the WLAN network.

Creating a List of Error Page URLs

The following procedure describes how to create a list of custom URLs and ACL rules for blocked websites either through the WebUI.

Table 116: *Configuring List of Error Page URLs*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Security** > **Custom Blocked Page URL**. 2. Click **+** and enter the URL that you want to block. 3. Repeat the procedure to add more URLs. You can add up to 8 URLs to the blocked page list. 4. Click **OK** in the **URL** window. 5. Click **Save**.	1. Navigate to **Security** > **Custom Blocked Page URL**. 2. Click **New** and enter the URL that you want to block. 3. Repeat the procedure to add more URLs. You can add up to 8 URLs to the blocked page list. 4. Click **OK** in the **URL** window. 5. Click **OK** in the **Custom Blocked Page URL** tab.

The following CLI command creates a list of error page URLs:

```
(Instant AP)(config)# dpi-error-page-url <idx> <url>
```

Configuring ACL Rules to Redirect Blocked HTTP Websites to a Custom Error Page URL

The following procedure describes how to redirect blocked HTTP websites to a custom error page URL.

Table 117: *Configuring ACL Rules to Redirect Blocked HTTP Websites to a Custom Error Page URL*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Security** > **Roles**. 2. In the **Roles** window, select any WLAN SSID or Wired profile role, and click **+** in the **Access Rules for <network>** section. 3. In the **New rule** window, select the rule type as **Redirect Page URL**. 4. Select the URLs from the existing list of custom redirect URLs and click **OK**. 5. Click **Save**.	1. Navigate to **Security** > **Roles**. 2. In the **Roles** window, select any WLAN SSID or Wired profile role, and click **New** in the **Access Rules for <network>**section. 3. In the **New Rule** window, select the rule type as **Redirect Page URL**. 4. Select the URLs from the existing list of custom redirect URLs. To add a new URL, click **New**, add the URL, and click **OK** in the **URL** window. 5. Click **OK** in the **Roles** tab to save the changes.

The following CLI commands configure an ACL rule to redirect blocked HTTP websites to a custom error page URL:

```
(Instant AP)(config)# wlan access-rule <access_rule_name>
```

```
(Instant AP) (Access Rule "<access_rule_name>")# dpi-error-page-url <idx>
```

Configuring ACL Rules to Redirect Blocked HTTPS Websites to a Custom Blocked Page URL



Before you configure an ACL rule for a specific WLAN SSID or Wired profile to redirect HTTPS websites to a custom error page, you must ensure that the Blocked Page URL rule is configured for the HTTP websites blocked for the same WLAN SSID or Wired profile. In this scenario, all the blocked HTTP and HTTPS websites will be redirected to the custom error page URL.

The following procedure describes how to redirect blocked HTTPS websites to a custom error page URL.

Table 118: *Configuring ACL Rules to Redirect Blocked HTTPS Websites to a Custom Blocked Page URL*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Security** > **Roles**. 2. Select any WLAN SSID or Wired profile role, and click **+** in the **Access Rules for <network>** section. 3. In the **New Rule** window, select the rule type as **Redirect Blocked HTTPS**. 4. Click **OK** in the **New rule** window.. 5. Click **Save**.	1. Navigate to **Security** > **Roles**. 2. Select any WLAN SSID or Wired profile role, and click **New** in the **Access Rules for <network>** section. 3. In the **New Rule** window, select the rule type as **Redirect Blocked HTTPS**. 4. Click **OK** in the **New Rule** window. 5. Click **OK** in the **Roles** tab to save the changes.

The following CLI commands configure an ACL rule to redirect blocked HTTPS to a custom error page URL:

```
(Instant AP)(config)# wlan access-rule <access_rule_name>
(Instant AP) (Access Rule "<access_rule_name>")# dpi-error-page-url <idx>
(Instant AP) (Access Rule "<access_rule_name>")# redirect-blocked-https-traffic
```

Configuring User Roles

Every client in the Instant network is associated with a user role that determines the network privileges for a client, the frequency of reauthentication, and the applicable bandwidth contracts.



Instant allows you to configure up to 64 user roles. If the number of roles exceed 64, an error message is displayed.

The user role configuration on an Instant AP involves the following procedures:

- Creating a User Role on page 277
- Assigning Bandwidth Contracts to User Roles on page 278
- Configuring Machine and User Authentication Roles on page 279
- Configuring Downloadable User Roles (DUR) on page 280
- ClearPass Policy Manager Certificate Validation for Downloadable User Roles (DUR) on page 281

Creating a User Role

The following procedure describes how to create a user role by using the WebUI:

Table 119: *Creating a User Role*

New WebUI	Old WebUI
1. Go to **Configuration** > **Security**. 2. Click the **Roles** tab. The **Roles** tab contents are displayed. 3. Under **Roles**, click **+**. 4. Enter a name for the new role and click **OK**. 5. Click **Save** in the **Roles** tab.	1. Click the **Security** link located directly above the Search bar in the Instant main window. The **Security** window is displayed. 2. Click the **Roles** tab. The Roles tab contents are displayed. 3. Under Roles, click **New**. 4. Enter a name for the new role and click **OK**. 5. Click **OK** in the **Roles** tab to save the changes.
NOTE: You can also create a user role when configuring wireless or wired network profiles. For more information, see Configuring Access Rules for a WLAN SSID Profile on page 146 and Configuring Access Rules for a Wired Profile on page 167.	

The following CLI commands configure user roles and access rules:

```
(Instant AP)(config)# wlan access-rule <access-rule-name>
(Instant AP)(Access Rule <Name>)# rule <dest> <mask> <match> <protocol> <start-port>
<end-port> {permit|deny|src-nat [vlan <vlan_id>|tunnel]|dst-nat {<IP-address>
<port>|<port>}}[<option1…option9>]
```

Assigning Bandwidth Contracts to User Roles

The administrators can manage bandwidth utilization by assigning either maximum bandwidth rates, or bandwidth contracts to user roles. The administrator can assign a bandwidth contract configured in Kbps to upstream (client to the Instant AP) or downstream (Instant AP to clients) traffic for a user role.

By default, all users that belong to the same role share a configured bandwidth rate for upstream or downstream traffic. The assigned bandwidth will be served and shared among all the users. You can also assign bandwidth rate per user to provide every user a specific bandwidth within a range of 1–65,535 Kbps. If there is no bandwidth contract specified for a traffic direction, unlimited bandwidth is allowed.



In the earlier releases, bandwidth contract could be assigned per SSID. In the current release, the bandwidth contract can also be assigned for each SSID user. If the bandwidth contract is assigned for an SSID in the Instant 6.2.1.0-3.4.0.0 version, and when the Instant AP is upgraded to a later release version, the bandwidth configuration per SSID will be treated as a per-user downstream bandwidth contract for that SSID.

The bandwidth contract for a user role can be applied to an Instant AP or to a cluster.

Example

In a cluster of 5 Instant APs with an upstream WAN limit of 100 Mbps, you must set the WAN limit to 20 Mbps for each Instant AP, in order to meet the requirement of maintaining the WAN limit of 100 Mbps. However, clients cannot exceed 20 Mbps when needed, even if the cluster output is less then 100 Mbps.

If you want to add more Instant APs, you must re-calculate the WAN limit and manually apply it. It is recommended that you apply the WAN limit at cluster level as it is more flexible. Also, there is no need to manually re-calculate the WAN limit if additional Instant APs are added or removed, in order to meet the upstream WAN constraints.

Table 120: *Assigning Bandwidth Contracts to User Roles*

New WebUI	Old WebUI
1. Go to **Configuration** > **Security**. 2. Expand **Roles** tab. 3. Create a new role (see Creating a User Role on page 277) or select an existing role. 4. Under **Access Rules**, click **+**. The **New rule** window is displayed. 5. Select **Bandwidth Contract** from the **Rule type** drop-down list. 6. Specify the downstream and upstream rates in Kbps. If the assignment is specific for each user, select the **Per user** check box. 7. Click **OK**. 8. Click **Save**. 9. To associate the user role to a WLAN SSID or a wired profile, navigate to the WLAN wizard or Wired window. ▪ Go to **Configuration** > **Networks** and select a network profile to modify and click **Edit**. ▪ Select **Access** tab. Select **Role-based** in the **Access Rules** drop-down list. ▪ Under **Role Assignment Rules**, click **+**. ▪ Select the user role from the **Role** drop-down list and then click **OK**. ▪ Click **Finish**.	1. Click the **Security** link located directly above the Search bar in the Instant main window. The **Security** window is displayed. 2. Click the **Roles** tab. The **Roles** tab contents are displayed. 3. Create a new role (see Creating a User Role on page 277) or select an existing role. 4. Under **Access Rules**, click **New**. The **New Rule** window is displayed. 5. Select **Bandwidth Contract** from the **Rule type** drop-down list. 6. Specify the downstream and upstream rates in Kbps. If the assignment is specific for each user, select the **Per user** check box. 7. Click **OK**. 8. Click **OK** in the **Roles** tab to save the changes. 9. Associate the user role to a WLAN SSID or a wired profile. 10. To associate the user role to a WLAN SSID or a wired profile, navigate to the WLAN wizard or Wired window. ▪ Go to the **Access** tab. Move the slider to **Role-based** in the **Access Rules** section. ▪ Under **Role Assignment Rules**, click **New**. ▪ Select the user role from the **Role** drop-down list and then click **OK**. ▪ Click **Next** and then click **Finish**.

The following CLI commands assign a bandwidth contract:

```
(Instant AP)(config)# wlan access-rule <name>
(Instant AP)  (Access Rule <name>)# bandwidth-limit {downstream <kbps>|upstream
<kbps>|peruser {downstream <kbps>| upstream <kbps>}}
```

The following CLI commands associate the access rule to a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# access-rule-name <access-rule-name>
```

Configuring Machine and User Authentication Roles

You can assign different rights to clients based on whether their hardware device supports machine authentication. Machine authentication is only supported on Windows devices, so that this can be used to distinguish between Windows devices and other devices such as iPads.

You can create any of the following types of rules:

- **Machine Auth only** role—This indicates a Windows machine with no user logged in. The device supports machine authentication and has a valid RADIUS account, but a user has not yet logged in and authenticated.
- **User Auth only** role—This indicates a known user or a non-Windows device. The device does not support machine authentication or does not have a RADIUS account, but the user is logged in and authenticated.

When a device does both machine and user authentication, the user obtains the default role or the derived role based on the RADIUS attribute.

The following procedure describes how to configure machine authentication with role-based access control using the WebUI.

Table 121: *Configuring Machine Authentication with Role-Based Access Control*

New WebUI	Old WebUI
1. Go to **Configuration** > **Networks**. To modify an existing network profile, select the profile and click **Edit**. To create a new network, click **+**. 2. Select the **Access** tab. 3. Select **Role-based** from the **Access Rules** drop-down list. 4. Toggle the **Enforce Machine Authentication** switch to enable. 5. Configure access rules for these roles by selecting the roles in the **Machine auth only** and **User auth only** drop-down lists. For more information on configuring access rules, see Configuring ACL Rules for Network Services on page 260. 6. Click **Next** and then click **Finish** to apply these changes. 7. Click **Finish**.	1. In the **Access** tab of the WLAN wizard (**New WLAN** or **Edit <WLAN-profile>**) or in the wired profile configuration window (**New Wired Network** or **Edit Wired Network**), click the **Enforce Machine Authentication** check box. 2. Configure access rules for these roles by selecting the roles in the **Machine auth only** and **User auth only** drop-down lists. For more information on configuring access rules, see Configuring ACL Rules for Network Services on page 260. 3. Select **Enforce Machine Authentication** and select the **Machine auth only** and **User auth only** roles. 4. Click **Finish** to apply these changes.

The following CLI commands configure machine and user authentication roles for a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role-machine-auth <machine_only> <user_only>
```

The following CLI commands configure machine and user authentication roles for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# set-role-machine-auth <machine_only> <user_
only>
```

Configuring Downloadable User Roles (DUR)

Aruba Instant and ClearPass Policy Manager include support for centralized policy definition and distribution. When ClearPass Policy Manager successfully authenticates a user, the user is assigned a role by ClearPass Policy Manager. If the role is not defined on the Instant AP, the role attributes can also be downloaded automatically.

In order to provide highly granular per-user level access, user roles can be created when a user has been successfully authenticated. During the configuration of a policy enforcement profile in ClearPass

Policy Manager, the administrator can define a role that should be assigned to the user after successful authentication. In RADIUS authentication, when ClearPass Policy Manager successfully authenticates a user, the user is assigned a role by ClearPass Policy Manager. If the role is not defined on the Instant AP, the role attributes can also be downloaded automatically. This feature supports roles obtained by the following authentication methods:

- 802.1X (WLAN and wired users)
- MAC authentication
- Captive Portal

The following procedure enables role download on a SSID using the WebUI:

1. Go to **Configuration** > **Networks**. To modify an existing network profile, select the profile and click **Edit**. To create a new network, click **+**.
2. Select the **Access** tab.
3. Slide the toggle switch next to **Download roles**, to the right, to enable user role download on the SSID.

The following CLI commands enable role download:

```
(Instant AP)(config)# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile <profile_name>)# download-role
(Instant AP)(SSID Profile <profile_name>)# end
(Instant AP)# commit apply
```

The following CLI commands configure a ClearPass Policy Manager username and password for RADIUS authentication:

```
(Instant AP)(config)# wlan auth-server <profile_name>
(Instant AP)(Auth Server <profile_name>)# cppm {username <username> password
<password>}
(Instant AP)(Auth Server <profile_name>)# end
(Instant AP)# commit apply
```

The following CLI command checks if role download is enabled on the network profile:

```
(Instant AP)# show network <profile_name>
```

ClearPass Policy Manager Certificate Validation for Downloadable User Roles (DUR)

When a ClearPass Policy Manager server is configured as the domain for RADIUS authentication for downloading user roles, in order to validate the ClearPass Policy Manager server certificate, Instant will automatically download the root CA for the HTTPS server from the well-known URI (**http://<clearpass-fqdn>/.well-known/aruba/clearpass/https-root.pem**). The <clearpass-fqdn> is automatically filled with the name that is configured in the radius server configuration as IP address. This means that the FQDN should be entered as the IP Address, otherwise the certificate cannot be validated.

Upon configuring the domain of the ClearPass Policy Manager server for RADIUS authentication along with a username and password, the Instant AP tries to retrieve the CA from the above well-known URI and store it in flash memory.

The following CLI command shows the current ClearPass Policy Manager CA uploaded on the Instant AP:

```
(Instant AP)# show clearpassca
```

The following CLI command shows the ClearPass Policy Manager CA count in the AP checksum:

```
(Instant AP)# show ap checksum
```

The following CLI command clears the ClearPass Policy Manager CA from the Instant AP:

```
(Instant AP)# clear-cert clearpassca
```

Configuring Derivation Rules

Instant allows you to configure role and VLAN derivation-rules. You can configure these rules to assign a user role or a VLAN to the clients connecting to an SSID or a wired profile.

Understanding Role Assignment Rule

When an SSID or a wired profile is created, a default role for the clients connecting to this SSID or wired profile is assigned. You can assign a user role to the clients connecting to an SSID by any of the following methods. The role assigned by some methods may take precedence over the roles assigned by the other methods.

RADIUS VSA Attributes

The user role can be derived from Aruba VSA for RADIUS server authentication. The role derived from an Aruba VSA takes precedence over roles defined by other methods.

MAC-Address Attribute

The first three octets in a MAC address are known as OUI, and are purchased from the IEEE, Incorporated RA. This identifier uniquely identifies a vendor, manufacturer, or other organization (referred to by the IEEE as the “assignee”) globally and effectively reserves a block of each possible type of derivative identifier (such as MAC addresses) for the exclusive use of the assignee.

Instant APs use the OUI part of a MAC address to identify the device manufacturer and can be configured to assign a desired role for users who have completed 802.1X authentication and MAC authentication. The user role can be derived from the user attributes after a client associates with an Instant AP. You can configure rules to assign a user role to clients that match a MAC-address-based criteria. For example, you can assign a voice role to any client with a MAC address starting with a0:a1:a2.

Roles Based on Client Authentication

The user role can be the default user role configured for an authentication method, such as 802.1X authentication. For each authentication method, you can configure a default role for the clients who are successfully authenticated using that method.

Understanding Device Identification

The device identification feature allows you to assign a user role or VLAN to a specific device type by identifying a DHCP option and signature for that device. If you create a user role with the **DHCP-Option** rule type, the first two characters in the attribute value must represent the hexadecimal value of the DHCP option that this rule should match with, while the rest of the characters in the attribute value indicate the DHCP signature the rule should match with. To create a rule that matches DHCP option 12 (host name), the first two characters of the in the attribute value must be the hexadecimal value of 12, which is 0C. To create a rule that matches DHCP option 55, the first two characters in the attribute value must be the hexadecimal value of 55, which is 37.

The following table describes some of the DHCP options that are useful for assigning a user role or VLAN:

Table 122: *DHCP Option Values*

DHCP Option	Description	Decimal Value	Hexadecimal Value
Hostname	The name of the client device.	12	0C
Parameter Request List	The configuration values requested by the client.	55	37
Vendor Class Identifier	Vendors use the option to convey configuration information about the client to the Server.	60	3C
Client Identifier	Clients use this option to uniquely identify themselves and value corresponds to the MAC address of client.	61	3D
Client FQDN	The FQDN name of the client with the domain name.	81	51

DHCP Option and DHCP Fingerprinting

The DHCP fingerprinting allows you to identify the operating system of a device by looking at the options in the DHCP frame. Based on the operating system type, a role can be assigned to the device.

For example, to create a role assignment rule with the DHCP option, select **equals** from the **Operator** drop-down list and enter 370103060F77FC in the **String** text box. Since 370103060F77FC is the fingerprint for Apple iOS devices such as iPad and iPhone, Instant AP assigns Apple iOS devices to the role that you choose.

Table 123: *Validated DHCP Fingerprint*

Device	DHCP Option	DHCP Fingerprint
Apple iOS	Option 55	370103060F77FC
Android	Option 60	3C64686370636420342E302E3135
Blackberry	Option 60	3C426C61636B4265727279
Windows 7/Vista Desktop	Option 55	37010f03062c2e2f1f2179f92b
Windows XP (SP3, Home, Professional)	Option 55	37010f03062c2e2f1f21f92b
Windows Mobile	Option 60	3c4d6963726f736f66742057696e646f777320434500
Windows 7 Phone	Option 55	370103060f2c2e2f
Apple Mac OS X	Option 55	370103060f775ffc2c2e2f

Creating a Role Derivation Rule

You can configure rules for determining the role that is assigned for each authenticated client.



When creating more than one role assignment rule, the first matching rule in the rule list is applied.

The following procedure describes how to create a role assignment rule using the WebUI:

Table 124: *Creating a Role Assignment*

New WebUI	Old WebUI
1. Navigate to the WLAN wizard or the Wired settings window: ▪ Go to **Configuration** > **Networks**. To modify an existing network profile, select the profile and click **Edit**. To create a new network, click **+**. 2. Select the **Access** tab. 3. Select **Role-based** in the **Access Rules** drop-down list. 4. Under **Role Assignment Rules**, click **+**. The **New Role Assignment** window allows you to define a match method by which the string in *Operand* is matched with the attribute value returned by the authentication server. 5. Select the attribute that matches with the rule from the **Attribute** drop-down list. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options. For For more information on a list of RADIUS attributes, see RADIUS Server Authentication with VSA on page 226. 6. Select the operator from the **Operator** drop-down list. The following types of operators are supported: ▪ **contains**—The rule is applied only if the attribute value contains the string specified in *Operand*. ▪ **Is the role**—The rule is applied if the attribute value is the role. ▪ **equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*. ▪ **not-equals**—The rule is applied only if the attribute value is not equal to the string specified in *Operand*. ▪ **starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*. ▪ **ends-with**—The rule is applied only if the attribute value ends with the string	1. Navigate to the WLAN wizard or the Wired settings window: ▪ To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile. ▪ To configure access rules for a wired profile, go to **More** > **Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile. 2. Click the **Access** tab. 3. Under **Role Assignment Rules**, click **New**. The **New Role Assignment** window allows you to define a match method by which the string in *Operand* is matched with the attribute value returned by the authentication server. 4. Select the attribute that matches with the rule from the **Attribute** drop-down list. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options. For information on a list of RADIUS attributes, see RADIUS Server Authentication with VSA on page 226. 5. Select the operator from the **Operator** drop-down list. The following types of operators are supported: ▪ **contains**—The rule is applied only if the attribute value contains the string specified in *Operand*. ▪ **Is the role**—The rule is applied if the attribute value is the role. ▪ **equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*. ▪ **not-equals**—The rule is applied only if the attribute value is not equal to the string specified in *Operand*. ▪ **starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*.

New WebUI	Old WebUI
specified in *Operand*. ▪ **matches-regular-expression**—The rule is applied only if the attribute value matches the Regex pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** drop-down list. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for the WLAN clients. 7. The following types of operators are supported: ▪ **contains**—The rule is applied only if the attribute value contains the string specified in *Operand*. ▪ **Is the role**—The rule is applied if the attribute value is the role. ▪ **equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*. ▪ **not-equals**—The rule is applied only if the attribute value is not equal to the string specified in *Operand*. ▪ **starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*. ▪ **ends-with**—The rule is applied only if the attribute value ends with the string specified in *Operand*. ▪ **matches-regular-expression**—The rule is applied only if the attribute value matches the Regex pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** drop-down list. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for the WLAN clients. 8. Enter the string to match the attribute in the **String** text box. 9. Select the appropriate role from the **Role** drop-down list. 10. Click **OK**.	▪ **ends-with**—The rule is applied only if the attribute value ends with the string specified in *Operand*. ▪ **matches-regular-expression**—The rule is applied only if the attribute value matches the Regex pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** drop-down list. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for the WLAN clients. 6. Enter the string to match the attribute in the **String** text box. 7. Select the appropriate role from the **Role** drop-down list. 8. Click **OK**. 9. Click **Finish**.

New WebUI	Old WebUI
11. Click **Finish**.	

NOTE:

- When **Enforce Machine Authentication** is enabled, both the device and the user must be authenticated for the role assignment rule to apply.
- Each device type may not have a unique DHCP fingerprint signature. For example, devices from different manufacturers may use vendor class identifiers that begin with similar strings. If you create a DHCPOption rule that uses the **starts-with** condition instead of the **equals** condition, the rule may assign a role or VLAN to more than one device type.

The following CLI commands configure role assignment rules for a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role <attribute>{{equals|not-equals|starts-
with|ends-with|contains|matches-regular-expression} <operator><role>|value-of}
```

The following CLI commands configure role assignment rules for a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(wired ap profile <name>)# set-role <attribute>{{equals|not-equal|starts-
with|  ends-with|contains}<operator> <role>|value-of}
```

Example

```
(Instant AP)(config)# wlan ssid-profile Profile1
(Instant AP)(SSID Profile "Profile1")# set-role mac-address-and-dhcp-options matches-
regular-expression \bring\b Profile1
```

Understanding VLAN Assignment

You can assign VLANs to a client based on the following configuration conditions:

- The default VLAN configured for the WLAN can be assigned to a client.
- If VLANs are configured for a WLAN SSID or an Ethernet port profile, the VLAN for the client can be derived before the authentication, from the rules configured for these profiles.
- If a rule derives a specific VLAN, it is prioritized over the user roles that may have a VLAN configured.
- The user VLANs can be derived from the default roles configured for 802.1X authentication or MAC authentication.
- After client authentication, the VLAN can be derived from VSA for RADIUS server authentication.
- The DHCP-based VLANs can be derived for captive portal authentication.
- After client authentication, the VLAN can be derived from Microsoft Tunnel attributes (Tunnel-Type, Tunnel Medium Type, and Tunnel Private Group ID). All three attributes must be present as shown below. This does not require a server-derived rule. For example:

  ```
  Tunnel-Type="VLAN"(13)
  Tunnel-Medium-Type="IEEE-802" (6)
  Tunnel-Private-Group-Id="101"
  ```

NOTE

Instant supports role derivation based on the DHCP option for captive portal authentication. When the captive portal authentication is successful, the role derivation based on the DHCP option assigns a new user role to the guest users, instead of the pre-authenticated role.

VSA

When an external RADIUS server is used, the user VLAN can be derived from the **Aruba-User-Vlan** VSA. The VSA is then carried in an *Access-Accept* packet from the RADIUS server. The Instant AP can analyze the return message and derive the value of the VLAN which it assigns to the user.

Figure 5 *RADIUS Access-Accept Packets with VSA*

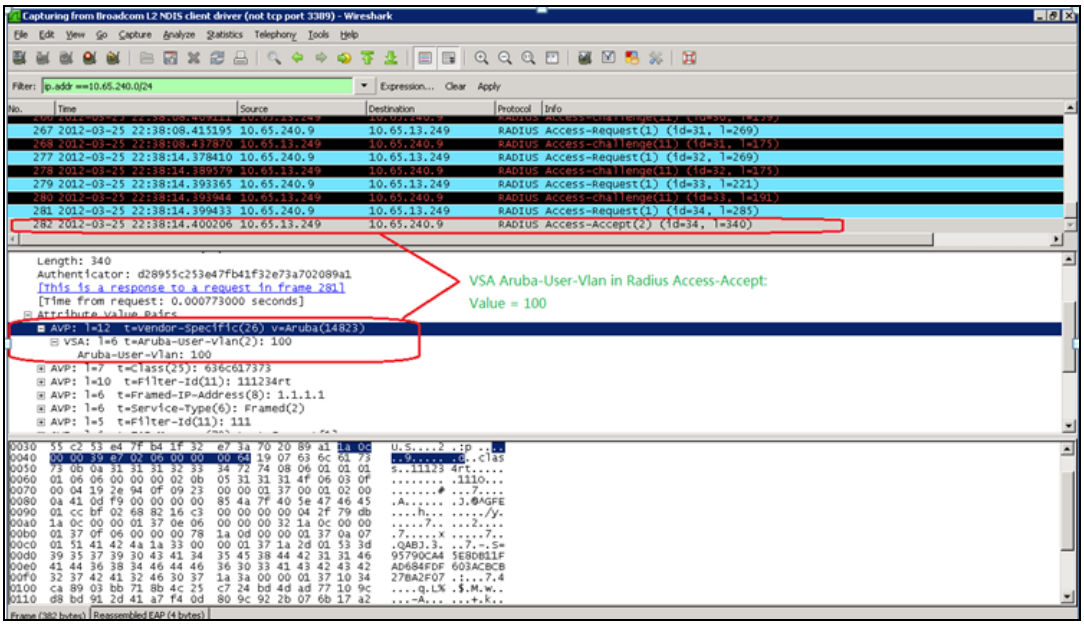
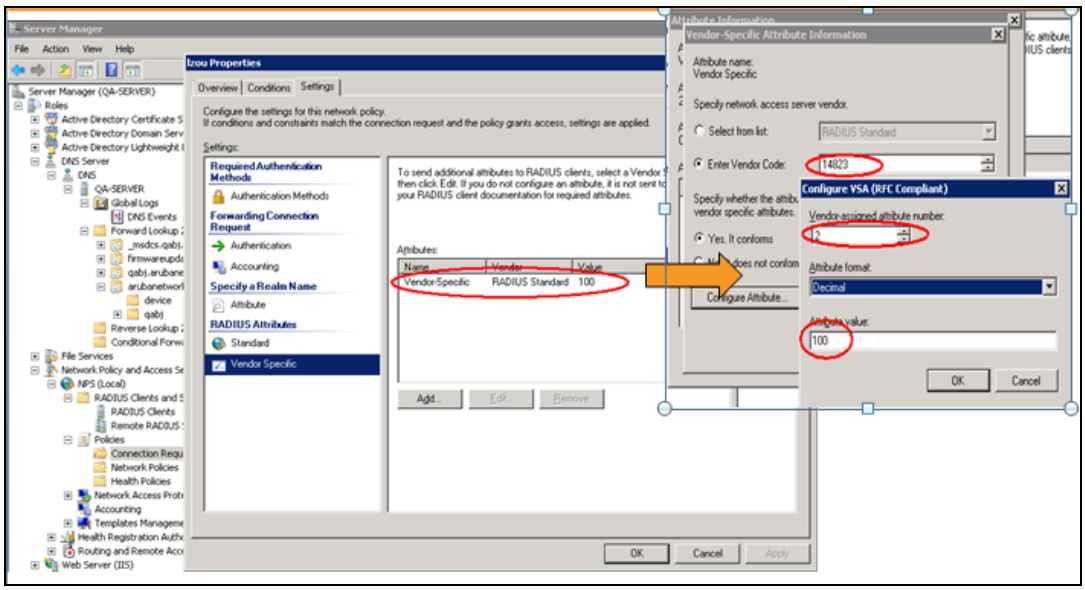


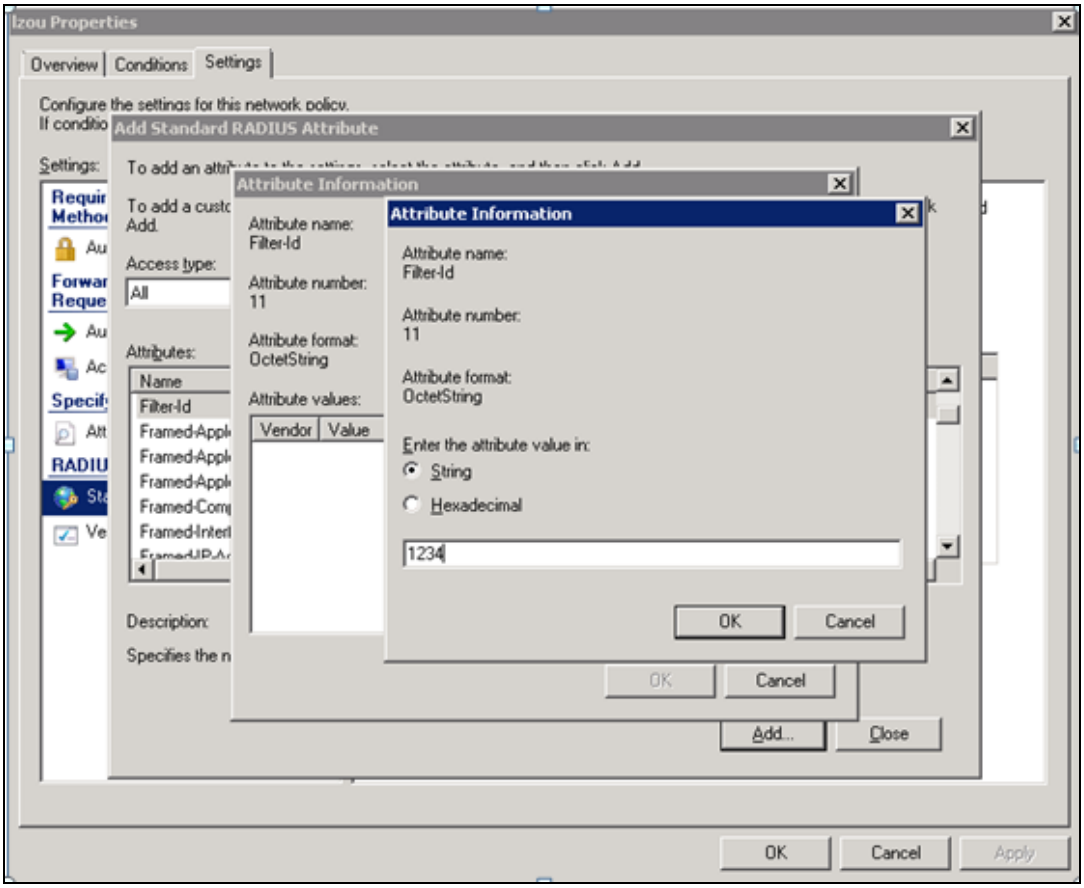
Figure 6 *Configure VSA on a RADIUS Server*



VLAN Assignment Based on Derivation Rules

When an external RADIUS server is used for authentication, the RADIUS server may return a reply message for authentication. If the RADIUS server supports return attributes, and sets an attribute value to the reply message, the Instant AP can analyze the return message and match attributes with a user pre-defined VLAN derivation rule. If the rule is matched, the VLAN value defined by the rule is assigned to the user. For a complete list of RADIUS server attributes, see RADIUS Server Authentication with VSA on page 226.

Figure 7 *Configuring RADIUS Attributes on the RADIUS Server*



User Role

If the VSA and VLAN derivation rules are not matching, then the user VLAN can be derived by a user role.

VLANs Created for an SSID

If the VSA and VLAN derivation rules are not matching, and the User Role does not contain a VLAN, the user VLAN can be derived by VLANs configured for an SSID or an Ethernet port profile.

Configuring VLAN Derivation Rules

The VLAN derivation rules allow administrators to assign a VLAN to the Instant AP clients based on the attributes returned by the RADIUS server.

The following procedure describes how to configure VLAN derivation rules for an SSID profile by using the WebUI:

Table 125: *Configuring Destination NAT Access Rule*

New WebUI	Old WebUI
1. To configure VLAN derivation rule for a WLAN SSID profile or a Wired network, navigate to **Configuration** > **Networks**. ■ To create a new network, click **+**. ■ To edit an existing network, select the profile and click **Edit**. 2. Select the **VLAN** tab. a. Set **Client IP assignment** to **Network assigned**. b. Select the **Dynamic** radio button under **Client VLAN assignment**. This step is applicable only to WLAN profiles. 3. Under **VLAN Assignment Rules**, click **+** to create a VLAN assignment rule. The **New VLAN Assignment Rule** window is displayed. In this window, you can define a match method by which the string in *Operand* is matched with the attribute values returned by the authentication server. 4. Select the attribute from the **Attribute** drop-down list. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options. For information on a list of RADIUS attributes, see RADIUS Server Authentication with VSA on page 226. 5. Select the operator from the **Operator** drop-down list. The following types of operators are supported: ■ **contains**—The rule is applied only if the attribute value contains the string specified in *Operand*. ■ **Is the VLAN**—The rule is applied if the VLAN is the same as the one returned by the RADIUS attribute. ■ **equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*. ■ **not-equals**—The rule is applied only if the attribute value is not equal to the string specified in *Operand*.	1. To configure VLAN derivation rule for a WLAN SSID profile, navigate to **Network > New > New WLAN > VLAN** or **Network > edit > Edit <WLAN-profile> > VLAN**. Select the **Dynamic** radio button under **Client VLAN assignment**. The **Dynamic** radio button is visible only when the **Client IP assignment** is set to **Network assigned**. 2. To configure VLAN derivation rule for a wired network profile, navigate to **Wired > New > New Wired Network > VLAN** or **Wired > Edit > Edit Wired Network > VLAN**. The **VLAN** tab contents are displayed. 3. Under **VLAN Assignment Rules**, click **New** to create a VLAN assignment rule. The **New VLAN Assignment Rule** window is displayed. In this window, you can define a match method by which the string in *Operand* is matched with the attribute values returned by the authentication server. 4. Select the attribute from the **Attribute** drop-down list. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options. For information on a list of RADIUS attributes, see RADIUS Server Authentication with VSA on page 226. 5. Select the operator from the **Operator** drop-down list. The following types of operators are supported: ■ **contains**—The rule is applied only if the attribute value contains the string specified in *Operand*. ■ **Is the VLAN**—The rule is applied if the VLAN is the same as the one returned by the RADIUS attribute. ■ **equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*. ■ **not-equals**—The rule is applied only if the attribute value is not equal to the string specified in *Operand*.

New WebUI	Old WebUI
▪ **starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*. ▪ **ends-with**—The rule is applied only if the attribute value ends with the string specified in *Operand*. 6. Enter the string to match the attribute in the **String** text box. 7. Enter the appropriate VLAN ID in the **VLAN** text box. 8. Click **OK** and then click **Next**. 9. Ensure that the required security and access parameters are configured. 10. Click **Finish** to apply the changes.	▪ **starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*. ▪ **ends-with**—The rule is applied only if the attribute value ends with the string specified in *Operand*. 6. Enter the string to match the attribute in the **String** text box. 7. Select the appropriate VLAN ID from the **VLAN** text box. 8. Click **OK**. 9. Ensure that the required security and access parameters are configured. 10. Click **Finish** to apply the changes.

The following CLI commands create a VLAN assignment rule for a WLAN SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-vlan <attribute>{equals|not-equals|starts-
with|ends-with|contains}<operator><VLAN-ID>|value-of}
```

The following CLI commands configure a VLAN assignment rule for a wired profile:

```
(Instant AP)(config)# wired-port-profile <nname>
(Instant AP)(wired ap profile <name>)# set-vlan <attribute>{equals|not-equals|starts-
with|ends-with|contains}<operator><VLAN-ID>|value-of}
```

Using Advanced Expressions in Role and VLAN Derivation Rules

For complex policies of role and VLAN derivation using device DHCP fingerprints, you can use a Regex to match with the combined string of the MAC address and the DHCP options. The combined string is formed by concatenating the hexadecimal presentation of the MAC address and all of the DHCP options sent by a particular device. The Regex is a powerful pattern description language that can be used to perform advanced pattern matching of the above string.

If the combined device fingerprint string matches the specified Regex, the role or VLAN can be set to the WLAN client.

The following table lists some of the most commonly used Regex, which can be used in user role and user VLAN derivation rules:

Table 126: *Regular Expression*

Operator	Description
.	Matches any character. For example, l..k matches lack, lark, link, lock, look, Lync, and so on.
\	Matches the character that follows the backslash. For example, \192.\.0\.. matches IP address ranges that start with 192.0, such as 192.0.1.1. The expression looks up only for the single characters that match.

Operator	Description
[ ]	Matches any one character listed between the brackets. For example, [bc]lock matches block and clock.
\b	Matches the words that begin and end with the given expression. For example, \bdown matches downlink, linkdown, shutdown.
\B	Matches the middle of a word. For example, \Bvice matches services, devices, serviceID, deviceID, and so on.
^	Matches the characters at starting position in a string. For example, ^bcd matches bcde or bcdf, but not abcd.
[^]	Matches any characters that are not listed between the brackets. For example, [^u]link matches downlink, link, but not uplink.
?	Matches any one occurrence of the pattern. For example, ?est matches best, nest, rest, test, and so on.
$	Matches the end of an input string. For example, eth$ matches Eth, but not Ethernet.
*	Matches the declared element multiple times if it exists. For example, eth* matches all occurrences of eth, such as Eth, Ethernet, Eth0, and so on.
+	Matches the declared element one or more times. For example, aa+ matches occurrences of aa and aaa.
( )	Matches nested characters. For example, (192)* matches any number of the character string 192.
|	Matches the character patterns on either side of the vertical bar. You can use this expression to construct a series of options.
\<	Matches the beginning of the word. For example, \<wire matches wired, wireless, and so on.
\>	Matches the end of the word. For example, \>list matches blacklist, whitelist, and so on.
{n}	Where n is an integer. Matches the declared element exactly n times. For example, {2}link matches uplink, but not downlink.
{n,}	Where n is an integer. Matches the declared element at n times. For example, {2,}ink matches downlink, but not uplink.

For information on how to use a Regex in role and VLAN derivation rules, see the following topics:

- Creating a Role Derivation Rule on page 283
- Configuring VLAN Derivation Rules on page 288

Configuring a User Role for VLAN Derivation

This section describes the following procedures:

- Creating a User VLAN Role on page 291
- Assigning User VLAN Roles to a Network Profile on page 292

Creating a User VLAN Role

The following procedure describes how to create a user role for VLAN derivation using the WebUI:

Table 127: *Creating a User VLAN Rule*

New WebUI	Old WebUI
1. Go to **Configuration** > **Security**. 2. Expand the **Roles** tab. 3. Under **Roles**, click **+**. 4. Enter a name for the new role and click **OK**. 5. Under **Access rules**, click **+**. The **New rule** window is displayed. 6. Select the **Rule type** as **VLAN assignment**. 7. Enter the ID of the VLAN in the **VLAN ID** text box. 8. Click **OK** in the **New rule** window. 9. Click **Save** in the **Roles** tab.	1. Click the **Security** link located directly above the Search bar in the Instant main window. 2. Click the **Roles** tab. The **Roles** tab contents are displayed. 3. Under **Roles**, click **New**. 4. Enter a name for the new role and click **OK**. 5. Under **Access rules**, click **New**. 6. Select the **Rule type** as **VLAN assignment**. 7. Enter the ID of the VLAN in the **VLAN ID** text box. 8. Click **OK** in the **New Rule** window. 9. Click **OK** in the **Roles** tab.

The following CLI commands create a VLAN role:

```
(Instant AP)(config)# wlan access-rule <rule-name>
(Instant AP)(Access Rule <rule-name>)# vlan 200
```

Assigning User VLAN Roles to a Network Profile

The following procedure describes how to configure user VLAN roles for a network profile using the WebUI:

Table 128: *Configuring User VLAN Roles for a Network Profile*

New WebUI	Old WebUI
1. Under **Configuration** > **Networks** , click **+** to create a new WLAN profile or select a network profile to modify and click **Edit**. 2. Select the **Access** tab. 3. Select **Role-based** from the **Access Rules** drop-down list. 4. Click **+** under the **Role Assignment Rules** window. The **New Role Assignment Rule** window is displayed. 5. Configure the following parameters: a. Select the attribute from the **Attribute** drop-down list. b. Select the operator to match attribute from the **Operator** drop-down list. c. Enter the string to match in the **String** text box. d. Select the role to be assigned from the **Role**	1. Click **Networks** > **New** > **New WLAN** > **Access** or click **Network** > **edit** > **Edit <WLAN-profile** > **Access**. 2. On the **Access** tab, ensure that the slider is at the **Role-based** option. 3. Click **New** under the **Role Assignment Rules** window. The **New Role Assignment Rule** window is displayed. 4. Configure the following parameters: a. Select the attribute from the **Attribute** drop-down list. b. Select the operator to match attribute from the **Operator** drop-down list. c. Enter the string to match in the **String** text box. d. Select the role to be assigned from the **Role** text box.

New WebUI	Old WebUI
text box. 6. Click **OK** in the **New Role Assignment Rule** window. 7. Click **Finish**.	5. Click **OK** in the **New Role Assignment Rule** window. 6. Click **Finish** in the **Access** tab.

The following CLI commands assign VLAN role to a WLAN profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role <attribute>{{equals <operator> <role>|not-equals <operator> <role>|starts-with <operator> <role>|ends-with <operator> <role>|contains <operator> <role>}|value-of}
```

Downloadable User Roles

Aruba Instant and ClearPass Policy Manager include support for centralized policy definition and distribution. Aruba Instant now supports downloadable user roles. By using this feature, when ClearPass Policy Manager successfully authenticates a user, the user is assigned a role by ClearPass Policy Manager. If the role is not defined on the Instant AP, the role attributes can also be downloaded automatically.

In order to provide highly granular per-user level access, user roles can be created when a user has been successfully authenticated. During the configuration of a policy enforcement profile in ClearPass Policy Manager, the administrator can define a role that should be assigned to the user after successful authentication. In RADIUS authentication, when ClearPass Policy Manager successfully authenticates a user, the user is assigned a role by ClearPass Policy Manager. If the role is not defined on the Instant AP, the role attributes can also be downloaded automatically. This feature supports roles obtained by the following authentication methods:

- 802.1X (WLAN and wired users)
- MAC authentication
- Captive Portal

Enabling Downloadable User Roles on an Instant AP

The following CLI commands enable role download:

```
(Instant AP)(config)# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile <profile_name>)# download-role
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Verifying the Configuration

The following CLI command checks if role download is enabled on the network profile:

```
(Instant AP)# show network <profile_name>
```

This chapter provides the following information:

- Configuring DHCP Scopes on page 294
- Configuring the Default DHCP Scope for Client IP Assignment on page 309

Configuring DHCP Scopes

The virtual controller supports different modes of DHCP address assignment. With each DHCP address assignment mode, various client traffic forwarding modes are associated. For more information on client traffic forwarding modes for IAP-VPN, see IAP-VPN Forwarding Modes on page 333.



When using a local DHCP scope in anInstant AP cluster, ensure that the VLANs configured for this DHCP scope is allowed in the uplink switch.

In a single Instant AP network, when using a client DHCP scope for wired clients, ensure that client VLAN is not added in the allowed VLAN list for the port to which the Instant AP Ethernet 0 port is connected.

This section describes the following procedures:

- In the Old WebUI on page 298
- Configuring Distributed DHCP Scopes on page 298
- Enabling DHCP Relay Agent Information Option (Option 82) on page 303
- Enabling DHCP Relay Agent Information Option (Option 82) on page 303

Configuring Local DHCP Scopes

You can configure Local, Local L2, and Local L3 DHCP scopes through the WebUI or the CLI.

- **Local**—In this mode, the virtual controller acts as both the DHCP server and the default gateway. The configured subnet and the corresponding DHCP scope are independent of the subnets configured in other Instant AP clusters. The virtual controller assigns an IP address from a local subnet and forwards traffic to both **corporate** and **non-corporate** destinations. The network address is translated appropriately and the packet is forwarded through the IPsec tunnel or through the uplink. This DHCP assignment mode is used in the NAT forwarding mode.
- **Local, L2**—In this mode, the virtual controller acts as a DHCP server and the gateway located outside the Instant AP.
- **Local, L3**—This DHCP assignment mode is used with the L3 forwarding mode. In this mode, the virtual controller acts as a DHCP server and the gateway, and assigns an IP address from the local subnet. The Instant AP routes the packets sent by clients on its uplink. The Local L3 subnets can access corporate network through the IPsec tunnel. The network address for all client traffic, which is generated in the Local L3 subnets and destined to the corporate network, is translated at the source

with the tunnel inner IP. However, if corporate access to Local L3 is not required, you can configure ACL rules to deny access.

In the Old WebUI

To configure a Local or a Local L3 DHCP scope:

1. Click **More** > **DHCP Server**. The **DHCP Servers** window is displayed.
2. To configure a **Local**, **Local, L2**, or **Local, L3** DHCP scope, click **New** under **Local DHCP Scopes**. The **New DHCP Scope** window is displayed.
3. Based on the type of DHCP scope selected, configure the following parameters:

Table 129: *Local DHCP Mode Configuration Parameters*

Parameter	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: ■ **Local**—On selecting **Local**, the DHCP server for local branch network is used for keeping the scope of the subnet local to the Instant AP. In the NAT mode, the traffic is forwarded through the IPsec tunnel or the uplink. ■ **Local, L2**—On selecting **Local, L2**, the virtual controller acts as a DHCP server and a default gateway in the local network that is used. ■ **Local, L3**—On selecting **Local, L3**, the virtual controller acts as a DHCP server and a gateway. In this mode, the network address for traffic destined to the corporate network is translated at the source with the inner IP of the IPsec tunnel and is forwarded through the IPsec tunnel. The traffic destined to the non-corporate network is routed.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile on page 136 and Configuring VLAN for a Wired Profile on page 163.
Network	Specify the network to use.
Netmask	If **Local**, **Local, L2**, or **Local, L3** is selected, specify the subnet mask. The subnet mask and the network determine the size of the subnet.
Excluded address	Specify a range of IP addresses to exclude. You can add up to two exclusion ranges. Based on the size of the subnet and the value configured for **Excluded address**, the IP addresses either before or after the defined range are excluded.
Default Router	If **Local, L2** is selected for type of DHCP scope, specify the IP address of the default router.
DNS Server	If required, specify the IP address of a DNS server for the **Local**; **Local, L2**; and **Local, L3** scopes. You can configure up to 4 DNS servers for each DHCP scope.

Table 129: *Local DHCP Mode Configuration Parameters*

Parameter	Description
Domain Name	If required, specify the domain name for the **Local**; **Local, L2**; and **Local, L3** scopes.
Lease Time	Specify a lease time for the client in minutes within a range of 2–1440 minutes. The default value is 720 minutes.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, and 161. Click **+** to add multiple DHCP options.

4. Click **OK**.
5. Click **OK** in the **DHCP Servers** window.

In the New WebUI

To configure a Local or a Local L3 DHCP scope:

1. Click **Configuration** > **DHCP Server**. The **DHCP Servers** window is displayed.
2. To configure a **Local**, **Local,L2**, or **Local,L3** DHCP scope, click **+** under **Local DHCP Scopes**.
3. Based on the type of DHCP scope selected, configure the following parameters:

Table 130: *Local DHCP Mode Configuration Parameters*

Parameter	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: ■ **Local**—On selecting **Local**, the DHCP server for local branch network is used for keeping the scope of the subnet local to the Instant AP. In the NAT mode, the traffic is forwarded through the IPsec tunnel or the uplink. ■ **Local,L2**—On selecting **Local,L2**, the virtual controller acts as a DHCP server and a default gateway in the local network that is used. ■ **Local,L3**—On selecting **Local,L3**, the virtual controller acts as a DHCP server and a gateway. In this mode, the network address for traffic destined to the corporate network is translated at the source with the inner IP of the IPsec tunnel and is forwarded through the IPsec tunnel. The traffic destined to the non-corporate network is routed.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile on page 136 and Configuring VLAN for a Wired Profile on page 163.
Network	Specify the network to use.
Netmask	If **Local**, **Local, L2**, or **Local, L3** is selected, specify the subnet mask. The subnet mask and the network determine the size of the subnet.

Table 130: *Local DHCP Mode Configuration Parameters*

Parameter	Description
Excluded address	Specify a range of IP addresses to exclude. You can add up to two exclusion ranges. Based on the size of the subnet and the value configured for **Excluded address**, the IP addresses either before or after the defined range are excluded.
Default router	If **Local, L2** is selected for type of DHCP scope, specify the IP address of the default router.
DNS server	If required, specify the IP address of a DNS server for the **Local**; **Local, L2**; and **Local, L3** scopes. You can configure up to 4 DNS servers for each DHCP scope.
Domain name	If required, specify the domain name for the **Local**; **Local, L2**; and **Local, L3** scopes.
Lease time	Specify a lease time for the client in minutes within a range of 2–1440 minutes. The default value is 720 minutes.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, and 161. Click **+** to add multiple DHCP options.

4. Click **OK**.
5. Click **Save** in the **DHCP Servers** window.

In the CLI

To configure a Local DHCP scope:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# server-type <local>
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP)(DHCP Profile <profile-name>)# subnet <IP-address>
(Instant AP)(DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(Instant AP)(DHCP Profile <profile-name>)# dns-server <dns_server>
(Instant AP)(DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant AP)(DHCP Profile <profile-name>)# lease-time <seconds>
(Instant AP)(DHCP Profile <profile-name>)# option <type> <value>
```

To configure a Local L2 DHCP scope:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# server-type <local,l2>
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP)(DHCP Profile <profile-name>)# subnet <IP-address>
(Instant AP)(DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(Instant AP)(DHCP Profile <profile-name>)# exclude-address <IP-address>
(Instant AP)(DHCP Profile <profile-name>)# default-router
(Instant AP)(DHCP Profile <profile-name>)# dns-server <dns_server>
(Instant AP)(DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant AP)(DHCP Profile <profile-name>)# lease-time <seconds>
(Instant AP)(DHCP Profile <profile-name>)# option <type> <value>
```

To configure a Local L3 DHCP scope:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# server-type <local,l3>
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
```

```
(Instant AP)(DHCP Profile <profile-name>)# subnet <IP-address>
(Instant AP)(DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(Instant AP)(DHCP Profile <profile-name>)# exclude-address <IP-address>
(Instant AP)(DHCP Profile <profile-name>)# dns-server <dns_server>
(Instant AP)(DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant AP)(DHCP Profile <profile-name>)# lease-time <seconds>
(Instant AP)(DHCP Profile <profile-name>)# option <type> <value>
```

VLAN and Default Router Settings

Instant supports DHCP scopes in which both, the DHCP server and the default gateway on a virtual controller can configure a default gateway IP address. For the Centralized, L3, Local, Local, L2, and Local, L3 scopes, an option is introduced to configure a VLAN IP address to the existing service VLAN of a DHCP pool. This feature can prevent changes that may occur in DHCP range exclusions.

You can configure a local DHCP profile by using the WebUI or CLI.

To configure a default router and VLAN parameters in a local DHCP profile:

1. Click **More** > **DHCP Server**. The **DHCP Servers** window is displayed.
2. To configure a local DHCP scope, click **New** under **Local DHCP Scopes**. The **New DHCP Scope** window is displayed.
3. Select the **Type** and configure the parameters available in the WebUI. The **Default router** parameter can be set on Local and Local L3 profiles. The **VLAN IP** and **Netmask** parameters can be set only on the Local L2 profile.
4. Click **OK**.

To configure a default router and VLAN parameters in a local DHCP profile:

1. Click **Configuration** > **DHCP Server**. The **DHCP Servers** window is displayed.
2. To configure a local DHCP scope, click **+** under **Local DHCP Scopes**. The **New DHCP Scope** window is displayed.
3. Select the **Type** and configure the parameters available in the WebUI. The **Default router** parameter can be set on Local and Local L3 profiles. The **VLAN IP** and **VLAN mask** parameters can be set only on the Local L2 profile.
4. Click **OK**.

To configure VLAN IP in a Local DHCP profile:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# vlan-ip <VLAN_IP> mask <VLAN mask>
```

To configure a default router in a Local DHCP profile:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# default-router <default_router>
```

The value of the VLAN IP and default router for the Local or Local, L3 profile must be the same.

Configuring Distributed DHCP Scopes

Instant allows you to configure the DHCP address assignment for the branches connected to the corporate network through VPN. You can configure the range of DHCP IP addresses used in the branches and the number of client addresses allowed per branch. You can also specify the IP addresses that must be excluded from those assigned to clients, so that they are assigned statically.

Instant supports the following distributed DHCP scopes:

- **Distributed, L2**—In this mode, the virtual controller acts as the DHCP server, but the default gateway is in the data center. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the virtual controller controls a scope that is a subset of the complete IP address range for the subnet distributed across all the branches. This DHCP assignment mode is used with the L2 forwarding mode.
- **Distributed, L3**—In this mode, the virtual controller acts as the DHCP server and the default gateway. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the virtual controller is configured with a unique subnet and a corresponding scope.

In the Old WebUI

To configure distributed DHCP scopes such as Distributed L2 or Distributed L3:

1. Click **More** > **DHCP Server**. The **DHCP Servers** window is displayed.
2. To configure a distributed DHCP mode, click **New** under **Distributed DHCP Scopes**. The **New DHCP Scope** window is displayed.
3. Based on the type of distributed DHCP scope, configure the following parameters in the **Network** tab:

Table 131: *Distributed DHCP Mode Configuration Parameters*

Parameter	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: ▪ **Distributed, L2**—On selecting **Distributed, L2**, the virtual controller acts as the DHCP server but the default gateway is in the data center. Traffic is bridged into VPN tunnel. ▪ **Distributed, L3**—On selecting **Distributed, L3**, the virtual controller acts as both DHCP server and default gateway. Traffic is routed into the VPN tunnel.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile on page 136 and Configuring VLAN for a Wired Profile on page 163.
Netmask	If **Distributed, L2** is selected for the type of DHCP scope, specify the subnet mask. The subnet mask and the network determine the size of subnet.
Default router	If **Distributed, L2** is selected for the type of DHCP scope, specify the IP address of the default router.

Table 131: *Distributed DHCP Mode Configuration Parameters*

Parameter	Description
DNS server	If required, specify the IP address of a DNS server. You can configure upto four DNS servers at the same time. Use commas to separate the DNS servers.
Domain name	If required, specify the domain name.
Lease time	Specify a lease time for the client in minutes within a range of 2–1440 minutes. The default value is 720 minutes.
Dynamic DNS	Select the **Dynamic DNS** check box to enable dynamic DNS on the Distributed L3 client. **Key**—Enter the TSIG shared secret key.
IP Address Range	Specify a range of IP addresses to use. Click **+** to add another range. You can specify up to four different ranges of IP addresses. For the **Distributed, L2** mode, ensure that all IP ranges are in the same subnet as the default router. On specifying the IP address ranges, a subnet validation is performed to ensure that the specified ranges of IP address are in the same subnet as the default router and subnet mask. The configured IP range is divided into blocks based on the configured client count. For the **Distributed, L3** mode, you can configure any discontiguous IP ranges. The configured IP range is divided into multiple IP subnets that are sufficient to accommodate the configured client count. You can allocate multiple branch IDs per subnet. The Instant AP generates a subnet name from the DHCP IP configuration, which the controller can use as a subnet identifier. If static subnets are configured in each branch, all of them are assigned the with branch ID 0, which is mapped directly to the configured static subnet.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, 161, and so on. Click **+** to add multiple DHCP options. You can add up to eight DHCP options.

4. Click **Next**.
5. In the **Branch Size** tab, specify the number of clients to use per branch in the **Clients per branch** text box. The client count configured for a branch determines the use of IP addresses from the IP address range defined for a DHCP scope. For example, if 20 IP addresses are available in an IP address range configured for a DHCP scope and a client count of 9 is configured, only a few IP addresses (in this example, 9) from this range will be used and allocated to a branch. The Instant AP does not allow the administrators to assign the remaining IP addresses to another branch, although a lower value is configured for the client count.
6. Click **Next**. The **Static IP** tab is displayed.
7. In the **Reserve first** and **Reserve last** text boxes, specify the number of first and last IP addresses to reserve in the subnet.
8. Click **Finish**.
9. Click **OK** in the **DHCP Servers** window.

In the New WebUI

To configure distributed DHCP scopes such as Distributed L2 or Distributed L3:

1. Click **Configuration** > **DHCP Server**. The **DHCP Servers** window is displayed.
2. To configure a distributed DHCP mode, click **+** under **Distributed DHCP Scopes**. The **New DHCP Scope** window is displayed.
3. Based on the type of distributed DHCP scope, configure the following parameters in the **Network** tab:

Table 132: *Distributed DHCP Mode Configuration Parameters*

Parameter	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: ▪ **Distributed, L2**—On selecting **Distributed, L2**, the virtual controller acts as the DHCP server but the default gateway is in the data center. Traffic is bridged into VPN tunnel. ▪ **Distributed, L3**—On selecting **Distributed, L3**, the virtual controller acts as both DHCP server and default gateway. Traffic is routed into the VPN tunnel.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile on page 136 and Configuring VLAN for a Wired Profile on page 163.
Netmask	If **Distributed, L2** is selected for the type of DHCP scope, specify the subnet mask. The subnet mask and the network determine the size of subnet.
Default router	If **Distributed, L2** is selected for the type of DHCP scope, specify the IP address of the default router.
DNS server	If required, specify the IP address of a DNS server. You can configure up to four DNS servers at the same time. Use commas to separate the DNS servers.
Domain name	If required, specify the domain name.
Lease time	Specify a lease time for the client in minutes within a range of 2–1440 minutes. The default value is 720 minutes.
Dynamic DNS	Click the **Dynamic DNS** toggle switch to enable dynamic DNS on the Distributed L3 client. **Key**—Enter the TSIG shared secret key.
IP Address Range	Specify a range of IP addresses to use. Click **+** to add another range. You can specify up to four different ranges of IP addresses. For the **Distributed, L2** mode, ensure that all IP ranges are in the same subnet as the default router. On specifying the IP address ranges, a subnet validation is performed to ensure that the specified ranges of IP address are in the same subnet as the default router and subnet mask. The configured IP range is divided into blocks based on the configured client count. For the **Distributed, L3** mode, you can configure any discontiguous IP ranges. The configured IP range is divided into multiple IP subnets that are sufficient to accommodate the configured client count.

Table 132: *Distributed DHCP Mode Configuration Parameters*

Parameter	Description
	You can allocate multiple branch IDs per subnet. The Instant AP generates a subnet name from the DHCP IP configuration, which the controller can use as a subnet identifier. If static subnets are configured in each branch, all of them are assigned the with branch ID 0, which is mapped directly to the configured static subnet.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, 161, and so on. Click **+** to add multiple DHCP options. You can add up to eight DHCP options.

4. Click **Next**.
5. In the **Branch Size** tab, specify the number of clients to use per branch in the **Clients per branch** text box. The client count configured for a branch determines the use of IP addresses from the IP address range defined for a DHCP scope. For example, if 20 IP addresses are available in an IP address range configured for a DHCP scope and a client count of 9 is configured, only a few IP addresses (in this example, 9) from this range will be used and allocated to a branch. The Instant AP does not allow the administrators to assign the remaining IP addresses to another branch, although a lower value is configured for the client count.
6. Click **Next**. The **Static IP** tab is displayed.
7. In the **Reserve first** and **Reserve last** text boxes, specify the number of first and last IP addresses to reserve in the subnet.
8. Click **Finish**.
9. Click **Save** in the **DHCP Servers** window.

In the CLI

To configure a Distributed L2 DHCP scope:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# ip dhcp server-type <Distributed,L2>
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP)(DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(Instant AP)(DHCP Profile <profile-name>)# default-router <IP-address>
(Instant AP)(DHCP Profile <profile-name>)# client-count <number>
(Instant AP)(DHCP Profile <profile-name>)# dns-server <name>
(Instant AP)(DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant AP)(DHCP Profile <profile-name>)# lease-time <seconds>
(Instant AP)(DHCP Profile <profile-name>)# ip-range <start-IP> <end-IP>
(Instant AP)(DHCP Profile <profile-name>)# reserve {first|last} <count>
(Instant AP)(DHCP Profile <profile-name>)# option <type> <value>
```

To configure a Distributed L3 DHCP scope:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# ip dhcp server-type <Distributed,L3>
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP)(DHCP Profile <profile-name>)# client-count <number>
(Instant AP)(DHCP Profile <profile-name>)# dns-server <name>
(Instant AP)(DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant AP)(DHCP Profile <profile-name>)# lease-time <seconds>
(Instant AP)(DHCP Profile <profile-name>)# dynamic-dns [key <TSIG KEY>]
(Instant AP)(DHCP Profile <profile-name>)# ip-range <start-IP> <end-IP>
(Instant AP)(DHCP Profile <profile-name>)# reserve {first|last} <count>
(Instant AP)(DHCP Profile <profile-name>)# option <type> <value>
```

Enabling DHCP Relay Agent Information Option (Option 82)

The DHCP Relay Agent Information option (Option 82) allows the DHCP Relay Agent to insert circuit specific information into a request that is being forwarded to a DHCP server.

The master Instant AP, when acting as a DHCP relay agent, inserts information about the slave Instant AP and SSID through which a client connects to the DHCP request. Many service providers use this mechanism to make access control decisions.

Option 82 can be customized to cater to the requirements of any ISP using the master Instant AP. To facilitate customization using a XML definition, multiple parameters for Circuit ID and Remote ID options of DHCP Option 82 have been introduced. The XML file is used as the input from the user and is validated against an XSD file in the master Instant AP. The format in the XML file is parsed and stored in the DHCP relay which is used to insert Option 82 related values in the DHCP request packets sent from the client to the server.

When IP Helper is enabled on an L3 interface, DHCP discover broadcast is filtered at the datapath level and is unicast to the configured helper device.



DHCP Option-82 is supported only for IPv4.

DHCP Option-82 on L2 VLAN can be enabled without the helper address.

Sample XML Format

The following is a sample XML file which specifies DHCP Option-82 circuit and remote IDs.

```
<?xml version="1.0" encoding="UTF-8"?>
<dhcpopt82>
  <circuit_id>
    <param>
      <type>var</type>
        <val>apmac</val>
        <delim>-</delim>
    </param>
   </circuit_id>
   <remote_id>
    <param>
     <type>var</type>
       <val>uemac</val>
       <delim>:</delim>
     </param>
   </remote_id>
</dhcpopt82>
```

The table below lists the elements introduced in the **param** sub-options of the **Circuit ID** and **Remote ID** fields:

XML File Parameters

Parameter	Description
Type	Listed below are the types available: ■ var–A DHCP option-82 allowed keyword ■ hex–A hexadecimal string with a maximum of 64 characters ■ str–An ASCII string with a maximum of 64 characters

Parameter	Description
Val	This field contains either a hexadecimal string or ASCII string limited to 64 characters, if the type is hex or str. If the type is var then one of the following DHCP option-82 keywords: ■ **apname/APNAME**–AP name ■ **apgrpname/APGRPNAME**–AP group name (zone name) ■ **apmac/APMAC**–AP MAC ■ **ssidt/SSIDT**–SSID Type ■ **bssid/BSSID**–BSSID of AP ■ **uemac/UEMAC**–User MAC (Client)
Delim	The **delim** option is available only for mac based keywords - **apmac/APMAC**, **uemac/UEMAC**, and **bssid/BSSID**. The delim field is used if MAC addresses are required to be in ASCII format with octets separated with either a colon (:) or a hyphen (-). By default, the ASCII MAC separated by a delimiter, will be in lower case. If the user wants to use upper case then the respective MAC-based val keywords must be written in upper case in XML file. For example: ■ <param> ■ <type>var</type> ■ <val>UEMAC</val> ■ <delim>:</delim> ■ </param> If the **delim** field is not present in MAC-based keywords, then the MAC addresses are sent in option82 in hexadecimal format. For example: ■ <param> ■ <type>var</type> ■ <val>apmac</val> (sent in hex format) ■ </param>

Configuring XML Based DHCP Option 82 Specification

Listed below is the sequence of steps to be followed if a user wants to use XML based DHCP option 82:

1. From the master Instant AP, upload the XML file containing Option 82 specification to flash using the **download-dhcpopt82 xml <URL>** command. For example:

   If the XML file is not in the specified format, then the incorrect file will not be loaded to flash. This can be checked using the **show dhcp opt82 xml-config** command, where the load status will be set to **Success** or **Fail**. If the load fails, the error is displayed in the output of the **show dhcp opt82 xml-config** command.

   ```
   (Instant AP) #download-dhcpopt82 xml http://10.20.52.131/dhcp_option82_1.xml
   ```

2. In the configuration terminal, execute the following command:

   ```
   (Instant AP)(config) #dhcp option82-xml <mydhcpoption82.xml>
   ```

   The XML file is always saved in flash with the name **mydhcpoption82.xml**. For example:

   ```
   (Instant AP)(config) # dhcp option82-xml mydhcpoption82.xml
   ```

You can see the parameters configured for Option 82 by executing the **show dhcp opt82 xml-config** command.



This command is not successful if the **option82 alu** parameter is enabled in any of the centralized L2 or L3 DHCP profiles. If **option82 alu** is enabled, then disable it in the respective DHCP profile using the **no option82** parameter.

3. After the **dhcp option82-xml mydhcpoption82.xml** command is executed, then execute the **dhcp option82 xml** command in a centralized L2 or L3 DHCP profile configuration to apply the **option82 xml** configuration to the DHCP packets that need to be relayed from that centralized L2 or L3 DHCP profile.

   For example:

```
(Instant AP)(config) # ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# server-type <centralized>
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP)(DHCP Profile <profile-name>) # option82 xml
```

4. Execute the following command if the user wants to remove global option82 configuration:

```
(Instant AP)(config)# no dhcp option82-xml
```



This command is not successful if there is a DHCP profile configured with the **option82 xml** parameter. To remove the **option82 xml** configuration, go to the respective DHCP profile and execute the **no option82** command, and then execute the **no dhcp option82-xml** command.

If there are multiple centralized L2 or L3 DHCP profiles configured, each profile can have only one type of Option 82 configured at the same time. For example, no two or more profiles can have **option82 xml** and **option82 alu** enabled at the same time.

Configuring ALU Based DHCP Option 82 Specification

1. The Alcatel based DHCP Option 82 configuration in a DHCP profile is similar to the XML-based configuration.

   For example:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# server-type <centralized>
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP)(DHCP Profile <profile-name>)# option82 alu
```

   Before you configure the **option82 alu** parameter in any of the centralized L2 or L3 DHCP profiles, ensure that no other DHCP profile is configured with **option82 xml**, from the specific DHCP profile. Disable it using the **no option82** command and enure that the global XML configuration is not enabled. Now, disable it using the **no dhcp option82-xml** command in configuration mode.

2. To remove ALU based Option 82 configuration , execute the **no option82** command from the specific DHCP profile.

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# no option82
```

Configuring Centralized DHCP Scopes

When a centralized DHCP scope is configured, the following points are to be noted:

- The virtual controller does not assign an IP address to the client and the DHCP traffic is directly forwarded to the DHCP server.
- For Centralized L2 clients, the virtual controller bridges the DHCP traffic to the controller over the VPN or GRE tunnel. The IP address is obtained from the DHCP server behind the controller serving the VLAN or GRE of the client. This DHCP assignment mode also allows you to add the DHCP option 82 to the DHCP traffic forwarded to the controller. You can configure up to 32 VLAN IDs in a single DHCP profile when split-tunnel is disabled. Totally 192 VLAN IDs can be configured for Centralized, L2 clients, 32 VLAN IDs per Centralized, L2 DHCP scope.
- For Centralized L3 clients, the virtual controller acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located either in the corporate or local network. The Centralized L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

You can configure a centralized DHCP scope through the WebUI or the CLI.

In the Old WebUI

To configure a centralized DHCP scope:

1. Click **More** > **DHCP Server**. The **DHCP Servers** window is displayed.
2. To configure a centralized DHCP scope, click **New** under **Centralized DHCP Scopes**. The **New DHCP Scopes** window is displayed.
3. To configure a centralized profile, select the profile type as **Centralized, L2** or **Centralized, L3** and configure the following parameters.

Table 133: *Centralized DHCP Mode Configuration Parameters*

Parameter	Description
Name	Enter a name for the DHCP scope.
Type	Set the type as follows: ■ **Centralized, L2** for the Centralized L2 profile ■ **Centralized, L3** for the Centralized L3 profile
VLAN	Specify a VLAN ID. You can specify up to 32 VLAN IDs for Centralized, L2. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile on page 136 and Configuring VLAN for a Wired Profile on page 163.
Split tunnel	Set this to **Enabled** or **Disabled** for split tunnel functionality for the Centralized L2 subnet.

Table 133: *Centralized DHCP Mode Configuration Parameters*

Parameter	Description
	Enabling split tunnel allows a VPN user to access a public network and a local LAN or WAN network at the same time through the same physical network connection. For example, a user can use a remote access VPN software client connecting to a corporate network using a home wireless network. The user with split tunneling enabled is able to connect to file servers, database servers, mail servers, and other servers on the corporate network through the VPN connection. When the user connects to Internet resources (websites, FTP sites, and so on), the connection request goes directly to the gateway provided by the home network. The split-DNS functionality intercepts DNS requests from clients for non-corporate domains (as configured in Enterprise Domains list) and forwards to the Instant AP's own DNS server. When split-tunnel is disabled, all the traffic including the corporate and Internet traffic is tunneled irrespective of the routing profile specifications. If the GRE tunnel is down and when the corporate network is not reachable, the client traffic is dropped.
DHCP relay	If you are configuring a Centralized L2 DHCP profile, you can select **Enabled** to allow the Instant APs to intercept the broadcast packets and relay DHCP requests to the centralized DHCP server. The **DHCP relay** option is not available for Centralized L3 profile configuration.
Helper address	Specify the IP address of the DHCP server. For Centralized L3 DHCP profiles, the **Helper address** option is displayed only when DHCP relay is enabled.
VLAN IP	Specify the Centralized L3 DHCP subnet gateway IP.
VLAN Mask	Specify the subnet mask of the Centralized L3 DHCP subnet gateway IP.
Option 82	Select **Alcatel** to enable DHCP Option 82 and allow clients to send DHCP packets with the Option 82 string. The Option 82 string is available only in the Alcatel format. The Alcatel format for the Option 82 string consists of the following: ▪ Remote Circuit ID; X AP-MAC; SSID; SSID-Type ▪ Remote Agent; X IDUE-MAC The Option 82 string is specific to Alcatel and is not configurable.

4. Click **OK**.
5. Click **OK** in the **DHCP Servers** window.

In the New WebUI

To configure a centralized DHCP scope:

1. Navigate to the **Configuration** > **DHCP Server** page.
2. To configure a centralized DHCP scope, click **+** under **Centralized DHCP Scopes**.
3. To configure a centralized profile, select the profile type as **Centralized,L2** or **Centralized,L3** and configure the following parameters.

Table 134: *Centralized DHCP Mode Configuration Parameters*

Parameter	Description
Name	Enter a name for the DHCP scope.
Type	Set the type as follows: ■ **Centralized, L2** for the Centralized L2 profile ■ **Centralized, L3** for the Centralized L3 profile
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile on page 136 and Configuring VLAN for a Wired Profile on page 163.
Split tunnel	Click the toggle switch depending on whether you want to enable or disable the split tunnel functionality for the Centralized L2 subnet. Enabling split tunnel allows a VPN user to access a public network and a local LAN or WAN network at the same time through the same physical network connection. For example, a user can use a remote access VPN software client connecting to a corporate network using a home wireless network. The user with split tunneling enabled is able to connect to file servers, database servers, mail servers, and other servers on the corporate network through the VPN connection. When the user connects to Internet resources (websites, FTP sites, and so on), the connection request goes directly to the gateway provided by the home network. The split-DNS functionality intercepts DNS requests from clients for non-corporate domains (as configured in Enterprise Domains list) and forwards to the Instant AP's own DNS server. When split-tunnel is disabled, all the traffic including the corporate and Internet traffic is tunneled irrespective of the routing profile specifications. If the GRE tunnel is down and when the corporate network is not reachable, the client traffic is dropped.
DHCP relay	If you are configuring a Centralized L2 DHCP profile, click the the **DHCP relay** toggle switch to allow the Instant APs to intercept the broadcast packets and relay DHCP requests to the centralized DHCP server. The **DHCP relay** option is not available for Centralized L3 profile configuration.
Helper address	Specify the IP address of the DHCP server. For Centralized L3 DHCP profiles, the **Helper address** option is displayed only when DHCP relay is enabled.
VLAN IP	Specify the Centralized L3 DHCP subnet gateway IP.
VLAN Mask	Specify the subnet mask of the Centralized L3 DHCP subnet gateway IP.
Option 82	Select **Alcatel** to enable DHCP Option 82 and allow clients to send DHCP packets with the Option 82 string. The Option 82 string is available only in the Alcatel format. The Alcatel format for the Option 82 string consists of the following: ■ Remote Circuit ID; X AP-MAC; SSID; SSID-Type ■ Remote Agent; X IDUE-MAC The Option 82 string is specific to Alcatel and is not configurable.

4. Click **OK**.
5. Click **OK** in the **DHCP Servers** window.

The following table describes the behavior of the DHCP Relay Agent and Option 82 in the Instant AP.

Table 135: *DHCP Relay and Option 82*

DHCP Relay	Option 82	Result
Enabled	Enabled	DHCP packet relayed with the ALU-specific Option 82 string
Enabled	Disabled	DHCP packet relayed without the ALU-specific Option 82 string
Disabled	Enabled	DHCP packet not relayed, but broadcast with the ALU-specific Option 82 string
Disabled	Disabled	DHCP packet not relayed, but broadcast without the ALU-specific Option 82 string

In the CLI

To configure a Centralized L2 DHCP profile:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# server-type <centralized>
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP)(DHCP Profile <profile-name>)# option82 alu
(Instant AP)(DHCP Profile <profile-name>)# disable-split-tunnel
```

To configure a Centralized L3 DHCP profile:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# server-type <centralized>
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP)(DHCP Profile <profile-name>)# dhcp-relay
(Instant AP)(DHCP Profile <profile-name>)# dhcp-server <DHCP-relay-server>
(Instant AP)(DHCP Profile <profile-name>)# vlan-ip <DHCP IP address> mask <VLAN mask>
```

Configuring the Default DHCP Scope for Client IP Assignment

The DHCP server is a built-in server, used for networks in which clients are assigned IP address by the virtual controller. You can customize the DHCP pool subnet and address range to provide simultaneous access to more number of clients. The largest address pool supported is 2048. The default size of the IP address pool is 512.

When a DHCP server is configured and if the **Client IP assignment** parameter for an SSID profile is set to **Virtual Controller Assigned**, the virtual controller assigns the IP addresses to the WLAN or the wired clients. By default, the Instant AP automatically determines a suitable DHCP pool for **Virtual Controller Assigned** networks.



Instant APs typically select the 172.31.98.0/23 subnet. If the IP address of the Instant AP is within the 172.31.98.0/23 subnet, the Instant AP selects the 10.254.98.0/23 subnet. However, this mechanism does not guarantee that it would avoid all possible conflicts with the wired network. If your wired network uses either 172.31.98.0/23 or 10.254.98.0/23, and you experience problems with the **Virtual Controller Assigned** networks after upgrading to ArubaInstant 6.2.1.0-3.4.0.0 or later, manually configure the DHCP pool by following the steps described in this section.

You can configure a domain name, DNS server, and DHCP server for client IP assignment using the WebUI or the CLI.

In the Old WebUI

To configure a DHCP pool:

1. Navigate to the **More** > **DHCP Server** tab.
2. Enter the domain name of the client in the **Domain name** text box.
3. Enter the IP addresses of the DNS servers separated by a comma (,) in the **DNS Server(s)** text box.
4. Enter the duration of the DHCP lease in the **Lease time** text box. Select any of the following values from the drop-down list next to **Lease time**:
   - **Minutes**—For minutes, specify a value between 2 and 59.
   - **Hours**—For hours, specify a value between 1 and 23.
   - **Days** —For days, specify a value between 1 and 30.

   The default lease time is 0.
5. Enter the network range for the client IP addresses in the **Network** text box. The system generates a network range automatically that is sufficient for 254 addresses. If you want to provide simultaneous access to more number of clients, specify a larger range.
6. Specify the subnet mask details for the network range in the **Mask** text box.

   The DNS cache function is only enabled when content-filtering is disabled.
7. Click **OK** to apply the changes.

In the New WebUI

To configure a DHCP pool:

1. Navigate to the **Configuration** > **DHCP Server** page.
2. Enter the domain name of the client in the **Domain name** text box.
3. Enter the IP addresses of the DNS servers separated by a comma (,) in the **DNS Server(s)** text box.
4. Enter the network range for the client IP addresses in the **Network** text box. The system generates a network range automatically that is sufficient for 254 addresses. If you want to provide simultaneous access to more number of clients, specify a larger range.
5. Specify the subnet mask details for the network range in the **Mask** text box.
6. Enter the duration of the DHCP lease in the **Lease time** text box. Select any of the following values from the drop-down list next to **Lease time**:
   - **Minutes**—For minutes, specify a value between 2 and 59.
   - **Hours**—For hours, specify a value between 1 and 23.
   - **Days** —For days, specify a value between 1 and 30.

   The default lease time is 0.

   The DNS cache function is only enabled when content-filtering is disabled.
7. Click **Save** to apply the changes.

In the CLI

To configure a DHCP pool:

```
(Instant AP)(config)# ip dhcp pool
(Instant AP)(DHCP)# domain-name <domain>
(Instant AP)(DHCP)# dns-server <DNS-IP-address>
(Instant AP)(DHCP)# lease-time <minutes>
(Instant AP)(DHCP)# subnet <IP-address>
(Instant AP)(DHCP)# subnet-mask <subnet-mask>
```

To view the DHCP database:

```
(Instant AP)# show ip dhcp database
```

Chapter 17
Configuring Time-Based Services

This chapter describes time range profiles and the procedure for configuring time-based services. It includes the following topics:

- Time Range Profiles on page 312
- Configuring a Time Range Profile on page 313
- Applying a Time Range Profile to a WLAN SSID on page 314
- Applying a Time Range Profile to a Role on page 316
- Verifying the Configuration on page 315

Time Range Profiles

Starting from Instant 6.4.3.4-4.2.1.0, Instant APs allow you to enable or disable an SSID for users at a particular time of the day. You can now create a time range profile and assign it to a WLAN SSID, so that user access to the Internet or network is restricted during a specific time period.

Instant APs support the configuration of both absolute and periodic time range profiles. You can configure an absolute time range profile to execute during a specific timeframe or create a periodic profile to execute at regular intervals based on the periodicity specified in the configuration.

The following configuration conditions apply to the time-based services:

- Time-based services require an active NTP server connection. Instant APs use the default NTP server for time synchronization. However, the administrators can also configure an NTP server on the Instant AP. To verify the time synchronization between the NTP server and the Instant AP, execute the **show time-range** command and check if the time on the NTP server is in synchronization with the local time. For more information on NTP server configuration, see NTP Server.
- For a time range profile configured to **enable** an SSID on the Instant AP:
  - When the timer starts, if the current time is greater than the start time and lesser than the end time, the SSID will be broadcast in the list of available networks by the AP. If an ACL rule is linked to the time profile, it is re-programmed and the rule which is time-based is applied. All the user sessions having this role assigned will be deleted.
  - When the timer ends, if the current time is greater than the end time, the SSID is disabled. If the SSID is already disabled, then there is no effect on the SSID.
  - If the SSID profile itself is disabled using the following configuration, then it will remain disabled and not be broadcast according to time range profile configuration.

```
(Instant AP)(SSID Profile "<profile_name>")# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile "<profile_name>")# disable
(Instant AP)(SSID Profile "<profile_name>")# time-range <profile_name> enable
```



In the above example, the time-range configuration will be accepted, but there will be no impact on the SSID and will continue to remain disabled.

- For a time range profile configured to **disable** an SSID on the Instant AP:
  - When the timer starts, if the current time is greater than the start time and lesser than the end time, the SSID will not be broadcast by the AP in the list of available networks. If an ACL rule is linked to the time profile, it is re-programmed and the rule which is time-based is not applied. All the user sessions having this role assigned will be deleted.
  - When the timer ends, if the current time is greater than the end time, the SSID is broadcast by the AP. If the SSID is already enabled, then there is no effect on the SSID.
- The enable and disable time-range profiles cannot be applied to an SSID profile at the same time.
- If an SSID has two time range profiles configured with an overlapping duration, the overlapping time range is rejected by the AP.

Configuring a Time Range Profile

You can create time range profiles using the WebUI or the CLI.

In the Old WebUI

To create a time range profile:

1. Navigate to **System** > **Show advanced options** > **Time Based Services**.
2. Click **New** under **Time Range Profiles**. The **New profile** window for creating time range profiles is displayed.
3. Configure the parameters listed in the following table:

Table 136: *Time Range Profile Configuration Parameters*

Parameter	Description
Name	Specify a name for the time range profile.
Type	Select the type of time range profile. ■ **Periodic**—When configured, the state of the Instant AP changes based on the time range configured in the profile. ■ **Absolute**—When configured, the state of the Instant AP changes during a specific date, day, and time.
Period type	For periodic time range profiles, specify a periodic interval (day, weekday, weekend, or daily) at which the time range profile must be applied.
Start Day and **End Day**	For absolute time range profiles, specify the start day and the end day to configure a specific time period during which the time range profile is applied. **NOTE:** Ensure that the year selected for Start Day and End Day cannot exceed 2037.
Start Time	Select the start time for the time range profile in the hh:mm format.
End Time	Select the end time for the time range profile in hh:mm format.

4. Click **OK**.
5. Click **OK** in the **System** window.

In the New WebUI

To create a time range profile:

1. Navigate to **Configuration** > **System** page.
2. Click **Show advanced options** at the bottom of the window.
3. Expand **Time Based Services**.
4. Click **+** under **Time Range Profiles**.
5. Configure the parameters listed in the following table:

Table 137: *Time Range Profile Configuration Parameters*

Parameter	Description
Name	Specify a name for the time range profile.
Type	Select the type of time range profile. ▪ **Periodic**—When configured, the state of the Instant AP changes based on the time range configured in the profile. Specify a periodic interval (day, weekday, weekend, or daily) at which the time range profile must be applied. ▪ **Absolute**—When configured, the state of the Instant AP changes during a specific date, day, and time.
Start Day and **End Day**	For absolute time range profiles, specify the start day and the end day to configure a specific time period during which the time range profile is applied. **NOTE:** Ensure that the year selected for Start Day and End Day cannot exceed 2037.
Start Time	Select the start time for the time range profile in the hh:mm format.
End Time	Select the end time for the time range profile in hh:mm format.

6. Click **OK**.
7. Click **Save**.

In the CLI

To create an absolute time range profile:

```
(Instant AP)(config)# time-range <name> absolute start <startday> <starttime> end
<endday> <endtime>
```

To configure a periodic time range profile:

```
(Instant AP)(config)# time-range <name> periodic {<startday>|daily|weekday|weekend}
<starttime> to  <endtime>
```

Applying a Time Range Profile to a WLAN SSID

You can apply a time range profile to a WLAN SSID using the WebUI.

In the Old WebUI

Applying a time range profile:

1. Navigate to the WLAN SSID profile configuration wizard.
   a. Click **Networks** > **New** or
   b. Select an existing WLAN SSID and click **edit**.
2. Click **Show advanced options**.
3. In the **Time Range** section, click the **Edit** link, select a time range profile from the list, then select a value from the **Status** drop-down list, and then click **OK**.
   - When a time range profile is enabled on an SSID, the SSID is made available to the users for the configured time range. For example, if the specified time range is 12:00–13:00, the SSID becomes available only between 12 PM and 1 PM on a given day.
   - If a time range is disabled, the SSID becomes unavailable for the configured time range. For example, if the configured time range is 14:00–17:00, the SSID is made unavailable from 2 PM to 5 PM on a given day.
4. Click **Next** in the **WLAN Settings**, **VLAN**, and **Security** tabs and then click **Finish** in the **Access** tab.

In the New WebUI

Applying a time range profile:

1. Navigate to the WLAN SSID profile configuration wizard.
   a. Go to **Configuration** > **Networks.**
   b. Click **+** to add a new profile or select an existing WLAN SSID profile and click **Edit**.
2. Click **Show advanced options** at the bottom of the page.
3. In the **Time Range** section, click **Edit** for **Time Range Profiles**, select a time range profile from the list, then select a value from the **Status** drop-down list, and then click **OK**.
   - When a time range profile is enabled on an SSID, the SSID is made available to the users for the configured time range. For example, if the specified time range is 12:00–13:00, the SSID becomes available only between 12 PM and 1 PM on a given day.
   - If a time range is disabled, the SSID becomes unavailable for the configured time range. For example, if the configured time range is 14:00–17:00, the SSID is made unavailable from 2 PM to 5 PM on a given day.
4. Click **Next** until **Finish**.

In the CLI

To enable an SSID during a specific time-range:

```
(Instant AP)(config)# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile "<name>")# time-range <profile_name> enable
```

To disable an SSID during a specific time-range:

```
(Instant AP)(config)# wlan ssid-profile <profile_name>
(Instant AP)(SSID Profile "<name>")# time-range <profile_name> disable
```

Verifying the Configuration

To view the time range profiles created on an Instant AP:

```
(Instant AP) # show time-range
```

To view the list of time range profiles configured on an Instant AP:

```
(Instant AP)# show time-profile
```

Applying a Time Range Profile to a Role

You can apply a time range profile to a rule using the WebUI.

In the Old WebUI

Applying a time range profile:

1. Navigate to **Security** > **Roles**.
   a. Click **Roles** > **New** and create a new role or
   b. Select an existing role under **Roles** and click **Access Rules for <Role>** > **New**.
2. Select **Time Range** and select a time range from the drop-down list.
3. Click **OK**.
   - When a time range profile is enabled on a role, the role is made available to the users for the configured time range. For example, if the specified time range is 12:00–13:00, the role becomes available only between 12 PM and 1 PM on a given day.
   - If a time range is disabled, the role becomes unavailable for the configured time range. For example, if the configured time range is 14:00–17:00, the role is made unavailable from 2 PM to 5 PM on a given day.

In the New WebUI

Applying a time range profile:

1. Navigate to **Configuration** > **Security** > **Roles**.
   a. Click **Roles** > **+** and create a new role or
   b. Select an existing role under **Roles** and click **Access Rules for <Role>** > **New**.
2. Select **Time Range** and select a time range from the drop-down list.
3. Click **OK**.
   - When a time range profile is enabled on a role, the role is made available to the users for the configured time range. For example, if the specified time range is 12:00–13:00, the role becomes available only between 12 PM and 1 PM on a given day.
   - If a time range is disabled, the role becomes unavailable for the configured time range. For example, if the configured time range is 14:00–17:00, the role is made unavailable from 2 PM to 5 PM on a given day.

In the CLI

To enable a role during a specific time-range:

```
(Instant AP)(config)# wlan access-rule <profile_name>
(Instant AP)(SSID Profile "<name>")# rule ... time-range <profile_name>
```

To disable a role during a specific time-range:

```
(Instant AP)(config)# wlan access-rule <profile_name>
(Instant AP)(SSID Profile "<name>")# no rule ... time-range <profile_name>
```

Chapter 18
VPN Configuration

This chapter describes the following VPN configuration procedures:

- Understanding VPN Features on page 317
- Configuring a Tunnel from an Instant AP to a Mobility Controller on page 319
- Configuring Routing Profiles on page 328

Understanding VPN Features

As Instant APs use a virtual controller architecture, the Instant AP network does not require a physical controller to provide the configured WLAN services. However, a physical controller is required for terminating VPN tunnels from the Instant AP networks at branch locations to data centers, where the Aruba controller acts as a VPN concentrator.

When a VPN is configured, the Instant AP acting as the virtual controller creates a VPN tunnel to an Aruba Mobility Controller in your corporate office. The controller acts as a VPN endpoint and does not supply the Instant AP with any configuration.

The VPN features are recommended for the following setups:

- Enterprises with many branches that do not have a dedicated VPN connection to the corporate office.
- Branch offices that require multiple Instant APs.
- Individuals working from home and, connecting to the VPN.

The survivability feature of Instant APs with the VPN connectivity of Remote APs allows you to provide corporate connectivity on non-corporate networks.

Supported VPN Protocols

Instant supports the following VPN protocols for remote access:

Table 138: *VPN Protocols*

VPN Protocol	Description
Aruba IPsec	IPsec is a protocol suite that secures IP communications by authenticating and encrypting each IP packet of a communication session. You can configure an IPsec tunnel to ensure that the data flow between the networks is encrypted. However, you can configure a split-tunnel to encrypt only the corporate traffic. When IPsec is configured, ensure that you add the Instant AP MAC addresses to the whitelist database stored on the controller or an external server. IPsec supports Local, L2, and L3 modes of IAP-VPN operations. **NOTE:** The Instant APs support IPsec only with Aruba Controllers.
Layer-2 GRE	GRE is a tunnel protocol for encapsulating multicast, broadcast, and L2 packets between a GRE-capable device and an endpoint. Instant APs support the configuration of L2 GRE tunnel with an Aruba controller to encapsulate the packets sent and received by the Instant AP.

Table 138: *VPN Protocols*

VPN Protocol	Description
	You can use the GRE configuration for L2 deployments when there is no encryption requirement between the Instant AP and controller for client traffic. Instant APs support two types of GRE configuration: ▪ **Manual GRE**—The manual GRE configuration sends unencrypted client traffic with an additional GRE header and does not support failover. When manual GRE is configured on the Instant AP, ensure that the GRE tunnel settings are enabled on the controller. ▪ **Aruba GRE**—With Aruba GRE, no configuration on the controller is required except for adding the Instant AP MAC addresses to the whitelist database stored on the controller or an external server. Aruba GRE reduces manual configuration when **Per-AP tunnel** configuration is required and supports failover between two GRE endpoints. **NOTE:** Instant APs support manual and Aruba GRE configuration only for L2 mode of operations. Aruba GRE configuration is supported only on Aruba Controllers.

Diffie-Hellman Algorithm

Diffie-Hellman is a key agreement algorithm that allows two parties to agree upon a shared secret, and is used within IKE to securely establish session keys.

Instant supports the following Diffie-Hellman groups:

- Group 2: 1024-bit Diffie–Hellman prime modulus group
- Group 14: 2048-bit Diffie–Hellman prime modulus group

By default, Instant APs attempt to use Diffie–Hellman Group 2 to set up an IAP VPN connection. If the controller rejects Diffie–Hellman Group 2, the Instant APs can use Diffie–Hellman Group 14.



Diffie–Hellman Group 2 is not permitted if FIPS mode is enabled on anInstant AP.

Enabling Cipher Algorithms

Starting from Instant 8.4.0.0, you can configure the following ciphers based on your preference, to establish an SSH connection with the Instant AP:

- AES-CBC
- AES-CTR



You cannot disable both the ciphers together. At any given point in time, either one of both the ciphers will be enabled.

By default, these ciphers are enabled. You can configure the ciphers by using the CLI.

The following command enables AES-CBC and disables AES-CTR on the SSH server:

```
(Instant AP)(config) #ssh disable-ciphers aes-ctr
```

The following command enables the disabled cipher encryptions on the SSH server:

```
(Instant AP)(config) #no ssh disable-ciphers
```

The following command displays the SSH configuration details:

```
(Instant AP) #show ssh
```

Configuring a Tunnel from an Instant AP to a Mobility Controller

Instant AP supports the configuration of tunneling protocols such as GRE and IPsec. This section describes the procedure for configuring VPN host settings on an Instant AP to enable communication with a controller in a remote location:

- Configuring an IPsec Tunnel on page 319
- Configuring an L2-GRE Tunnel on page 321

Configuring an IPsec Tunnel

An IPsec tunnel is configured to ensure that the data flow between the networks is encrypted. When configured, the IPsec tunnel to the controller secures corporate data.

You can configure an IPsec tunnel from the virtual controller using the WebUI or the CLI.

In the Old WebUI

To configure a tunnel for IPsec protocol:

1. Go to **More** > **Tunneling**.
2. Select **Aruba IPSec** from the **Protocol** drop-down list.
3. Enter the IP address or FQDN for the primary VPN or IPsec endpoint in the **Primary host** text box.
4. Enter the IP address or FQDN for the backup VPN or IPsec endpoint in the **Backup host** text box. This entry is optional. When you specify the primary and backup host details, the following details are displayed:
    a. To allow the VPN tunnel to switch back to the primary host when it becomes available again, select **Enabled** from the **Preemption** drop-down list. This step is optional.
    b. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches back to the primary host after the specified hold-time. The default value for **Hold time** is 600 seconds.
    c. To allow the Instant AP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately, select **Enabled** from the **Fast failover** drop-down list. When fast failover is enabled and if the primary tunnel fails, the Instant AP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.
    d. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, set **Reconnect User On Failover** to **Enabled**.
    e. To configure an interval during which the wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect Time On Failover** within a range of 30–900 seconds. By default, the reconnection duration is set to 60 seconds.

5. Specify the following parameters:
    a. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the Instant AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the Instant AP sends one packet to the controller every 5 seconds.
    b. Enter a value for **Max allowed test packet loss** to define a number for lost packets, exceeding which the Instant AP can determine that the VPN connection is unavailable. The default value is 2.
6. Click **Next**to create routing profiles. When the IPsec tunnel configuration is completed, the packets that are sent from and received by an Instant AP are encrypted.
7. Click **Finish**.

In the New WebUI

To configure a tunnel for IPsec protocol:

1. Go to the **Configuration** > **Tunneling** page.
2. Under **Controller**, select **Aruba IPSec** from the **Protocol** drop-down list.
3. Enter the IP address or FQDN for the primary VPN or IPsec endpoint in the **Primary host** text box.
4. Enter the IP address or FQDN for the backup VPN or IPsec endpoint in the **Backup host** text box. This entry is optional. When you specify the primary and backup host details, the following details are displayed:
    a. To allow the VPN tunnel to switch back to the primary host when it becomes available again, click the **Preemption** toggle switch. This step is optional.
    b. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches back to the primary host after the specified hold-time. The default value for **Hold time** is 600 seconds.
    c. To allow the Instant AP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately, toggle the **Fast failover** switch. When fast failover is enabled and if the primary tunnel fails, the Instant AP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.
    d. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, toggle the **Reconnect User On Failover** switch.
    e. To configure an interval during which the wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect Time On Failover** within a range of 30–900 seconds. By default, the reconnection duration is set to 60 seconds.
5. Specify the following parameters:
    a. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the Instant AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the Instant AP sends one packet to the controller every 5 seconds.

b. Enter a value for **Max allowed test packet loss** to define a number for lost packets, exceeding which the Instant AP can determine that the VPN connection is unavailable. The default value is 2.

6. Click **Save**.

In the CLI

To configure an IPsec VPN tunnel:

```
(Instant AP)(config)# vpn primary <name>
(Instant AP)(config)# vpn backup <name>
(Instant AP)(config)# vpn fast-failover
(Instant AP)(config)# vpn hold-time <seconds>
(Instant AP)(config)# vpn preemption
(Instant AP)(config)# vpn monitor-pkt-send-freq <frequency>
(Instant AP)(config)# vpn monitor-pkt-lost-cnt <count>
(Instant AP)(config)# vpn reconnect-user-on-failover
(Instant AP)(config)# vpn reconnect-time-on-failover <down_time>
```

Example

```
(Instant AP)(config)# vpn primary 192.0.2.18
(Instant AP)(config)# vpn backup  192.0.2.20
(Instant AP)(config)# vpn fast-failover
(Instant AP)(config)# vpn preemption

(Instant AP)(config)# ip dhcp distl2
(Instant AP)(DHCP Profile "distL2")# server-type Distributed,L2
(Instant AP)(DHCP Profile "distL2")# server-vlan 2
(Instant AP)(DHCP Profile "distL2")# ip-range 10.15.205.0 10.15.205.255
(Instant AP)(DHCP Profile "distL2")# subnet-mask 255.255.255.0
(Instant AP)(DHCP Profile "distL2")# lease-time 86400
(Instant AP)(DHCP Profile "distL2")# default-router 10.15.205.254
(Instant AP)(DHCP Profile "distL2")# dns-server 10.13.6.110,10.1.1.50
(Instant AP)(DHCP Profile "distL2")# domain-name arubanetworks.com
(Instant AP)(DHCP Profile "distL2")# client-count 5

(Instant AP)(config)# ip dhcp local
(Instant AP)(DHCP Profile "local")# server-type Local
(Instant AP)(DHCP Profile "local")# server-vlan 200
(Instant AP)(DHCP Profile "local")# subnet 172.16.200.1
(Instant AP)(DHCP Profile "local")# subnet-mask 255.255.255.0
(Instant AP)(DHCP Profile "local")# lease-time 86400
(Instant AP)(DHCP Profile "local")# dns-server 10.13.6.110,10.1.1.50
(Instant AP)(DHCP Profile "local")# domain-name arubanetworks.com
```

To view the VPN configuration:

```
(Instant AP)# show vpn config
```

Configuring an L2-GRE Tunnel

This section describes the following procedures:

- Configuring Manual GRE Parameters
- Configuring Aruba GRE Parameters

Configuring Manual GRE Parameters

You can configure a GRE tunnel between the Instant AP and the controller using either the virtual controller IP or the Instant AP IP, based on the following Instant AP settings:

- If a virtual controller IP is configured and if **Per-AP tunnel** is disabled, use virtual controller IP.
- If a virtual controller IP is not configured or if **Per-AP tunnel** is enabled, use the Instant AP IP.



The controller MAC address should not be used as the branch name in a cluster setup if **Per-AP tunnel** is enabled.

For information on the GRE tunnel configuration on the controller, refer to the *ArubaOS User Guide*.

In the Old WebUI

To configure a GRE tunnel:

1. Go to **More** > **Tunneling**.
2. Select **Manual GRE** from the **Protocol** drop-down list.
3. Specify the following parameters:
   a. Enter an IP address or an FQDN for the main VPN or GRE endpoint in the **Primary host** text box.
   b. Enter a value in the **GRE type** text box.
   c. Select **Enabled** or **Disabled** from the **Per-AP tunnel** drop-down list. Enable this option to create a GRE tunnel from each Instant AP to the VPN or GRE endpoint rather than the tunnels created just from the master Instant AP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the Instant AP itself and need not be forwarded through the master Instant AP.



By default, the **Per-AP tunnel** option is disabled.

4. Click **Next** to continue. When the GRE tunnel configuration is completed on both the Instant AP and the controller, the packets sent from and received by an Instant AP are encapsulated, but not encrypted.
5. Click **Finish**.

In the New WebUI

To configure a GRE tunnel:

1. Go to the **Configuration** > **Tunneling** page.
2. Expand the **Controller** section, select **Manual GRE** from the **Protocol** drop-down list.
3. Specify the following parameters:
   a. Enter an IP address or an FQDN for the main VPN or GRE endpoint in the **Primary host** text box.
   b. Enter a value in the **GRE type** text box.
   c. Toggle the **Per-AP tunnel** switch to create a GRE tunnel from each Instant AP to the VPN or GRE endpoint rather than the tunnels created just from the master Instant AP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the Instant AP itself and need not be forwarded through the master Instant AP. By default, this parameter is disabled.
4. Click **Save**.

In the CLI

To configure a manual GRE VPN tunnel:

```
(Instant AP)(config)# gre primary <name>
(Instant AP)(config)# gre type <type>
(Instant AP)(config)# gre per-ap-tunnel
```

To view VPN configuration details:

```
(Instant AP)# show vpn config
```

To configure GRE tunnel on the controller:

```
(Instant AP)(config)# interface tunnel <Number>
(Instant AP)(config-tunnel)# description <Description>
(Instant AP)(config-tunnel)# tunnel mode gre <ID>
(Instant AP)(config-tunnel)# tunnel source <controller-IP>
(Instant AP)(config-tunnel)# tunnel destination <AP-IP>
(Instant AP)(config-tunnel)# trusted
(Instant AP)(config-tunnel)# tunnel vlan <allowed-VLAN>
```

Configuring Aruba GRE Parameters

The Aruba GRE feature uses the IPsec connection between the Instant AP and the controller to send the control information for setting up a GRE tunnel. When Aruba GRE configuration is enabled, a single IPsec tunnel between the Instant AP cluster and the controller, and one or several GRE tunnels are created based on the Per-AP tunnel configuration on the Instant AP. For Aruba GRE, no manual configuration is required on the controller to create the GRE tunnel.

Aruba GRE is supported on ArubaControllers running ArubaOS 6.4.x.x or later versions.



Instant APs can send IPsec and GRE heartbeat packets to ArubaControllers. By default, Instant APs verify the status of heartbeat messages every 5 seconds, and look for lost packets 6 times before marking down the IPsec tunnel. However, these time intervals can be modified.

In the Old WebUI

To configure Aruba GRE:

1. Go to **More** > **Tunneling**.
2. Select **Aruba GRE** from the **Protocol** drop-down list.
3. Enter the IP address or the FQDN for the main VPN or IPsec endpoint in the **Primary host** text box.
4. Enter the IP address or the FQDN for the backup VPN or IPsec endpoint in the **Backup host** text box. This entry is optional. When you enter the primary host IP address and backup host IP address, the following details are displayed:
   a. To allow the VPN tunnel to switch back to the primary host when it becomes available again, select **Enabled** from the **Preemption** drop-down list. This step is optional.
   b. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches to the primary host after the specified hold time. The default value for **Hold time** is 600 seconds.
   c. To allow the Instant AP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately, select **Enabled** from the **Fast failover** drop-down list. If this option is enabled, when the primary

tunnel fails, the Instant AP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.

d. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, set **Reconnect User on Failover** to **Enabled**.

e. To configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect Time on Failover** within the range of 30–900 seconds. By default, the reconnection duration is set to 60 seconds.

5. Specify the following parameters:
   a. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the Instant AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the Instant AP sends one packet to the controller every 5 seconds.
   b. Enter a value for **Max allowed test packet loss** to define a number for lost packets, exceeding which the Instant AP can determine that the VPN connection is unavailable. The default value is 2.
   c. Select **Enabled** or **Disabled** from the **Per-AP tunnel** drop-down list. The administrator can enable this option to create a GRE tunnel from each Instant AP to the VPN or GRE endpoint rather than the tunnels created just from the master Instant AP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the Instant AP itself and need not be forwarded through the master Instant AP.
6. Click **Next**.
7. Click **Finish**.

In the New WebUI

To configure Aruba GRE:

1. Go to the **Configuration** > **Tunneling** page.
2. Expand **Controller**.
3. Select **Aruba GRE** from the **Protocol** drop-down list.
4. Enter the IP address or the FQDN for the main VPN or IPsec endpoint in the **Primary host** text box.
5. Enter the IP address or the FQDN for the backup VPN or IPsec endpoint in the **Backup host** text box. This entry is optional. When you enter the primary host IP address and backup host IP address, the following details are displayed:
   a. To allow the VPN tunnel to switch back to the primary host when it becomes available again, click the **Preemption** toggle switch. This step is optional.
   b. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches to the primary host after the specified hold time. The default value for **Hold time** is 600 seconds.
   c. To allow the Instant AP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately, toggle the **Fast failover** switch. If this option is enabled, when the primary tunnel fails, the Instant AP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.

d. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, toggle the **Reconnect User on Failover** switch.

e. To configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect Time on Failover** within the range of 30–900 seconds. By default, the reconnection duration is set to 60 seconds.

6. Specify the following parameters:

   a. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the Instant AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the Instant AP sends one packet to the controller every 5 seconds.

   b. Specify a value for **Max allowed test packet loss** to define a number for lost packets, exceeding which the Instant AP can determine that the VPN connection is unavailable. The default value is 2.

   c. Enable or disable the **Per-AP tunnel** toggle switch as required. The administrator can enable this option to create a GRE tunnel from each Instant AP to the VPN or GRE endpoint rather than the tunnels created just from the master Instant AP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the Instant AP itself and need not be forwarded through the master Instant AP.

7. Click **Save**.

In the CLI

To enable Aruba GRE tunnel:

```
(Instant AP)(config)# vpn gre-outside
(Instant AP)(config)# vpn primary <name/IP-address>
(Instant AP)(config)# vpn backup <<name/IP-address>>
(Instant AP)(config)# vpn fast-failover
(Instant AP)(config)# vpn hold-time <seconds>
(Instant AP)(config)# vpn preemption
(Instant AP)(config)# vpn monitor-pkt-send-freq <frequency>
(Instant AP)(config)# vpn monitor-pkt-lost-cnt <count>
(Instant AP)(config)# vpn reconnect-user-on-failover
(Instant AP)(config)# vpn reconnect-time-on-failover <down_time>
```

To view VPN configuration details:

```
(Instant AP)# show vpn config
```

Support for IAP-VPN Termination on Mobility Controller Virtual Appliance

Starting from Aruba Instant 8.3.0.0, IAP-VPN is supported on Mobility Controller Virtual Appliance by using default self-signed certificate (Aruba PKI). For Instant AP to establish IPsec connection with Mobility Controller Virtual Appliance, the controller presents a default self-signed certificate which is uploaded on the Instant AP using Activate.



Mobility Masters (Mobility Master Hardware Appliance, Mobility Master Virtual Appliance, and Master Controller Mode) do not support any AP termination including Campus APs, Remote APs and IAP-VPN tunnels.

Through Activate, you can push only one default self-signed certificate to Instant AP which can be used to establish IPsec tunnel with Mobility Controller Virtual Appliance.

VPN features are ideal for:

- Enterprises with many branches that do not have a dedicated VPN connection to the Head Quarter.
- Branch offices that require multiple APs.
- Individuals working from home, connecting to the VPN.

This new architecture and form factor seamlessly adds the survivability feature of Instant APs with the VPN connectivity of RAPs — providing corporate connectivity to branches.

Configuring Multiple Active Tunnels

Starting from Aruba Instant 8.4.0.0, you can configure multiple active VPN tunnels on an Instant AP. You can configure up to four pairs of Primary and Backup VPN tunnels, out of which one pair is considered the default tunnel and the other three pairs as non-default tunnels. Only one IPsec tunnel can be selected for each VPN primary and backup pair and a default VPN tunnel must be configured if you wish to keep more than one active VPN tunnel to pass Centralized, L2 traffic.



This feature is currently not supported for IPv6.

Limitations

Following are some of the limitations observed when configuring multiple active tunnels:

- Multiple active tunnels are not supported in shared VPN mode. Only per AP tunnels are supported.
- Multiple active tunnels are supported with GRE data tunnels only. No IPsec data tunnel support is provided.
- Multiple active tunnels supported in Centralized,L2 VPN mode only.
- Multiple active tunnels need to be in full tunnel mode and not split tunnel mode.

Configuring a Default VPN Tunnel

The following example configures a default VPN tunnel:

```
(Instant AP)(config)# vpn primary <IP address or domain name>
(Instant AP)(config)# vpn backup <IP address or domain name>
(Instant AP)(config)# vpn fast-failover
(Instant AP)(config)# vpn gre-outside
(Instant AP)(config)# gre per-ap-tunnel
(Instant AP)(config)# vpn hold-time <seconds>
(Instant AP)(config)# vpn preemption
(Instant AP)(config)# vpn monitor-pkt-send-freq <frequency>
(Instant AP)(config)# vpn monitor-pkt-lost-cnt <count>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Configuring a non-default VPN Tunnel

The following example configures a non-default VPN tunnel profile:

```
(Instant AP)(config)# vpn tunnel-profile <profile_name>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# primary <IP address or domain name>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# backup <IP address or domain name>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# gre-outside
(Instant AP)(VPN Tunnel Profile "<profile_name>")# per-ap-tunnel
(Instant AP)(VPN Tunnel Profile "<profile_name>")# fast-failover
(Instant AP)(VPN Tunnel Profile "<profile_name>")# hold-time <seconds>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# preemption
(Instant AP)(VPN Tunnel Profile "<profile_name>")# monitor-pkt-send-freq <frequency>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# monitor-pkt-lost-cnt <count>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# end
(Instant AP)# commit apply
```

Configuring Centralized, L2 DHCP Scopes to use Default VPN Tunnel

The following example configures a Centralized, L2 DHCP scope to use a default VPN tunnel:

```
(Instant AP)(config)# ip dhcp <profile_name>
(Instant AP)(DHCP Profile "<profile_name>")# server-type Centralized,L2
(Instant AP)(DHCP Profile "<profile_name>")# server-vlan <VLAN ID or VLAN List>
(Instant AP)(DHCP Profile "<profile_name>")# disable-split-tunnel
(Instant AP)(DHCP Profile "<profile_name>")# end
(Instant AP)# commit apply
```

Configuring Centralized, L2 DHCP Scopes to use a Non-Default VPN Tunnel

The following example configures a Centralized, L2 DHCP scope to use a non-default VPN tunnel:

```
(Instant AP)(config)# ip dhcp <profile_name>
(Instant AP)(DHCP Profile "<profile_name>")# server-type Centralized,L2
(Instant AP)(DHCP Profile "<profile_name>")# server-vlan <VLAN ID or VLAN List>
(Instant AP)(DHCP Profile "<profile_name>")# disable-split-tunnel
(Instant AP)(DHCP Profile "<profile_name>")# tunnel-profile <profile_name>
(Instant AP)(DHCP Profile "<profile_name>")# end
(Instant AP)# commit apply
```

Configure Customized Certificate for IPsec Tunnel

The following example configures an IPsec tunnel to use a customized certificate:

```
(Instant AP)(config)# vpn tunnel-profile <profile_name>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# use-custom-cert
(Instant AP)(VPN Tunnel Profile "<profile_name>")# primary <IP address or domain name>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# backup <IP address or domain name>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# fast-failover
(Instant AP)(VPN Tunnel Profile "<profile_name>")# hold-time <seconds>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# preemption
(Instant AP)(DHCP Profile "<profile_name>")# end
(Instant AP)# commit apply
```

Debugging

Use the following command to check the IPsec tunnel status:

```
(Instant AP)(config)# show vpn status
```

Use the following command to check the VPN registration status:

```
(Instant AP)(config)# show vpn tunnels
```

Use the following command to check the VPN logs:

```
(Instant AP)(config)# show log vpn-tunnel
```

Use the following command to view the Centralized,L2 configuration:

```
(Instant AP)(config)# show dhcps
```

Configuring Routing Profiles

Instant APs can terminate a single VPN connection on an Aruba Mobility Controller. The routing profile defines the corporate subnets which need to be tunneled through IPsec. You can configure routing profiles for policy based routing into the VPN tunnel using the WebUI or the CLI.

Table 139: *Configuring Routing Profiles*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **Routing** page. 2. In the **Routing** table, click **+**. 3. Update the following parameters: ▪ **Destination**— Specify the destination network that is reachable through the VPN tunnel. This defines the IP or subnet that must reach through the IPsec tunnel. Traffic to the IP or subnet defined here will be forwarded through the IPsec tunnel. ▪ **Netmask**—Specify the subnet mask to the destination. ▪ **Gateway**—Specify the gateway to which the traffic must be routed. This IP address must be the controller IP address on which the VPN connection is terminated. If you have a primary and backup host, configure two routes with the same destination and netmask, but ensure that the gateway is the primary controller IP for one route and the backup controller IP for the second route. ▪ **Metric**—The default metric value is 15. Specify a metric value for the datapath route. When two routes or more routes with the same network destination are available for data forwarding, the route with the least metric value takes preference. 4. Repeat steps 2 and 3 to create the required number of routing profiles. 5. Click **OK**. 6. Click **Save**.	1. Go to **More** > **Routing**. The **Routing** window is displayed. 2. Click **New**. The **Route** window is displayed. 3. Update the following parameters: ▪ **Destination**— Specify the destination network that is reachable through the VPN tunnel. This defines the IP or subnet that must reach through the IPsec tunnel. Traffic to the IP or subnet defined here will be forwarded through the IPsec tunnel. ▪ **Netmask**—Specify the subnet mask to the destination. ▪ **Gateway**—Specify the gateway to which the traffic must be routed. This IP address must be the controller IP address on which the VPN connection is terminated. If you have a primary and backup host, configure two routes with the same destination and netmask, but ensure that the gateway is the primary controller IP for one route and the backup controller IP for the second route. ▪ **Metric**—The default metric value is 15. Specify a metric value for the datapath route. When two routes or more routes with the same network destination are available for data forwarding, the route with the least metric value takes preference. 4. Repeat step 3 to create the required number of routing profiles. 5. Click **OK** in **Route** and then click **OK** in **Routing**.

The following CLI commands configure a routing profile:

```
(Instant AP)(config)# routing-profile
(Instant AP)(Routing-profile)# route <destination> <mask> <gateway> {<metric>}
```



Routing profile is primarily used for IAP-VPN scenarios, to control which traffic should flow between the master Instant AP and the VPN tunnel, and which traffic should flow outside of the tunnel.

Dynamic DNS Registration

This chapter describes the procedure for configuring Dynamic DNS on Instant APs and their Distributed, L3 clients. It includes the following topics:

- Enabling Dynamic DNS on page 329
- Configuring Dynamic DNS Updates for Clients on page 330
- Verifying the Configuration on page 331

Enabling Dynamic DNS

Starting from Instant 6.4.4.4-4.2.3.0, Instant APs support the dynamic DNS feature which enables updating the host name of the Instant AP and the DL3 clients connected to it. In a scenario where the public IP address is dynamically handed to the Instant AP by the ISP, the connectivity to the Instant AP is lost when there is a change in the public IP address. Similarly, in case of DL3 clients, where the Instant AP acts as a DHCP server, the host becomes unreachable when the dynamically assigned IP address is changed. The dynamic DNS feature eliminates these issues by configuring a host name, thus providing a uniform approach to access the Instant AP and the DL3 clients. The IP address of the Instant AP and the DL3 client is mapped to the host name and this gets automatically updated to the DNS server each time the IP address is changed.

The following procedure describes how to enable Dynamic DNS using the WebUI.

Table 140: *Configuring Dynamic DNS*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **Services** page. 2. Expand **Dynamic DNS**. 3. Toggle the **Enable Dynamic DNS** switch to enable. 4. Configure the settings defined in the Dynamic DNS Configuration Parameters table below. 5. Click **Save**.	1. Navigate to **More** > **Services** > **Dynamic DNS**. 2. Select the **Enable Dynamic DNS** check box. 3. Configure the settings defined in the Dynamic DNS Configuration Parameters table below. 4. Click **OK**.

Table 141: *Dynamic DNS Configuration Parameters*

Parameter	Description	Example
Key	Configures a Transaction Signature shared secret key to secure the dynamic updates. The following algorithm names are supported: ■ hmac-md5 (used by default if algo-name is not specified) ■ hmac-sha1 ■ hmac-sha256	`hmac-sha1:arubaddns: 16YuLPdH21rQ6PuK9udsVLtJw3Y=`

Table 141: *Dynamic DNS Configuration Parameters*

Parameter	Description	Example
	NOTE: When the **Key** value is configured, the update is successful only if the Instant AP and the DNS server clocks are in sync.	
Server IP	Enter the server IP address of the DNS server to which the client updates are sent. **NOTE:** If the DNS server IP address is not specified in the **Dynamic DNS** window, the Instant AP's updates will be sent to the Instant APits DNS server instead.	`10.17.132.85`
Interval	Specify the time interval (in seconds) at which the DNS updates are to be synced to the server. The default time interval is 12 hours, minimum time interval is 15 minutes, and maximum time interval is 100 days.	`900`

The following CLI command enables dynamic DNS on an Instant AP

```
(Instant AP)(config)# dynamic-dns-ap
```

The following CLI commands configure a TSIG key and server IP address:

```
(Instant AP)(config)# dynamic-dns-ap key <algo-name:keyname:keystring>
(Instant AP)(config)# dynamic-dns-ap server <ddns_server>
```

The following CLI command configures a time interval:

```
(Instant AP)(config)# dynamic-dns-interval <ddns_interval>
```

Configuring Dynamic DNS Updates for Clients

You can enable DDNS updates when creating or editing a DHCP scope for **Distributed, L3** clients. When enabled, the DDNS updates of the clients are periodically sent during the specified time to the DNS server that is configured in the DHCP profile. For the DL3 clients, if the DNS server IP is not configured in the DHCP profile, the client updates will be dropped. The DDNS updates are secured by using TSIG shared secret keys, when communicating between the client and the server. For more information, refer to Enabling Dynamic DNS on page 329 and Configuring Distributed DHCP Scopes on page 298.

Table 142: *Configuring Dynamic DNS Updates for Clients*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **DHCP Server** page. 2. Select the distributed L3 DHCP Scope under **Distributed DHCP Scopes** to modify a DHCP scope. 3. Toggle the **Dynamic DNS** switch to enable. 4. In the **Key** text box, enter the TSIG shared secret key. 5. Click **Next** until **Finish**.	1. Navigate to **More** > **DHCP Server**, select the distributed L3 DHCP Scope under **Distributed DHCP Scopes** and click **Edit**. 2. Select the **Dynamic DNS** check box. 3. Enter the TSIG shared secret **key**. 4. Click **Next** and then click **Finish**.

The following CLI commands enable DDNS for Instant AP clients:

```
(Instant AP)(config)# ip dhcp <profile name>
```

```
(Instant AP)(DHCP profile "<name>")# dynamic-dns
(Instant AP)(DHCP profile "<name>")# server-type <Distributed,L3>
(Instant AP)(DHCP profile "<name>")# dynamic-dns key <algo-name:keyname:keystring>
```

Verifying the Configuration

The following CLI command shows the DDNS status on an Instant AP:

```
(Instant AP)# show ddns
```

The following CLI command shows the list of DDNS clients:

```
(Instant AP)# show ddns clients
```



- DHCP profile name is None for the Master Instant AP update sent.
- The **show running-config** command displays the key in the encrypted format.
- You can also configure dynamic DNS on anInstant AP or clients using the privileged execution mode in the CLI. For more information, refer to the **show ddns clients** command in the latest *ArubaInstant CLI Reference Guide.*

This section provides the following information:

- Understanding IAP-VPN Architecture on page 332
- Configuring Instant AP and Controller for IAP-VPN Operations on page 336
- IAP-VPN Deployment Scenarios on page 346

Understanding IAP-VPN Architecture

The IAP-VPN architecture includes the following two components:

- Instant APs at branch sites
- Controller at the datacenter

The master Instant AP at the branch site acts as the VPN endpoint and the controller at the datacenter acts as the VPN concentrator. When an Instant AP is set up for VPN, it forms an IPsec tunnel to the controller to secure sensitive corporate data. IPsec authentication and authorization between the controller and the Instant APs are based on the RAP whitelist configured on the controller.



Only the master Instant AP in anInstant AP cluster forms the VPN tunnel.

From the controller perspective, the master Instant APs that form the VPN tunnel are considered as VPN clients. The controller terminates VPN tunnels and routes or switches the VPN traffic. The Instant AP cluster creates an IPsec or GRE VPN tunnel from the virtual controller to a Mobility Controller in a branch office. The controller only acts as an IPsec or GRE VPN endpoint and it does not configure the Instant AP.

IAP-VPN Scalability Limits

The controller scalability in IAP-VPN architecture depends on factors such as IAP-VPN branches, route limit, and VLAN limit.

Table 143: *IAP-VPN Scalability*

Platforms	IAP-VPN Branches (Preferred)	Route Limit	User Limit (L2 Mode)	VLAN Limit
7280	8,192	32,769	16,384	4,094
7240XM	8,192	32,769	16384	4,094
7220	4,096	16,384	16,384	4,094
7210	2,048	8,192	12,228	4,094
7205	1,024	8,192	8,192	2,048

Table 143: *IAP-VPN Scalability*

Platforms	IAP-VPN Branches (Preferred)	Route Limit	User Limit (L2 Mode)	VLAN Limit
7030	256	8,189	3,582	256
7024	128	4,093	1,792	128
7010	128	4,093	1,792	128
7008	64	4,093	896	128
7005	64	4,093	896	128

The following table provides the IAP-VPN scalability information for various controller platforms:

- **IAP-VPN Branches**—The number of IAP-VPN branches that can be terminated on a given controller platform.
- **Route Limit**—The number of L3 routes supported on the controller.
- **User Limit**—For extended VLANs.
- **VLAN Limit**—The number of VLANs supported on the controller.

IAP-VPN Forwarding Modes

The forwarding modes determine whether the DHCP server and default gateway for clients reside in the branch or at the datacenter. These modes do not determine the firewall processing or traffic forwarding functionality. The virtual controller enables different DHCP pools (various assignment modes) in addition to allocating IP subnets for each branch.

The virtual controller allows different modes of forwarding traffic from the clients on a VLAN based on the DHCP scope configured on the Instant AP.

For the IAP-VPN deployments, the following forwarding modes are supported:

- Local mode
- L2 Switching mode
- L3 routing mode

The DHCP scopes associated with these forwarding modes are described in the following sections.



Ensure that VLAN 1 is not configured for any of the DHCP scopes as it is reserved for a different purpose.

Local Mode

In this mode, the Instant AP cluster at that branch has a local subnet and the master Instant AP of the cluster acts as the DHCP server and gateway for clients. The local mode provides access to the corporate network using the inner IP of the IPsec tunnel. The network address for traffic destined to the corporate network is translated at the source with the inner IP of the IPsec tunnel and is forwarded through the IPsec tunnel. The traffic destined to the non-corporate network is translated using the IP address of the Instant AP and is forwarded through the uplink.



When the local mode is used for forwarding client traffic, hosts on the corporate network cannot establish connections to the clients on the Instant AP, because the source addresses of the clients are translated.

Local, L2 Mode

In this mode, the Instant AP cluster at that branch has a local subnet and the master Instant AP of the cluster acts as the DHCP server. The default gateway is located outside the Instant AP and the network address for the client traffic is not translated at source. In the Local, L2 mode, access to the corporate network is supported only in a single Instant AP cluster. The traffic to the non-corporate network is locally bridged.

Local, L3 Mode

In this mode, the network address for traffic destined to the corporate network is translated at the source with the inner IP of the IPsec tunnel and is forwarded through the IPsec tunnel. The traffic destined to the non-corporate network is routed.

Distributed, L2 Mode

In this mode, the Instant AP assigns an IP address from the configured subnet and forwards traffic to both corporate and non-corporate destinations. Clients receive the corporate IP with virtual controller as the DHCP server. The default gateway for the client still resides in the datacenter and hence this mode is an L2 extension of corporate VLAN to remote site. Either the controller or an upstream router can be the gateway for the clients. Client traffic destined to datacenter resources is forwarded by the master Instant AP (through the IPsec tunnel) to the client's default gateway in the datacenter.

When an Instant AP registers with the controller, the controller automatically adds the VPN tunnel associated to this Instant AP into the VLAN multicast table. This allows the clients connecting to the L2 mode VLAN to be part of the same L2 broadcast domain on the controller.

Distributed, L3 Mode

The Distributed, L3 mode contains all broadcast and multicast traffic to a branch. The Distributed, L3 mode reduces the cost and eliminates the complexity associated with the classic site-to-site VPN. However, this mode is very similar to a classic site-to-site IPsec VPN where two VPN endpoints connect individual networks together over a public network.

In Distributed, L3 mode, each branch location is assigned a dedicated subnet. The master Instant AP in the branch manages the dedicated subnet and acts as the DHCP server and gateway for clients. Client traffic destined to datacenter resources is routed to the controller through the IPsec tunnel, which then routes the traffic to the appropriate corporate destinations.

When an Instant AP registers with the controller, the controller adds a route to enable the routing of traffic from the corporate network to clients on this subnet in the branch.

Centralized, L2 Mode

The Centralized, L2 mode extends the corporate VLAN or broadcast domain to remote branches. The DHCP server and the gateway for the clients reside in the datacenter. Either the controller or an upstream router can be the gateway for the clients. For DHCP services in Centralized, L2 mode, Aruba recommends using an external DHCP server and not the DHCP server on the controller. Client traffic destined to datacenter resources is forwarded by the master Instant AP (through the IPsec tunnel) to the client's default gateway in the datacenter.

Centralized, L3 Mode

For Centralized, L3 clients, the virtual controller acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located behind the controller in the corporate network and reachable through the IPsec tunnel. The Centralized, L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

DHCP Scope and VPN Forwarding Modes Mapping

The following table provides a summary of the DHCP scope and VPN forwarding modes mapping:

Table 144: *DHCP Scope and VPN Forwarding Modes Matrix*

Options	Local	Local, L2	Local, L3	Centralized, L2	Centralized, L3	Distributed, L2	Distributed, L3
DHCP server	Virtual controller	Virtual controller	Virtual controller	DHCP Server in the Datacenter	DHCP Server in the Datacenter and virtual controller acts as a relay agent	Virtual controller	Virtual controller
Default Gateway for clients	Virtual controller	Default Gateway in the local network	Virtual controller	Controller or a router in the Datacenter	Virtual controller	Controller or a router in the Datacenter	Virtual controller
Corporate Traffic	Source-NAT is performed with inner IP of the IPsec tunnel	Not applicable	Source-NAT is performed with inner IP of the IPsec tunnel	L2 reachable	Routed	L2 reachable	Routed
Internet Traffic	Source-NAT is performed with local IP of the Virtual controller	Locally bridged	Routed	CL2 full tunnel mode—ource-NAT is performed with local IP of controller or a router in the datacenter. CL2 split-tunnel mode—Source-NAT is performed with local IP of the Virtual controller	Source-NAT is performed with local IP of the Virtual controller	Source-NAT is performed with local IP of the Virtual controller	Source-NAT is performed with local IP of the Virtual controller

Options	Local	Local, L2	Local, L3	Centralized, L2	Centralized, L3	Distributed, L2	Distributed, L3
Branch access from datacenter	No	No	No	Yes	Yes	Yes	Yes

Configuring Instant AP and Controller for IAP-VPN Operations

This section describes the configuration procedures for the Instant AP and the controller to realize generic use cases. For information on specific deployment scenarios, see IAP-VPN Deployment Scenarios on page 346.

Points to Remember:

- To seamlessly process the register requests without causing service disruption, ensure that the Instant AP and managed device are both upgraded to the 8.4.0.0 software version respectively. However, it is highly important that you first upgrade the managed device to the 8.4.0.0 software version, enable backward compatibility on the managed device, and only then upgrade the Instant AP to the 8.4.0.0 software version.
- Also, you must not upgrade the Instant AP to the 8.4.0.0 software version first when the managed device, terminating on the IAP-VPN is running an older software version.
- IAP-VPN termination is not supported on ArubaOS Controller clusters.
- Instant APs running Instant 8.3.x.x or earlier versions can terminate IAP-VPN connections with controllers running ArubaOS 8.4.0.0 or later versions only if the backward compatibility feature is enabled on the controller.
- Instant APs running Instant 8.4.0.0 or later versions cannot terminate IAP-VPN connections with controllers running ArubaOS 8.3.x.x or earlier versions.

Configuring an Instant AP Network for IAP-VPN Operations

An Instant AP network requires the following configurations for IAP-VPN operations.

- Defining the VPN Host Settings
- Configuring Routing Profiles
- Configuring DHCP Profiles
- Configuring an SSID or Wired Port Profile
- Enabling Dynamic RADIUS Proxy
- Configuring Enterprise Domains
- Configuring Reconnect Duration for Controller Failover

Defining the VPN Host Settings

The VPN endpoint on which a master Instant AP terminates its VPN tunnel is considered as the host. A master Instant AP in an Instant AP network can be configured with a primary and backup host to provide VPN redundancy. You can define VPN host settings through **More > Tunneling > Controller** in the old WebUI and through **Configuration** > **Tunneling** > **Controller** in the new WebUI.

You can configure the following VPN profiles for the IAP-VPN operations. For more information, see Configuring a Tunnel from an Instant AP to a Mobility Controller on page 319.

- Aruba IPsec
- L2TPv3
- Manual GRE
- Aruba GRE

Configuring Routing Profiles

The routing profile on the Instant AP determines whether the traffic destined to a subnet must be tunneled through IPsec or bridged locally. If the routing profile is empty, the client traffic will always be bridged locally. For example, if the routing profile is configured to tunnel 10.0.0.0 /8, the traffic destined to 10.0.0.0 /8 will be forwarded through the IPsec tunnel and the traffic to all other destinations is bridged locally.

You can also configure a routing profile with 0.0.0.0 as gateway to allow both the client and Instant AP traffic to be routed through a non-tunnel route. If the gateway is in the same subnet as uplink IP address, it is used as a static gateway entry. A static route can be added to all master and slave Instant APs for these destinations. The VPN traffic from the local subnet of Instant AP or the Virtual controller IP address in the local subnet is not routed to tunnel, but will be switched to the relevant VLAN. For example, when a 0.0.0.0/0.0.0.0 routing profile is defined, to bypass certain IPs, you can add a route to the IP by defining 0.0.0.0 as the destination, thereby forcing the traffic to be routed through the default gateway of the Instant AP.

You can configure routing profiles through **More > Tunneling > Controller** in the old WebUI and through **Configuration** > **Routing** in the new WebUI. For step-by-step procedural information on configuring routing profile, see Configuring Routing Profiles on page 328.



The Instant AP network has only one active tunnel even when fast failover is enabled. At any given time, traffic can be tunneled only to one VPN host.

Configuring DHCP Profiles

You can create DHCP profiles to determine the IAP-VPN mode of operation. An Instant AP network can have multiple DHCP profiles configured for different modes of IAP-VPN. You can configure up to eight DHCP profiles. For more information on the IAP-VPN modes of operation, see IAP-VPN Forwarding Modes on page 333.

You can create any of the following types of DHCP profiles for the IAP-VPN operations:

- Local
- Local, L2
- Local, L3
- Distributed, L2
- Distributed, L3
- Centralized, L2
- Centralized, L3

For more information on configuring DHCP profiles, see Configuring DHCP Scopes on page 294.



A Centralized, L2 or Distributed, L2 VLAN or subnet cannot be used to serve Instant APs in a hierarchical mode of deployment. Ensure that the physical IP of the Instant APs connecting to the master Instant AP in hierarchical mode of deployment is not on a VLAN or subnet that is in Centralized, L2 or Distributed, L2 mode of operation. For information on hierarchical mode of deployment, see Understanding Hierarchical Deployment on page 173.

Configuring an SSID or Wired Port Profile

For a client to connect to the IAP-VPN network, an SSID or wired port profile on an Instant AP must be configured with appropriate IAP-VPN mode of operation. The VLAN configuration in an SSID or wired port profile determines whether an SSID or wired port is configured for the IAP-VPN operations.

To configure an SSID or wired port for a specific IAP-VPN mode, the VLAN ID defined in the SSID or wired port profile must match the VLAN ID defined in the DHCP profile configuration. If the VLAN assignment for an SSID or wired port profile is set to Virtual controller assigned, custom, or a static VLAN ID that does not match the VLAN ID configured in the DHCP profiles, the IAP-VPN operations are affected. For example, if a local DHCP profile is configured with a VLAN ID of 200, the VLAN configuration on the SSID must be set to a static VLAN ID 200.



Ensure that the VLAN assignment for an SSID or wired port profile is not set to default as the VPN tunnel is not supported on the default VLAN.

An Instant AP will not send a registration request to the controller if **SetMeUp** is configured on the Instant AP.

For information on how to configure an SSID or wired port profile, see Wireless Network Profiles on page 130 and Configuring a Wired Profile on page 161, respectively.

Enabling Dynamic RADIUS Proxy

The RADIUS server can be deployed at different locations and VLANs. In most cases, a centralized RADIUS or local server is used to authenticate users. However, some user networks can use a local RADIUS server for employee authentication and a centralized RADIUS-based captive portal server for guest authentication. To ensure that the RADIUS traffic is routed to the required RADIUS server, the dynamic RADIUS proxy feature must be enabled. When enabled, dynamic RADIUS proxy ensures that all the RADIUS traffic is sourced from the Virtual controller IP or inner IP of the Instant AP IPsec tunnel depending on the RADIUS server IP and routing profile.



Ensure that a static Virtual controller IP is configured before enabling dynamic RADIUS proxy in order to tunnel the RADIUS traffic to the central RADIUS server in the datacenter.

For information on enabling dynamic RADIUS proxy, see Configuring Dynamic RADIUS Proxy Parameters on page 239.

Configuring Enterprise Domains

By default, all the DNS requests from a client are forwarded to the client's DNS server. In a typical Instant AP deployment without VPN configuration, client DNS requests are resolved by the DNS server of clients. For the IAP-VPN scenario, the enterprise domain settings on the Instant AP are used to determine how client DNS requests are routed. For information on how to configure enterprise domains, see Configuring Enterprise Domains on page 274.

Configuring Reconnect Duration for Controller Failover

The connectivity of IAP-VPN connections is monitored using a heartbeat between the IAP and the terminating controller. The IAP sends a heartbeat to the controller every second. By default, the IAP fails over to the backup controller. When the heartbeat is not heard for 30 seconds, the connectivity to the controlleris considered broken and the Instant AP failovers to the backup controller.

The number of seconds the IAP attempts to reconnect to the controller can be configured using the **vpn reconnect duration** command. This duration takes effect only when fast failover is not enabled on the Instant AP and applies to non-default VPN profiles.This is a configuration mode command and can configured only using the CLI.

Use the following syntax to configure the vpn reconnect duration, **vpn reconnect-duration <1-3600>**, value in seconds. Default value is 30.

```
(Instant AP) # configure terminal
(Instant AP) (config) # vpn reconnect-duration <1-3600>
```

Configuring a Controller for IAP-VPN Operations

Instant Controllers provide an ability to terminate the IPsec and GRE VPN tunnels from the Instant AP and provide corporate connectivity to the branch network. This section describes the configuration procedures for the controller to realize generic use cases. For information on specific deployment scenarios, see IAP-VPN Deployment Scenarios on page 346.

For IAP-VPN operations, ensure that the following configuration and verification procedures are completed on the controller:

- OSPF Configuration
- VPN Configuration
- Branch-ID Allocation
- Branch Status Verification

OSPF Configuration

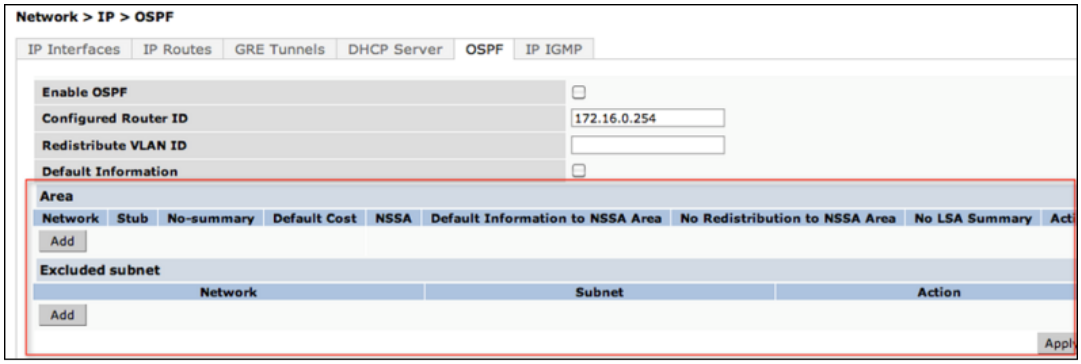
OSPF is a dynamic IGP based on IETF RFC 2328. The premise of OSPF is that the shortest or fastest routing path is used. The implementation of OSPFv2 allows controllers to deploy effectively in a Layer 3 topology. The controllers can act as the default gateway for all clients and forward user packets to the upstream router.

Each IAP-VPN can be defined a separate subnet derived from the corporate intranet pool to allow IAP-VPN devices to work independently. For sample topology , refer to the *ArubaOS User Guide*.

To configure general OSPF settings from the controller, perform the following steps:

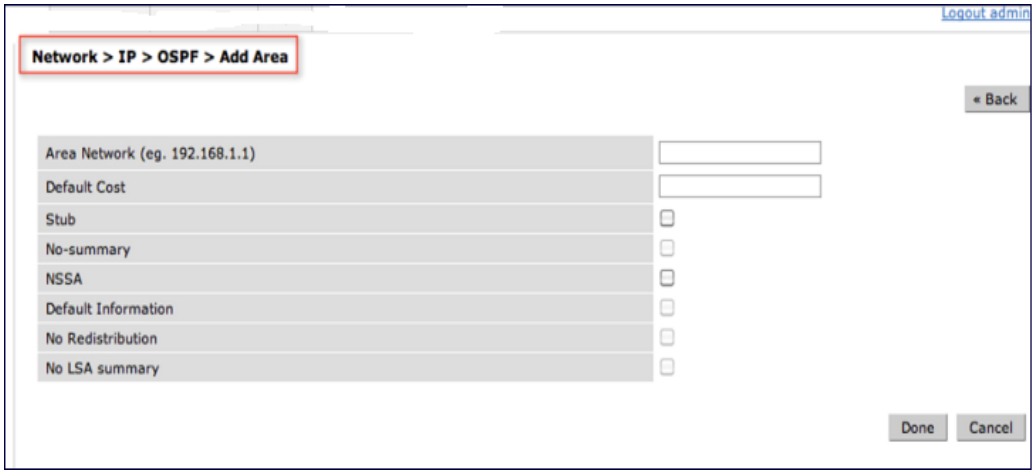
1. Navigate to the **Configuration > IP** page. The Area and Excluded subnets are displayed in table format. If not explicitly specified for OSPF, the router ID defaults to the switch IP.

Figure 8 *General OSPF Configuration*



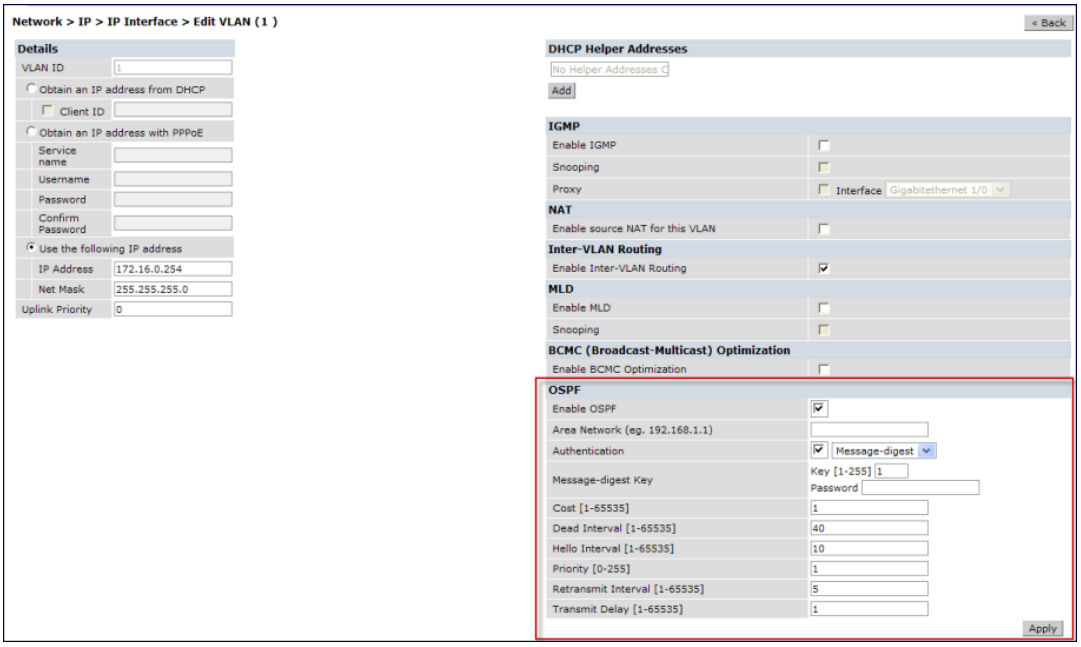
2. Click **Add** to add an area.

Figure 9 *Add an OSPF Area*



3. Configure the OSPF interface settings in the Configuration screen. If OSPF is enabled, the parameters contain the correct default values. You can edit the OSPF values only when you enable OSPF on the interface.

Figure 10 *Edit OSPF VLAN Settings*



OSPF monitoring is available from an IP Routing sub-section (**Controller > IP Routing > Routing**). Both Static and OSPF routes are available in table format.

OSPF Interfaces and Neighboring information is available from the **OSPF** tab. The Interface information includes transmit (TX) and receive (RX) statistics.

The following CLI command redistributes IAP-VPN routes into the OSPF process:

```
(host)(config) # router ospf redistribute rapng-vpn
```

The following CLI command verifies if the redistribution of the IAP-VPN is enabled:

```
(host) #show ip ospf redistribute
```

The following CLI command configures aggregate route for IAP-VPN routes:

```
(host)(config) # router ospf aggregate-route rapng-vpn
```

The following CLI command views the aggregated routes for IAP-VPN routes:

```
(host) #show ip ospf rapng-vpn aggregate-routes
RAPNG VPN aggregate routes
--------------------------
Prefix Mask Contributing routes Cost
------ ---- ------------------- ----
201.201.200.0 255.255.252.0 5 268779624
100.100.2.0 255.255.255.0 1 10
The following CLI command verifies the details of a configured aggregated route:
(host) # show ip ospf rapng-vpn aggregated-routes <net> <mask>
(host) # show ip ospf rapng-vpn aggregate-routes 100.100.2.0 255.255.255.0
Contributing routes of RAPNG VPN aggregate route
------------------------------------------------
Prefix Mask Next-Hop Cost
------ ---- -------- ----
100.100.2.64 255.255.255.224 5.5.0.10 10
```

The following CLI command shows all the redistributed routes:

```
(host)# show ip ospf database
```

```
OSPF Database Table
-------------------
Area ID    LSA Type      Link ID        Adv Router     Age   Seq#         Checksum
-------    --------      -------        ----------     ---   ----         --------
0.0.0.15   ROUTER        9.9.9.9        9.9.9.9        159   0x80000016   0xee92
0.0.0.15   ROUTER        10.15.148.12   10.15.148.12   166   0x80000016   0x4c0d
0.0.0.15   NETWORK       10.15.148.12   10.15.148.12   167   0x80000001   0x9674
0.0.0.15   NSSA          12.12.2.0      9.9.9.9        29    0x80000003   0x7b54
0.0.0.15   NSSA          12.12.12.0     9.9.9.9        164   0x80000008   0x63a
0.0.0.15   NSSA          12.12.12.32    9.9.9.9        164   0x80000008   0x7b8
0.0.0.15   NSSA          50.40.40.0     9.9.9.9        164   0x80000007   0x8ed4
0.0.0.15   NSSA          51.41.41.128   9.9.9.9        164   0x80000007   0x68f6
0.0.0.15   NSSA          53.43.43.32    9.9.9.9        164   0x80000007   0x2633
0.0.0.15   NSSA          54.44.44.16    9.9.9.9        164   0x80000007   0x353
N/A        AS_EXTERNAL   12.12.2.0      9.9.9.9        29    0x80000003   0x8c06
N/A        AS_EXTERNAL   12.12.12.0     9.9.9.9        169   0x80000001   0x25e4
N/A        AS_EXTERNAL   12.12.12.32    9.9.9.9        169   0x80000001   0x2663
N/A        AS_EXTERNAL   50.40.40.0     9.9.9.9        169   0x80000001   0xab80
N/A        AS_EXTERNAL   51.41.41.128   9.9.9.9        169   0x80000001   0x85a2
N/A        AS_EXTERNAL   53.43.43.32    9.9.9.9        169   0x80000001   0x43de
N/A        AS_EXTERNAL   54.44.44.16    9.9.9.9        169   0x80000001   0x20fe
```

The following CLI command verifies if the redistributed routes are installed or not:

```
(host)# show ip route
Codes: C - connected, O - OSPF, R - RIP, S - static
M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN
Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10
Gateway of last resort is 10.15.148.254 to network 0.0.0.0 at cost 1
S*    0.0.0.0/0  [1/0] via 10.15.148.254*
V    12.12.2.0/24 [10/0] ipsec map
V    12.12.12.0/25 [10/0] ipsec map
V    12.12.12.32/27 [10/0] ipsec map
V    50.40.40.0/24 [10/0] ipsec map
V    51.41.41.128/25 [10/0] ipsec map
V    53.43.43.32/27 [10/0] ipsec map
V    54.44.44.16/28 [10/0] ipsec map
C    9.9.9.0/24 is directly connected, VLAN9
C    10.15.148.0/24 is directly connected, VLAN1
C    43.43.43.0/24 is directly connected, VLAN132
C    42.42.42.0/24 is directly connected, VLAN123
C    44.44.44.0/24 is directly connected, VLAN125
C    182.82.82.12/32 is an ipsec map 10.15.149.69-182.82.82.12
C    182.82.82.14/32 is an ipsec map 10.17.87.126-182.82.82.14
```

VPN Configuration

The following VPN configuration steps on the controller enable the Instant APs to terminate their VPN connection on the controller:

Whitelist Database Configuration

The whitelist database is a list of the MAC addresses of the Instant APs that are allowed to establish VPN connections with the controller. This list can be either stored in the controller database or on an external server.

The following CLI command configures the whitelist database entries if the controller is acting as the whitelist database:

```
(host)# whitelist-db rap add mac-address 00:11:22:33:44:55 ap-group test
```

The **ap-group** parameter is not used for any configuration, but needs to be configured. The parameter can be any valid string.

If an external server is used as the location for the whitelist database, add the MAC addresses of the valid Instant APs in the external database or external directory server and then configure a RADIUS server to authenticate the Instant APs using the entries in the external database or external directory server.

If you are using the Windows 2003 server, perform the following steps to configure the external whitelist database on it. There are equivalent steps available for the Windows Server 2008 and other RADIUS servers.

1. Add the MAC addresses of all the Instant APs in the Active Directory of the RADIUS server:
   a. Open the **Active Directory and Computers** window, add a new user and specify the MAC address (without the colon delimiter) of the Instant AP for the username and password, respectively.
   b. Right-click the user that you have just created and click **Properties**.
   c. On the **Dial-in** tab, select **Allow access** in the **Remote Access Permission** section and click **OK**.
   d. Repeat Step a through Step c for all Instant APs.
2. Define the remote access policy in the IAS:
   a. In the **Internet Authentication Service** window, select **Remote Access Policies**.
   b. Launch the wizard to configure a new remote access policy.
   c. Define filters and select **grant remote access permission** in the **Permissions** window.
   d. Right-click the policy that you have just created and select **Properties**.
   e. In the **Settings** tab, select the policy condition, and click **Edit Profile**.
   f. In the **Advanced** tab, select **Vendor Specific**, and click **Add** to add a new VSAs.
   g. Add a new VSA and click **OK**.
   h. In the **IP** tab, provide the IP address of the Instant AP and click **OK**.

If you have locally managed Instant APs, then these Instant APs must be allowlisted to establish VPN connections.

The following command can be used to configure an IAP-VPN branch as trusted:

```
(host) (config) #iap trusted-branch-db add mac-address 01:01:0e:3e:4c:33
Trusted branch added
```

The following command configures all IAP-VPN branches as trusted:

```
(host) [mynode] #iap trusted-branch-db allow-all
All IAP+VPN branches are trusted
(host) # ip local pool "rapngpool" <startip> <endip>
```

VPN Local Pool Configuration

The VPN local pool is used to assign an IP address to the Instant AP after successful XAUTH VPN.

```
(host) # ip local pool "rapngpool" <startip> <endip>
```

Role Assignment for the Authenticated Instant APs

Define a role that includes an Source-NAT rule to allow connections to the RADIUS server and for the Dynamic RADIUS Proxy in the Instant AP to work. This role is assigned to Instant APs after successful authentication.

```
(host) (config) #ip access-list session iaprole
(host) (config-sess-iaprole)#any host <radius-server-ip> any src-nat
(host) (config-sess-iaprole)#any any any permit
(host) (config-sess-iaprole)#!
(host) (config) #user-role iaprole
(host) (config-role) #session-acl iaprole
```

VPN Profile Configuration

The VPN profile configuration defines the server used to authenticate the Instant AP (internal or an external server) and the role assigned to the Instant AP after successful authentication.

```
(host) (config) #aaa authentication vpn default-iap
(host) (VPN Authentication Profile "default-iap") #server-group default
(host) (VPN Authentication Profile "default-iap") #default-role iaprole
```

Branch-ID Allocation

For branches deployed in Distributed, L3 and Distributed, L2 modes, the master Instant AP in the branch and the controller should agree upon a subnet or IP addresses to be used for DHCP services in the branch. The process or protocol used by the master Instant AP and the controller to determine the subnet or IP addresses used in a branch is called BID allocation. The BID allocation process is not essential for branches deployed in local or Centralized, L2 mode. The following are some of the key functions of the BID allocation process:

- Determines the IP addresses used in a branch for Distributed, L2 mode
- Determines the subnet used in a branch for Distributed, L3 mode
- Avoids IP address or subnet overlap (that is, avoids IP conflict)
- Ensures that a branch is allocated the same subnet or range of IP addresses irrespective of which Instant AP in the branch becomes the master in the Instant AP cluster

Branch Status Verification

To view the details of the branch information connected to the controller, execute the **show iap table** command. This example shows the details of the branches connected to the controller:

```
(host) #show iap table long

IAP Branch Table
----------------
Name              VC MAC Address     Status   Inner IP       Assigned Subnet  Assigned
Vlan
----              --------------     ------   --------       ---------------  ---------
----
Tokyo-CB:D3:16    6c:f3:7f:cc:42:f8  DOWN     0.0.0.0

Paris-CB:D3:16    6c:f3:7f:cc:3d:04  UP       10.15.207.140  10.15.206.99/29  2
LA                6c:f3:7f:cc:42:25  UP       10.15.207.111  10.15.206.24/29  2
Munich            d8:c7:c8:cb:d3:16  DOWN     0.0.0.0

London-c0:e1      6c:f3:7f:c0:e1:b1  UP       10.15.207.120  10.15.206.64/29  2
Instant-CB:D3     6c:f3:7f:cc:42:1e  DOWN     0.0.0.0

Delhi             6c:f3:7f:cc:42:ca  DOWN     0.0.0.0

Singapore         6c:f3:7f:cc:42:cb  UP       10.15.207.122  10.15.206.120/29 2
```

```
Key         Bid(Subnet Name)
---         ----------------
b3c65c...
b3c65c...
b3c65c...   2(10.15.205.0-10.15.205.250,5),1(10.15.206.1-10.15.206.252,5)
a2a65c...   0
b3c65c...   7(10.15.205.0-10.15.205.250,5),8(10.15.206.1-10.15.206.252,5)
b3c65c...
b3c65c...   1(10.15.205.0-10.15.205.250,5),2(10.15.206.1-10.15.206.252,5)
b3c65c...   14(10.15.205.0-10.15.205.250,5),15(10.15.206.1-10.15.206.252,5)
```

The output of this command provides the following information:

Table 145: *Branch Details*

Parameter	Description
Name	Displays the name of the branch.
VC MAC Address	Displays the MAC address of the virtual controller of the branch.
Status	Displays the current status of the branch (UP or DOWN).
Inner IP	Displays the internal VPN IP of the branch.
Assigned Subnet	Displays the subnet mask assigned to the branch.
Assigned Vlan	Displays the VLAN ID assigned to the branch.
Key	Displays the key for the branch, which is unique to each branch.
Bid(Subnet Name)	Displays the branch ID of the subnet. In the example above, the controller displays bid-per-subnet-per-branch i.e., for "LA" branch, BID "2" for the ip-range "10.15.205.0-10.15.205.250" with client count per branch "5"). If a branch has multiple subnets, it can have multiple BIDs. If a branch is in **UP** state and does not have a **Bid(Subnet Name)**, it means that the Instant AP is connected to a controller, which did not assign any BID for any subnet. In the above example, "Paris-CB:D3:16" branch is **UP** and does not have a **Bid(Subnet Name)**. This means that either the Instant AP is connected to a backup controller or it is connected to a primary controller without any Distributed, L2 or Distributed, L3 subnets.



The **show iap table** command output does not display the **Key** and **Bid(Subnet Name)** details.

IAP-VPN Termination on Mobility Controller Virtual Appliance

Starting from ArubaInstant 8.3.0.0, IAP-VPN is supported on Mobility Controller Virtual Appliance by using default self-signed certificate (Aruba PKI). For Instant AP to establish IPsec connection with Mobility Controller Virtual Appliance, the controller presents a default self-signed certificate which is uploaded on the Instant AP using Activate.

To terminate IAP-VPN connections on a Mobility Controller Virtual Appliance , the default self signed certificate or Trust Anchor (TA) certificate of the Virtual Mobility Controller in the case of standalone controllers or the TA certificate of the Virtual Mobility Master that manages the Virtual Mobility Controller must be uploaded to the IAP to authneticate the identity of the Mobility Controller Virtual

Appliance and establish an IPsec tunnel. The Trust Anchor certificate must be uploaded to Activate which will then be sent to the IAP, to authenticate and establish an IPsec tunnel to virtual controller.

For information on uploading and managing TA certficates on Activate for IAP-VPN termination on Mobility Controller Virtual Appliances, see Aruba Activate APIs section in the Aruba Activate User Guide.



Mobility Masters (Mobility Master Hardware Appliance, Mobility Master Virtual Appliance, and Master Controller Mode) do not support any AP termination including Campus APs, Remote APs and IAP-VPN tunnels.

Through Activate, you can push only one default self-signed certificate to Instant AP which can be used to establish IPsec tunnel with Mobility Controller Virtual Appliance.

IAP-VPN Deployment Scenarios

This section describes the most common IAP-VPN deployment models and provides information to carry out the necessary configuration procedures. The examples in this section refer to more than one DHCP profile and wired port configuration in addition to wireless SSID configuration. All these are optional. In most networks, a single DHCP profile and wireless SSID configuration referring to a DHCP profile is sufficient.

The following scenarios are described in this section:

- Scenario 1—IPsec: Single Datacenter Deployment with No Redundancy on page 346
- Scenario 2—IPsec: Single Datacenter with Multiple Controller for Redundancy on page 351
- Scenario 3—IPsec: Multiple Datacenter Deployment with Primary and Backup Controller for Redundancy on page 356
- Scenario 4—GRE: Single Datacenter Deployment with No Redundancy on page 363

Scenario 1—IPsec: Single Datacenter Deployment with No Redundancy

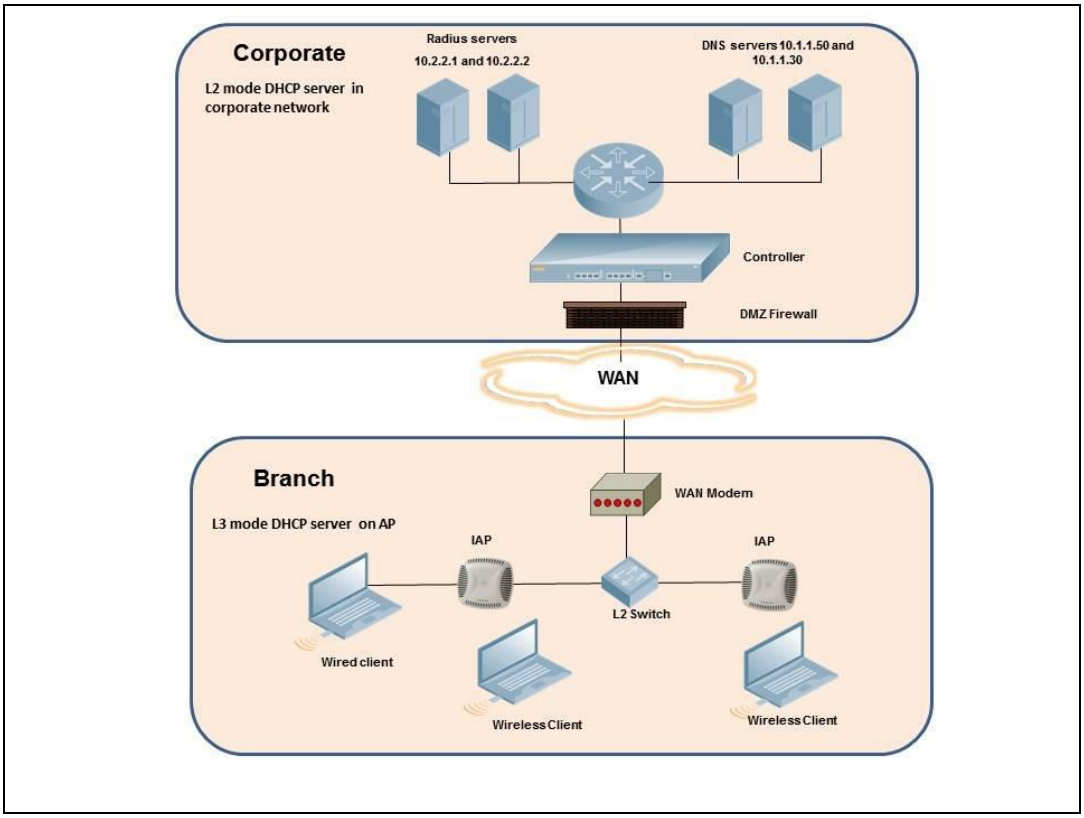
This scenario includes the following configuration elements:

1. Single VPN primary configuration using IPsec.
2. Split-tunneling of client traffic.
3. Split-tunneling of DNS traffic from clients.
4. Distributed, L3 and Centralized, L2 mode DHCP.
5. RADIUS server within corporate network and authentication survivability for branch survivability.
6. Wired and wireless users in L2 and L3 modes, respectively.
7. Access rules defined for wired and wireless networks to permit all traffic.

Topology

Figure 11 shows the topology and the IP addressing scheme used in this scenario.

Figure 11 *Scenario 1—IPsec: Single datacenter Deployment with No Redundancy*



The following IP addresses are used in the examples for this scenario:

- 10.0.0.0/8 is the corporate network
- 10.20.0.0/16 subnet is reserved for L2 mode
- 10.30.0.0/16 subnet is reserved for L3 mode
- Client count in each branch is 200

Instant AP Configuration

The following table provides information on the configuration steps performed through the CLI with example values. For information on the WebUI procedures, see the topics referenced in the *WebUI Procedure* column.

Table 146: *Instant AP Configuration for Scenario 1—IPsec: Single Datacenter Deployment with No Redundancy*

Configuration Steps	CLI Commands	WebUI Procedure
Configure the primary host for VPN with the Public VRRP IP address of the controller.	▪ `(Instant AP)(config)# vpn primary <public VRRP IP of` controller>	See Configuring an IPsec Tunnel
Configure a routing profile to tunnel all 10.0.0.0/8 subnet traffic to controller.	▪ `(Instant AP)(config)# routing-profile` ▪ `(Instant AP)(routing-profile)# route 10.0.0.0 255.0.0.0 <public VRRP IP of`	See Configuring Routing Profiles

Table 146: *Instant AP Configuration for Scenario 1—IPsec: Single Datacenter Deployment with No Redundancy*

Configuration Steps	CLI Commands	WebUI Procedure
	controller>	
Configure Enterprise DNS for split DNS. The example in the next column uses a specific enterprise domain to only tunnel all DNS queries matching that domain to corporate.	▪ `(Instant AP)(config)# internal-domains` ▪ `(Instant AP)(domains)# domain-name corpdomain.com`	See Configuring Enterprise Domains
Configure Centralized, L2 and Distributed, L3 with VLAN 20 and VLAN 30, respectively.	**Centralized, L2 profile** ▪ `(Instant AP)(config)# ip dhcp l2-dhcp` ▪ `(Instant AP)(DHCP Profile "l2-dhcp")# server-type Centralized,L2` ▪ `(Instant AP)(DHCP Profile "l2-dhcp")# server-vlan 20` **Distributed, L3 profile** ▪ `(Instant AP)(config)# ip dhcp l3-dhcp` ▪ `(Instant AP)(DHCP Profile "l3-dhcp")# server-type Distributed,L3` ▪ `(Instant AP)(DHCP Profile "l3-dhcp")# server-vlan 30` ▪ `(Instant AP)(DHCP Profile "l3-dhcp")# ip-range 10.30.0.0 10.30.255.255` ▪ `(Instant AP)(DHCP Profile "l3-dhcp")# dns-server 10.1.1.50,10.1.1.30` ▪ `(Instant AP)(DHCP Profile "l3-dhcp")# domain-name corpdomain.com` ▪ `(Instant AP)(DHCP Profile "l3-dhcp")# client-count 200` **NOTE:** The IP range configuration on each branch will be the same. Each Instant AP will derive a smaller subnet based on the client count scope using the BID allocated by controller.	See Enabling DHCP Relay Agent Information Option (Option 82) and Configuring Distributed DHCP Scopes
Create authentication servers for user authentication. The example in the next column assumes 802.1X SSID.	▪ `(Instant AP)(config)# wlan auth-server server1` ▪ `(Instant AP)(Auth Server`	See Configuring an External Server for Authentication

Table 146: *Instant AP Configuration for Scenario 1—IPsec: Single Datacenter Deployment with No Redundancy*

Configuration Steps	CLI Commands	WebUI Procedure
	"server1")# ip 10.2.2.1 ■ (Instant AP)(Auth Server "server1")# port 1812 ■ (Instant AP)(Auth Server "server1")# acctport 1813 ■ (Instant AP)(Auth Server "server1")# key "presharedkey" ■ (Instant AP)(Auth Server "server1")# exit ■ (Instant AP)(config)# wlan auth-server server2 ■ (Instant AP)(Auth Server "server2")# ip 10.2.2.2 ■ (Instant AP)(Auth Server "server2")# port 1812 ■ (Instant AP)(Auth Server "server2")# acctport 1813 ■ (Instant AP)(Auth Server "server2")# key "presharedkey"	
Configure wired port and wireless SSIDs using the authentication servers.	Configure wired ports to operate in L2 mode and associate Centralized, L2 mode VLAN 20 to the wired port profile. ■ (Instant AP)(config) # wired-port-profile wired-port ■ (Instant AP)(wired-port-profile "wired-port")# switchport-mode access ■ (Instant AP)(wired-port-profile "wired-port")# allowed-vlan all ■ (Instant AP)(wired-port-profile "wired-port")# native-vlan 20 ■ (Instant AP)(wired-port-profile "wired-port")# no shutdown ■ (Instant AP)(wired-port-profile "wired-port")# access-rule-name wired-port ■ (Instant AP)(wired-port-profile "wired-port")# type	See Configuring a Wired Profile and Wireless Network Profiles

Table 146: *Instant AP Configuration for Scenario 1—IPsec: Single Datacenter Deployment with No Redundancy*

Configuration Steps	CLI Commands	WebUI Procedure
	employee ■ (Instant AP)(wired-port-profile "wired-port")# auth-server server1 ■ (Instant AP)(wired-port-profile "wired-port")# auth-server server2 ■ (Instant AP)(wired-port-profile "wired-port")# dot1x ■ (Instant AP)(wired-port-profile "wired-port")# exit ■ (Instant AP)(config)# enet1-port-profile wired-port Configure a wireless SSID to operate in L3 mode and associate Distributed, L3 mode VLAN 30 to the WLAN SSID profile. ■ (Instant AP)(config) # wlan ssid-profile wireless-ssid ■ (Instant AP)(SSID Profile "wireless-ssid")# enable ■ (Instant AP)(SSID Profile "wireless-ssid")# type employee ■ (Instant AP)(SSID Profile "wireless-ssid")# essid wireless-ssid ■ (Instant AP)(SSID Profile "wireless-ssid")# opmode wpa2-aes ■ (Instant AP)(SSID Profile "wireless-ssid")# vlan 30 ■ (Instant AP)(SSID Profile "wireless-ssid")# auth-server server1 ■ (Instant AP)(SSID Profile "wireless-ssid")# auth-server server2 ■ (Instant AP)(SSID Profile "wireless-ssid")# auth-survivability	
Create access rule for wired and wireless authentication. In this example, the rule permits all traffic.	**For wired profile:** ■ (Instant AP)(config)# wlan access-rule wired-port	See Configuring ACL Rules for Network Services

Table 146: *Instant AP Configuration for Scenario 1—IPsec: Single Datacenter Deployment with No Redundancy*

Configuration Steps	CLI Commands	WebUI Procedure
	▪ `(Instant AP)(Access Rule "wired-port")# rule any any match any any any permit` **For WLAN SSID:** ▪ `(Instant AP)(config)# wlan access-rule wireless-ssid` ▪ `(Instant AP)(Access Rule "wireless-ssid")# rule any any match any any any permit`	
NOTE: Ensure that you execute the **commit apply** command in the Instant CLI before saving the configuration and propagating changes across the Instant AP cluster.		

Instant AP-Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multiple Instant AP deployments, as client traffic from the slave to the master is tagged with the client VLAN.

Datacenter Configuration

For information on controller configuration, see Configuring a Controller for IAP-VPN Operations on page 339. Ensure that the upstream router is configured with a static route pointing to the controller for the L3 VLAN.

Scenario 2—IPsec: Single Datacenter with Multiple Controller for Redundancy

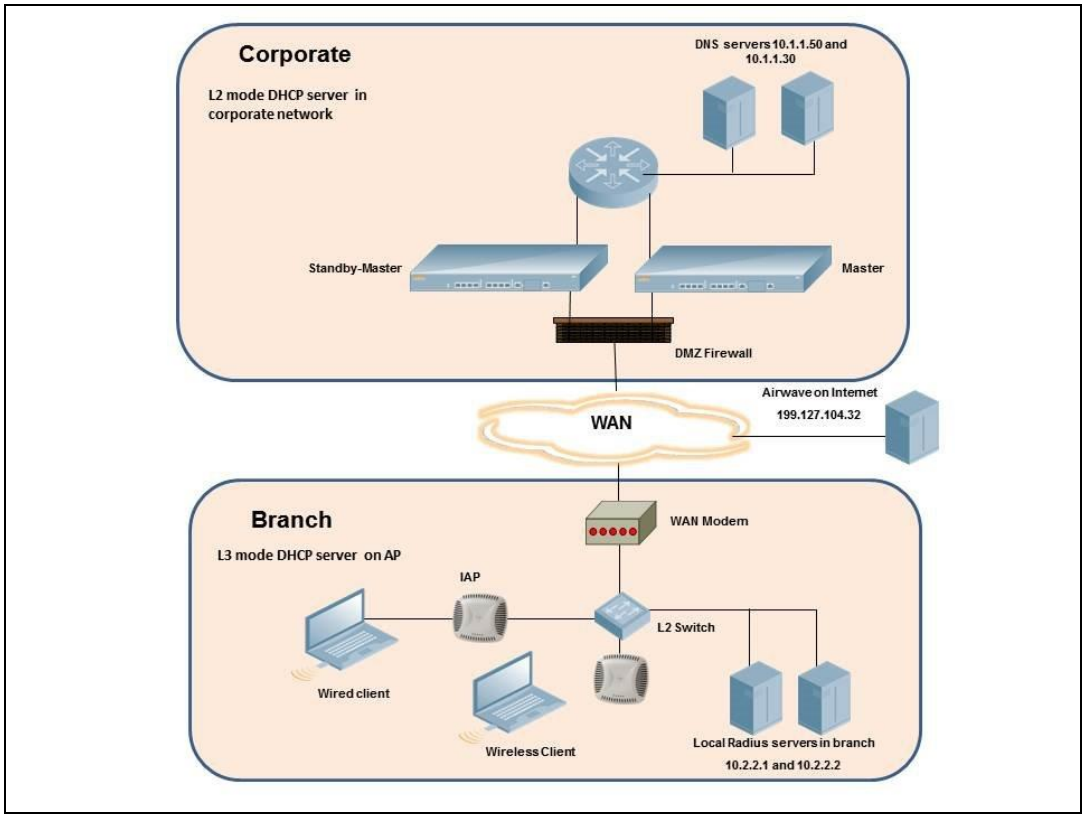
This scenario includes the following configuration elements:

- A VRRP instance between the master or standby-master pair, which is configured as the primary VPN IP address.
- Tunneling of all traffic to datacenter.
- Exception route to bypass tunneling of RADIUS and AirWave traffic, which are locally reachable in the branch and the Internet, respectively.
- All client DNS queries are tunneled to the controller.
- Distributed, L3 and Centralized, L2 mode DHCP on all branches. L3 is used by the employee network and L2 is used by the guest network with captive portal.
- Wired and wireless users in L2 and L3 modes.
- Access rules defined for wired and wireless networks.

Topology

Figure 12 shows the topology and the IP addressing scheme used in this scenario.

Figure 12 *Scenario 2—IPsec: Single Datacenter with Multiple Controllers for Redundancy*



The following IP addresses are used in the examples for this scenario:

- 10.0.0.0/8 is the corporate network
- 10.20.0.0/16 subnet is reserved for L2 mode – used for guest network
- 10.30.0.0/16 subnet is reserved for L3 mode
- Client count in each branch is 200
- 10.2.2.0/24 is a branch-owned subnet, which needs to override global routing profile
- 199.127.104.32 is used an example IP address of the AirWave server in the Internet

Instant AP Configuration

The following table provides information on the configuration steps performed through the CLI with example values. For information on the UI procedures, see the topics referenced in the *UI Procedure* column.

Table 147: *Instant AP Configuration for Scenario 2—IPsec: Single Datacenter with Multiple Controllers for Redundancy*

Configuration Steps	CLI Commands	WebUI Procedure
1. Configure the primary host for VPN with the Public VRRP IP address of the controller.	▪ `(Instant AP)(config)# vpn primary <public VRRP IP of controller>`	See Configuring an IPsec Tunnel
2. Configure routing profiles to tunnel traffic through IPsec.	▪ `(Instant AP)(config)# routing-`	See Configuring Routing Profiles

Table 147: *Instant AP Configuration for Scenario 2—IPsec: Single Datacenter with Multiple Controllers for Redundancy*

Configuration Steps	CLI Commands	WebUI Procedure
	profile ■ (Instant AP)(routing-profile)# route 0.0.0.0 0.0.0.0 <public VRRP IP of controller>	
3. Define routing profile exception RADIUS server and AirWave IPs, since the design requirement for this solution requires local RADIUS authentication, even though the IP matches the routing profile destination.	■ (Instant AP)(config)# routing-profile ■ (Instant AP)(routing-profile)# route 10.2.2.1 255.255.255.255 0.0.0.0 ■ (Instant AP)(routing-profile)# route 10.2.2.2 255.255.255.255 0.0.0.0 ■ (Instant AP)(routing-profile)# route 199.127.104.32 255.255.255.255 0.0.0.0	See Configuring Routing Profiles
4. Configure Enterprise DNS. The configuration example in the next column tunnels all DNS queries to the original DNS server of clients without proxying on Instant AP.	■ (Instant AP)(config)# internal-domains ■ (Instant AP)(domains)# domain-name *	See Configuring Enterprise Domains
5. Configure Centralized, L2 and Distributed, L3 with VLAN 20 and VLAN 30, respectively.	**Centralized, L2 profile** ■ (Instant AP)(config)# ip dhcp l2-dhcp ■ (Instant AP)(DHCP Profile "l2-dhcp")# server-type Centralized,L2 ■ (Instant AP)(DHCP Profile "l2-dhcp")# server-vlan 20 **Distributed, L3 profile** ■ (Instant AP)(config)# ip dhcp l3-dhcp ■ (Instant AP)(DHCP Profile "l3-dhcp")# server-type Distributed,L3 ■ (Instant AP)(DHCP Profile "l3-dhcp")# server-vlan 30 ■ (Instant AP)(DHCP Profile "l3-dhcp")# ip-range 10.30.0.0 10.30.255.255 ■ (Instant AP)(DHCP Profile "l3-dhcp")# dns-server 10.1.1.50,10.1.1.30	See Enabling DHCP Relay Agent Information Option (Option 82) and Configuring Distributed DHCP Scopes

Table 147: *Instant AP Configuration for Scenario 2—IPsec: Single Datacenter with Multiple Controllers for Redundancy*

Configuration Steps	CLI Commands	WebUI Procedure
	■ `(Instant AP)(DHCP Profile "l3-dhcp")# domain-name corpdomain.com` ■ `(Instant AP)(DHCP Profile "l3-dhcp")# client-count 200` **NOTE:** The IP range configuration on each branch will be the same. Each Instant AP will derive a smaller subnet based on the client count scope using the BID allocated by controller.	
6. Create authentication servers for user authentication. The example in the next column assumes 802.1X SSID.	■ `(Instant AP)(config)# wlan auth-server server1` ■ `(Instant AP)(Auth Server "server1")# ip 10.2.2.1` ■ `(Instant AP)(Auth Server "server1")# port 1812` ■ `(Instant AP)(Auth Server "server1")# acctport 1813` ■ `(Instant AP)(Auth Server "server1")# key "presharedkey"` ■ `(Instant AP)(Auth Server "server1")# exit` ■ `(Instant AP)(config)# wlan auth-server server2` ■ `(Instant AP)(Auth Server "server2")# ip 10.2.2.2` ■ `(Instant AP)(Auth Server "server2")# port 1812` ■ `(Instant AP)(Auth Server "server2")# acctport 1813` ■ `(Instant AP)(Auth Server "server2")# key "presharedkey"`	See Configuring an External Server for Authentication
7. Configure wired port and wireless SSIDs using the authentication servers.	Configure wired ports to operate in L3 mode and associate Distributed, L3 mode VLAN 30 to the wired port profile. ■ `(Instant AP)(config) # wired-port-profile wired-port` ■ `(Instant AP)(wired-port-profile "wired-port")# switchport-mode access` ■ `(Instant AP)(wired-port-profile`	See Configuring a Wired Profile and Wireless Network Profiles

Table 147: *Instant AP Configuration for Scenario 2—IPsec: Single Datacenter with Multiple Controllers for Redundancy*

Configuration Steps	CLI Commands	WebUI Procedure
	"wired-port")# allowed-vlan all ■ (Instant AP)(wired-port-profile "wired-port")# native-vlan 30 ■ (Instant AP)(wired-port-profile "wired-port")# no shutdown ■ (Instant AP)(wired-port-profile "wired-port")# access-rule-name wired-port ■ (Instant AP)(wired-port-profile "wired-port")# type employee ■ (Instant AP)(wired-port-profile "wired-port")# auth-server server1 ■ (Instant AP)(wired-port-profile "wired-port")# auth-server server2 ■ (Instant AP)(wired-port-profile "wired-port")# dot1x ■ (Instant AP)(wired-port-profile "wired-port")# exit ■ (Instant AP)(config)# enet1-port-profile wired-port Configure a wireless SSID to operate in L2 mode and associate Centralized, L2 mode VLAN 20 to the WLAN SSID profile. ■ (Instant AP)(config) # wlan ssid-profile guest ■ (Instant AP)(SSID Profile "guest")#enable ■ (Instant AP)(SSID Profile "guest")# type guest ■ (Instant AP)(SSID Profile "guest")# essid guest ■ (Instant AP)(SSID Profile "guest")# opmode opensystem ■ (Instant AP)(SSID Profile "guest")# vlan 20 ■ (Instant AP)(SSID Profile "guest")# auth-server server1 ■ (Instant AP)(SSID Profile "guest")# auth-server server2 ■ (Instant AP)(SSID Profile "guest")# captive-portal internal	

Table 147: *Instant AP Configuration for Scenario 2—IPsec: Single Datacenter with Multiple Controllers for Redundancy*

Configuration Steps	CLI Commands	WebUI Procedure
	NOTE: ■ This example uses internal captive portal use case using external authentication server. You can also use an external captive portal example. ■ The SSID type **guest** is used in this example to enable configuration of captive portal. However, corporate access through VPN tunnel is still allowed for this SSID because the VLAN associated to this SSID is a VPN-enabled VLAN (20 in this example).	
8. Create access rule for wired and wireless authentication. In this example, the rule permits all traffic.	**For wired profile:** ■ `(Instant AP)(config)# wlan access-rule wired-port` ■ `(Instant AP)(Access Rule "wired-port")# rule any any match any any any permit` **For WLAN SSID:** ■ `(Instant AP)(config)# wlan access-rule guest` ■ `(Instant AP)(Access Rule "guest")# rule any any match any any any permit`	See Configuring ACL Rules for Network Services
NOTE: Ensure that you execute the **commit apply** command in the Instant CLI before saving the configuration and propagating changes across the Instant AP cluster.		

Instant AP-Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multiple Instant AP deployments, as client traffic from the slave to the master is tagged with the client VLAN.

Datacenter Configuration

For information on controller configuration, see Configuring a Controller for IAP-VPN Operations on page 339. Ensure that the upstream router is configured with a static route pointing to the controller for the L3 VLAN.

Scenario 3—IPsec: Multiple Datacenter Deployment with Primary and Backup Controller for Redundancy

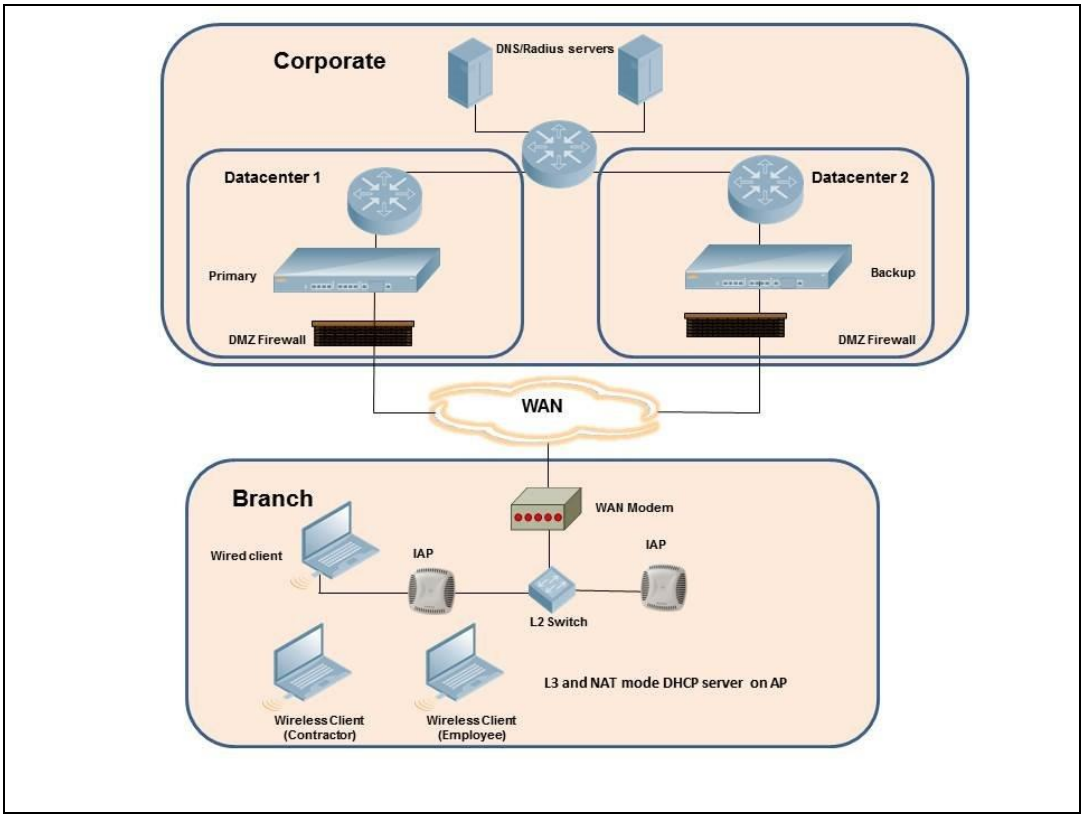
This scenario includes the following configuration elements:

- Multiple controller deployment model with Controllers in different data centers operating as primary or backup VPN with **Fast Failover** and preemption enabled.
- Split-tunneling of traffic.
- Split-tunneling of client DNS traffic.
- Two Distributed, L3 mode DHCPs, one each for employee and contractors; and one Local mode DHCP server.
- RADIUS server within corporate network and authentication survivability enabled for branch survivability.
- Wired and wireless users in L3 and NAT modes, respectively.
- Access rules for wired and wireless users with source-NAT-based rule for contractor roles to bypass global routing profile.
- OSPF based route propagation on controller.

Topology

Figure 13 shows the topology and the IP addressing scheme used in this scenario.

Figure 13 *Scenario 3—IPsec: Multiple Datacenter Deployment with Primary and Backup Controller for Redundancy*



The IP addressing scheme used in this example is as follows:

- 10.0.0.0/8 is the corporate network.
- 10.30.0.0/16 subnet is reserved for L3 mode –used by Employee SSID.
- 10.40.0.0/16 subnet is reserved for L3 mode –used by Contractor SSID.
- 172.16.20.0/24 subnet is used for NAT mode – used for wired network.

- Client count in each branch is 200.
- Contractors are only permitted to reach 10.16.0.0/16 network.

Instant AP Configuration

This section provides information on configuration steps performed through the CLI and the UI.

Table 148: *Instant AP Configuration for Scenario 3—IPsec: Multiple Datacenter Deployment*

Configuration Steps	CLI Commands	WebUI Procedure
1. Configure the primary IP address. This IP address is the Public IP address of the controller. **Fast Failover** is enabled for fast convergence.	▪ `(Instant AP)(config)# vpn primary <public IP of primary controller>` ▪ `(Instant AP)(config)# vpn backup <public IP of backup controller>` ▪ `(Instant AP)(config)# vpn preemption` ▪ `(Instant AP)(config)# vpn fast-failover`	See Configuring an IPsec Tunnel
2. Configure routing profiles to tunnel traffic through IPsec.	▪ `(Instant AP)(config)# routing-profile` ▪ `(Instant AP)(routing-profile)# route 0.0.0.0 0.0.0.0 <public IP of primary controller>` ▪ `(Instant AP)(routing-profile)# route 10.0.0.0 255.0.0.0 <public IP of backup controller>`	See Configuring Routing Profiles
3. Configure Enterprise DNS for split DNS. The example in the next column uses a specific enterprise domain to tunnel all DNS queries matching that domain to corporate.	▪ `(Instant AP)(config)# internal-domains` ▪ `(Instant AP)(domains)# domain-name corpdomain.com`	See Configuring Enterprise Domains
4. Configure Distributed, L3 DHCP profiles with VLAN 30 and VLAN 40.	**Distributed, L3 profile with VLAN 30** ▪ `(Instant AP)(config)# ip dhcp l3-dhcp` ▪ `(Instant AP)(DHCP profile "l3-dhcp")# server-type Distributed,L3` ▪ `(Instant AP)(DHCP profile "l3-dhcp")# server-vlan 30` ▪ `(Instant AP)(DHCP profile "l3-dhcp")# ip-range 10.30.0.0 10.30.255.255` ▪ `(Instant AP)(DHCP profile "l3-dhcp")# dns-server 10.1.1.50,10.1.1.30` ▪ `(Instant AP)(DHCP profile "l3-`	See Configuring Distributed DHCP Scopes and In the Old WebUI

Table 148: *Instant AP Configuration for Scenario 3—IPsec: Multiple Datacenter Deployment*

Configuration Steps	CLI Commands	WebUI Procedure
	dhcp")# domain-name corpdomain.com ■ (Instant AP)(DHCP profile "l3-dhcp")# client-count 200 **Distributed, L3 profile with VLAN 40** ■ (Instant AP)(config)# ip dhcp l3-dhcp ■ (Instant AP)(DHCP profile "l3-dhcp")# server-type Distributed,L3 ■ (Instant AP)(DHCP profile "l3-dhcp")# server-vlan 40 ■ (Instant AP)(DHCP profile "l3-dhcp")# ip-range 10.40.0.0 10.40.255.255 ■ (Instant AP)(DHCP profile "l3-dhcp")# dns-server 10.1.1.50,10.1.1.30 ■ (Instant AP)(DHCP profile "l3-dhcp")# domain-name corpdomain.com ■ (Instant AP)(DHCP profile "l3-dhcp")# client-count 200 **Local profile with VLAN 20** ■ (Instant AP)(config)# ip dhcp local ■ (Instant AP)(DHCP profile "local")# server-type Local ■ (Instant AP)(DHCP profile "local")# server-vlan 20 ■ (Instant AP)(DHCP profile "local")# subnet 172.16.20.1 ■ (Instant AP)(DHCP profile "local")# subnet-mask 255.255.255.0 ■ (Instant AP)(DHCP profile "local")# lease-time 86400 ■ (Instant AP)(DHCP profile "local")# dns-server 10.1.1.30,10.1.1.50 ■ (Instant AP)(DHCP profile "local")# domain-name arubanetworks.com	

Table 148: *Instant AP Configuration for Scenario 3—IPsec: Multiple Datacenter Deployment*

Configuration Steps	CLI Commands	WebUI Procedure
	The IP range configuration on each branch will be the same. Each Instant AP will derive a smaller subnet based on the client count scope using the BID allocated by the controller.	
5. Create authentication servers for user authentication. The example in the next column assumes 802.1X SSID.	■ `(Instant AP)(config)# wlan auth-server server1` ■ `(Instant AP)(Auth Server "server1")# ip 10.2.2.1` ■ `(Instant AP)(Auth Server "server1")# port 1812` ■ `(Instant AP)(Auth Server "server1")# acctport 1813` ■ `(Instant AP)(Auth Server "server1")# key "presharedkey"` ■ `(Instant AP)(Auth Server "server1")# exit` ■ `(Instant AP)(config)# wlan auth-server server2` ■ `(Instant AP)(Auth Server "server1")# ip 10.2.2.2` ■ `(Instant AP)(Auth Server "server1")# port 1812` ■ `(Instant AP)(Auth Server "server1")# acctport 1813` ■ `(Instant AP)(Auth Server "server1")# key "presharedkey"`	See Configuring an External Server for Authentication
6. Configure wired port and wireless SSIDs using the authentication servers and access rules; enable authentication survivability.	Configure wired ports to operate in NAT mode and associate VLAN 20 to the wired port profile. ■ `(Instant AP)(config) # wired-port-profile wired-port` ■ `(Instant AP)(wired-port-profile "wired-port")# switchport-mode access` ■ `(Instant AP)(wired-port-profile "wired-port")# allowed-vlan all` ■ `(Instant AP)(wired-port-profile "wired-port")# native-vlan 20` ■ `(Instant AP)(wired-port-profile "wired-port")# no shutdown` ■ `(Instant AP)(wired-port-profile "wired-port")# access-rule-name wired-port`	See Configuring a Wired Profile and Wireless Network Profiles

Table 148: *Instant AP Configuration for Scenario 3—IPsec: Multiple Datacenter Deployment*

Configuration Steps	CLI Commands	WebUI Procedure
	■ `(Instant AP)(wired-port-profile "wired-port")# type employee` ■ `(Instant AP)(wired-port-profile "wired-port")# auth-server server1` ■ `(Instant AP)(wired-port-profile "wired-port")# auth-server server2` ■ `(Instant AP)(wired-port-profile "wired-port")# dot1x` ■ `(Instant AP)(wired-port-profile "wired-port")# exit` ■ `(Instant AP)(config)# enet1-port-profile wired-port` Configure a wireless SSID to operate in L3 mode for employee and associate Distributed, L3 mode VLAN 30 to the WLAN SSID profile. ■ `(Instant AP)(config) # wlan ssid-profile wireless-ssid` ■ `(Instant AP)(SSID Profile "wireless-ssid")# enable` ■ `(Instant AP)(SSID Profile "wireless-ssid")# type employee` ■ `(Instant AP)(SSID Profile "wireless-ssid")# essid wireless-ssid` ■ `(Instant AP)(SSID Profile "wireless-ssid")# opmode wpa2-aes` ■ `(Instant AP)(SSID Profile "wireless-ssid")# vlan 30` ■ `(Instant AP)(SSID Profile "wireless-ssid")# auth-server server1` ■ `(Instant AP)(SSID Profile "wireless-ssid")# auth-server server2` ■ `(Instant AP)(SSID Profile "wireless-ssid")# auth-survivability` Configure a wireless SSID to operate in L3 mode for contractor and associate Distributed, L3 mode VLAN 40 to the WLAN SSID profile.	

Table 148: *Instant AP Configuration for Scenario 3—IPsec: Multiple Datacenter Deployment*

Configuration Steps	CLI Commands	WebUI Procedure
	■ `(Instant AP)(config) # wlan ssid-profile wireless-ssid-contractor` ■ `(Instant AP)(SSID Profile "wireless-ssid-contractor")# enable` ■ `(Instant AP)(SSID Profile "wireless-ssid-contractor")# type contractor` ■ `(Instant AP)(SSID Profile "wireless-ssid-contractor")# essid wireless-ssid-contractor` ■ `(Instant AP)(SSID Profile "wireless-ssid-contractor")# opmode wpa2-aes` ■ `(Instant AP)(SSID Profile "wireless-ssid-contractor")# vlan 40` ■ `(Instant AP)(SSID Profile "wireless-ssid-contractor")# auth-server server1` ■ `(Instant AP)(SSID Profile "wireless-ssid-contractor")# auth-server server2` ■ `(Instant AP)(SSID Profile "wireless-ssid-contractor")# auth-survivability`	
7. Create access rule for wired and wireless authentication. In this example, the rule permits all traffic. For contractor SSID role, the rule allows only 10.16.0.0/16 network and all other traffic address is translated at the source and the global routing profile definition is bypassed.	**For wired profile:** ■ `(Instant AP)(config)# wlan access-rule wired-port` ■ `(Instant AP)(Access Rule "wired-port")# rule any any match any any any permit` **For WLAN SSID employee roles:** ■ `(Instant AP)(config)# wlan access-rule wireless-ssid` ■ `(Instant AP)(Access Rule "wireless-ssid")# rule any any match any any any permit` **For WLAN SSID contractor roles:** ■ `(Instant AP)(config)# wlan access-rule wireless-ssid-contractor` ■ `(Instant AP)(Access Rule "wireless-ssid-contractor")#`	See Configuring ACL Rules for Network Services

Table 148: *Instant AP Configuration for Scenario 3—IPsec: Multiple Datacenter Deployment*

Configuration Steps	CLI Commands	WebUI Procedure
	`rule 10.16.0.0 255.255.0.0 match any any any permit` ■ `(Instant AP)(Access Rule "wireless-ssid-contractor")# rule any any match any any any src-nat`	
NOTE: Ensure that you execute the **commit apply** command in the Instant CLI before saving the configuration and propagating changes across the Instant AP cluster.		

Instant AP-Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multiple Instant AP deployments, as client traffic from the slave to the master is tagged with the client VLAN.

Datacenter Configuration

For information on controller configuration, see Configuring a Controller for IAP-VPN Operations on page 339.

The following OSPF configuration is required on the controller to redistribute IAP-VPN routes to upstream routers:

```
(host)(config) # router ospf
(host)(config) # router ospf router-id <ID>
(host)(config) # router ospf area 0.0.0.0
(host)(config) # router ospf redistribute rapng-vpn
```

Scenario 4—GRE: Single Datacenter Deployment with No Redundancy

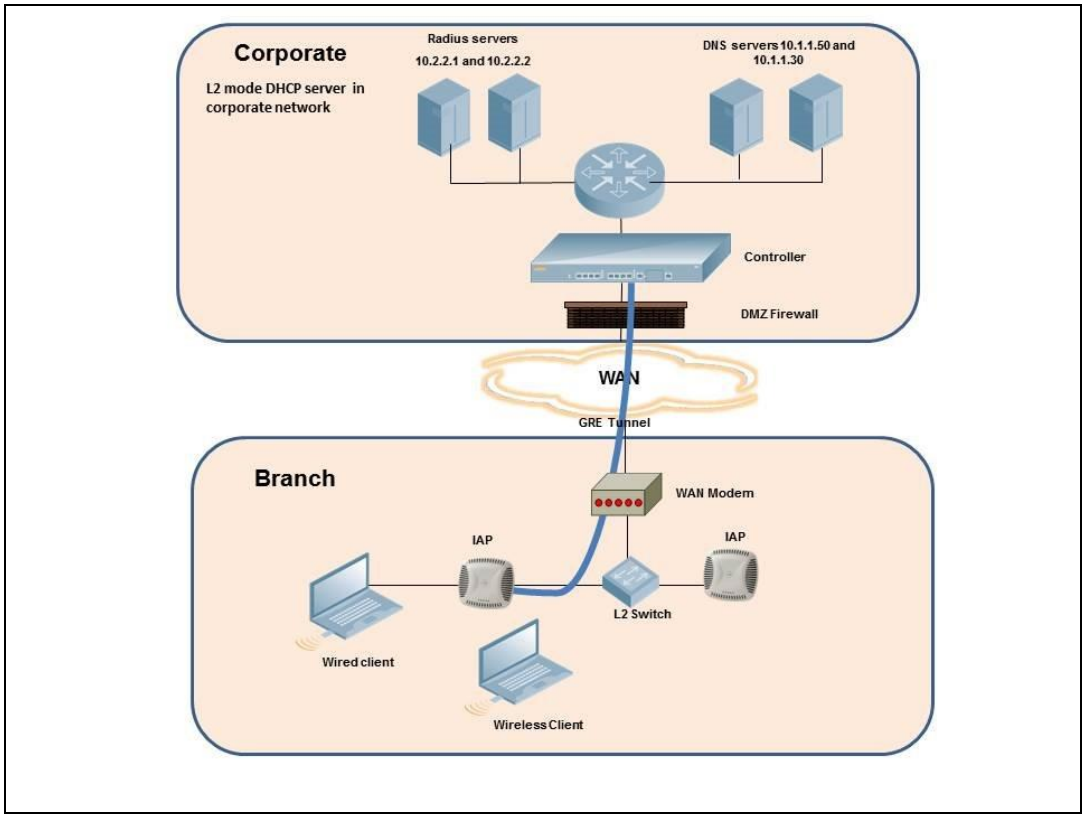
This scenario includes the following configuration elements:

- Single VPN primary configuration using GRE
  - **Aruba GRE**, does not require any configuration on the Mobility Controller that acts as a GRE endpoint.
  - **Manual GRE**, which requires GRE tunnels to be explicitly configured on the GRE endpoint that can be an Mobility Controller or any device that supports GRE termination.
- Tunneling of all traffic to datacenter
- Centralized, L2 mode DHCP profile
- RADIUS server within corporate network and authentication survivability for branch survivability.
- Wired and wireless users in L2 mode
- Access rules defined for wired and wireless networks to permit all traffic

Topology

Figure 14 shows the topology and the IP addressing scheme used in this scenario:

Figure 14 *Scenario 4—GRE: Single Datacenter Deployment with No Redundancy*



The following IP addresses are used in the examples for this scenario:

- 10.0.0.0/8 is the corporate network.
- 10.20.0.0/16 subnet is reserved for L2 mode.

Instant AP Configuration

This section provides information on configuration steps performed by using the CLI and the UI.

Table 149: *Instant AP Configuration for Scenario 4—GRE: Single Datacenter Deployment with No Redundancy*

Configuration Steps	CLI Commands	WebUI Procedure
1. Configure Aruba GRE or manual GRE ■ Aruba GRE uses an IPsec tunnel to facilitate controller configuration and requires VPN to be configured. This VPN tunnel is not used for any client traffic. ■ Manual GRE uses standard GRE tunnel configuration and requires controller configuration to complete the GRE tunnel.	**Aruba GRE configuration** ■ `(Instant AP)(config)# vpn primary <controller-IP>` ■ `(Instant AP)(config)# vpn gre-outside` **Manual GRE configuration** ■ `(Instant AP)(config)# gre primary <controller-IP>` ■ `(Instant AP)(config)# gre type 80` **Per-AP GRE tunnel configuration**	See Configuring Aruba GRE Parameters and Configuring Manual GRE Parameters

Table 149: *Instant AP Configuration for Scenario 4—GRE: Single Datacenter Deployment with No Redundancy*

Configuration Steps	CLI Commands	WebUI Procedure
	Optionally, per-AP GRE tunnel can also be enabled, which causes each Instant AP to form an independent GRE tunnel to the GRE end-point. Aruba GRE requires each Instant AP MAC to be present in the controller whitelist. Manual GRE requires GRE configuration for the IP of each Instant AP on the controller. ■ `(Instant AP)(config)# gre per-ap-tunnel` **NOTE:** If a virtual controller IP is configured and per-AP GRE tunnel is disabled, Instant AP uses virtual controller IP as the GRE source IP. For Manual GRE, this simplifies configuration on controller, since only the virtual controller IP destined GRE tunnel interface configuration is required.	
2. Configure routing profiles to tunnel traffic through GRE.	■ `(Instant AP)(config)# routing-profile` ■ `(Instant AP)(routing-profile)# route 0.0.0.0 0.0.0.0 <IP of GRE-endpoint>`	See Configuring Routing Profiles
3. Configure Enterprise DNS. The example in the next column tunnels all DNS queries to the client's original DNS server without proxying on Instant AP.	■ `(Instant AP)(config)# internal-domains` ■ `(Instant AP)(domains)# domain-name *`	See Configuring Enterprise Domains
4. Configure Centralized, L2 DHCP profile with VLAN 20.	**Centralized, L2 DHCP profile VLAN 20** ■ `(Instant AP)(config)# ip dhcp l2-dhcp` ■ `(Instant AP)(DHCP profile "l2-dhcp")# server-type Centralized,L2` ■ `(Instant AP)(DHCP profile "l2-dhcp")# server-vlan 20`	See Enabling DHCP Relay Agent Information Option (Option 82)
5. Create authentication servers for user authentication. The example in the next column assumes 802.1X SSID.	■ `(Instant AP)(config)# wlan auth-server server1` ■ `(Instant AP)(Auth Server "server1")# ip 10.2.2.1` ■ `(Instant AP)(Auth Server "server1")# port 1812` ■ `(Instant AP)(Auth Server "server1")# acctport 1813`	See Configuring an External Server for Authentication

Table 149: *Instant AP Configuration for Scenario 4—GRE: Single Datacenter Deployment with No Redundancy*

Configuration Steps	CLI Commands	WebUI Procedure
	■ `(Instant AP)(Auth Server "server1")# key "presharedkey"` ■ `(Instant AP)(Auth Server "server1")# exit` ■ ■ `(Instant AP)(config)# wlan auth-server server2` ■ `(Instant AP)(Auth Server "server1")# ip 10.2.2.2` ■ `(Instant AP)(Auth Server "server1")# port 1812` ■ `(Instant AP)(Auth Server "server1")# acctport 1813` ■ `(Instant AP)(Auth Server "server1")# key "presharedkey"`	
6. Configure wired and wireless SSIDs using the authentication servers and access rules; enable authentication survivability.	Configure wired ports to operate in Centralized, L2 mode and associate VLAN 20 to the wired port profile. ■ `(Instant AP)(config) # wired-port-profile wired-port` ■ `(Instant AP)(wired-port-profile "wired-port")# switchport-mode access` ■ `(Instant AP)(wired-port-profile "wired-port")# allowed-vlan all` ■ `(Instant AP)(wired-port-profile "wired-port")# native-vlan 20` ■ `(Instant AP)(wired-port-profile "wired-port")# no shutdown` ■ `(Instant AP)(wired-port-profile "wired-port")# access-rule-name wired-port` ■ `(Instant AP)(wired-port-profile "wired-port")# type employee` ■ `(Instant AP)(wired-port-profile "wired-port")# auth-server server1` ■ `(Instant AP)(wired-port-profile "wired-port")# auth-server server2` ■ `(Instant AP)(wired-port-profile "wired-port")# dot1x` ■ `(Instant AP)(wired-port-profile "wired-port")# exit` ■ `(Instant AP)(config)# enet1-`	See Configuring a Wired Profile and Wireless Network Profiles

Table 149: *Instant AP Configuration for Scenario 4—GRE: Single Datacenter Deployment with No Redundancy*

Configuration Steps	CLI Commands	WebUI Procedure
	`port-profile wired-port` Configure a wireless SSID to operate in Centralized, L2 mode and associate VLAN 20 to the WLAN SSID profile. ■ `(Instant AP)(config) # wlan ssid-profile wireless-ssid` ■ `(Instant AP)(SSID Profile "wireless-ssid")# enable` ■ `(Instant AP)(SSID Profile "wireless-ssid")# type employee` ■ `(Instant AP)(SSID Profile "wireless-ssid")# essid wireless-ssid` ■ `(Instant AP)(SSID Profile "wireless-ssid")# opmode wpa2-aes` ■ `(Instant AP)(SSID Profile "wireless-ssid")# vlan 20` ■ `(Instant AP)(SSID Profile "wireless-ssid")# auth-server server1` ■ `(Instant AP)(SSID Profile "wireless-ssid")# auth-server server2` ■ `(Instant AP)(SSID Profile "wireless-ssid")# auth-survivability`	
7. Create access rule for wired and wireless authentication.	**For wired profile:** ■ `(Instant AP)(config)# wlan access-rule wired-port` ■ `(Instant AP)(Access Rule "wired-port")# rule any any match any any any permit` **For WLAN SSID employee roles:** ■ `(Instant AP)(config)# wlan access-rule wireless-ssid` ■ `(Instant AP)(Access Rule "wireless-ssid")# rule any any match any any any permit`	See Configuring ACL Rules for Network Services
NOTE: Ensure that you execute the **commit apply** command in the Instant CLI before saving the configuration and propagating changes across the Instant AP cluster.		

Instant AP-Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multiple Instant AP deployments, as client traffic from the slave to the master is tagged with the client VLAN.

Datacenter Configuration

For information on controller configuration, see Configuring a Controller for IAP-VPN Operations on page 339.

The following GRE configuration is required on the controller:

```
(Instant AP)(config)# interface tunnel <Number>
(Instant AP)(config-tunnel)# description <Description>
(Instant AP)(config-tunnel)# tunnel mode gre <ID>
(Instant AP)(config-tunnel)# tunnel source <controller-IP>
(Instant AP)(config-tunnel)# tunnel destination <AP-IP>
(Instant AP)(config-tunnel)# trusted
(Instant AP)(config-tunnel)# tunnel vlan <allowed-VLAN>
```

Chapter 21
Adaptive Radio Management

This chapter provides the following information:

- ARM Overview on page 369
- Configuring ARM Features on an Instant AP on page 370
- Configuring Radio Settings on page 377

ARM Overview

ARM is an RF management technology that optimizes WLAN performance even in networks with the highest traffic by dynamically and intelligently choosing the best 802.11 channel and transmitting power for each Instant AP in its current RF environment. ARM works with all standard clients, across all operating systems, while remaining in compliance with the IEEE 802.11 standards. It does not require any proprietary client software to achieve its performance goals. ARM ensures low-latency roaming, consistently high performance, and maximum client compatibility in a multi-channel environment. By ensuring a fair distribution of the available Wi-Fi bandwidth to mobile devices, ARM ensures that data, voice, and video applications have sufficient network resources at all times. ARM allows mixed 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac client types to interoperate at the highest performance levels.

Channel or Power Assignment

The channel or power assignment feature automatically assigns channel and power settings for all the Instant APs in the network according to changes in the RF environment. This feature automates many setup tasks during network installation and the ongoing operations when RF conditions change.

Voice Aware Scanning

The Voice Aware scanning feature prevents an Instant AP supporting an active voice call from scanning for other channels in the RF spectrum and allows the Instant AP to resume scanning when there are no active voice calls. This significantly improves the voice quality when a call is in progress and simultaneously delivers the automated RF management functions. By default, this feature is enabled.

Load Aware Scanning

The Load Aware Scanning feature dynamically adjusts scanning function to maintain uninterrupted data transfer on resource-intensive systems when the network traffic exceeds a predefined threshold. The Instant APs resume complete monitoring scans when the traffic drops to the normal levels. By default, this feature is enabled.

Monitoring the Network with ARM

When ARM is enabled, an Instant AP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and sends reports to a virtual controller on WLAN network coverage, interference, and intrusion detection.

ARM Metrics

ARM computes coverage and interference metrics for each valid channel and chooses the best performing channel and transmit power settings for each Instant AP RF environment. Each Instant AP gathers other metrics on its ARM-assigned channel to provide a snapshot of the current RF health state.

Configuring ARM Features on an Instant AP

This section describes the following procedures for configuring ARM features:

- Band Steering on page 370
- Airtime Fairness Mode on page 370
- Client Match on page 371
- Access Point Control on page 374

Band Steering

The band steering feature assigns the dual-band capable clients to the 5 GHz band on dual-band Instant APs. This feature reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5 GHz band than that on the 2.4 GHz band. The following procedure describes how to configure band steering parameters through the WebUI.

Table 150: *Configuring Band Steering*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **RF** page. 2. Expand **ARM**. 3. Select one of the following options from the **Band steering mode** drop-down list: 4. **Prefer 5 GHz** - Select this option to use band steering in the 5 GHz mode. On selecting this, the Instant AP steers the client to the 5 GHz band (if the client is 5 GHz-capable), but allows the client connection on the 2.4 GHz band if the client persistently attempts for 2.4 GHz association. 5. **Force 5 GHz** - Select this option to enforce 5 GHz band steering mode on the Instant APs. 6. **Balance Bands** - Select this option to allow the Instant AP to balance the clients across the two radios to best utilize the available 2.4 GHz bandwidth. This feature takes into account the fact that the 5 GHz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40 MHz, while the 2.4 GHz band operates in 20 MHz. 7. **Disabled** - Select this option if you want to allow the clients to select the band to use. 8. Click **Save**.	1. Go to **RF** > **ARM**. 2. Select one of the following options from the **Band steering mode** drop-down list: 3. **Prefer 5 GHz** - Select this option to use band steering in the 5 GHz mode. On selecting this, the Instant AP steers the client to the 5 GHz band (if the client is 5 GHz-capable), but allows the client connection on the 2.4 GHz band if the client persistently attempts for 2.4 GHz association. 4. **Force 5 GHz** - Select this option to enforce 5 GHz band steering mode on the Instant APs. 5. **Balance Bands** - Select this option to allow the Instant AP to balance the clients across the two radios to best utilize the available 2.4 GHz bandwidth. This feature takes into account the fact that the 5 GHz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40 MHz, while the 2.4 GHz band operates in 20 MHz. 6. **Disabled** - Select this option if you want to allow the clients to select the band to use. 7. Click **OK**.

The following CLI commands configure band steering:

```
(Instant AP)(config)# arm
(Instant AP)(ARM)# band-steering-mode {<Prefer 5 GHz>| <Force 5 GHz>|<Balance
Bands>|<Disabled>}
```

Airtime Fairness Mode

The airtime fairness feature provides equal access to all clients on the wireless medium, regardless of client type, capability, or operating system, thus delivering uniform performance to all clients. This feature prevents the clients from monopolizing resources. The following procedure describes how to configure airtime fairness mode parameters through the WebUI.

Table 151: *Configuring Airtime Fairness Mode*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **RF** page. 2. Expand **ARM**. 3. Select one of the following options from the **Airtime fairness mode** drop-down list: 4. **Default Access** - Select this option to provide access based on client requests. When **Air Time Fairness** is set to default access, per-user and per-SSID bandwidth limits are not enforced. 5. **Fair Access** - Select this option to allocate Airtime evenly across all the clients. 6. **Preferred Access** - Select this option to set a preference where 802.11n clients are assigned more airtime than 802.11a or 802.11g. The 802.11a or 802.11g clients get more airtime than 802.11b. The ratio is 16:4:1. 7. Click **Save**.	1. Go to **RF** > **ARM** > **Show advanced options**. 2. Select one of the following options from the **Airtime fairness mode** drop-down list: 3. **Default Access** - Select this option to provide access based on client requests. When **Air Time Fairness** is set to default access, per-user and per-SSID bandwidth limits are not enforced. 4. **Fair Access** - Select this option to allocate Airtime evenly across all the clients. 5. **Preferred Access** - Select this option to set a preference where 802.11n clients are assigned more airtime than 802.11a or 802.11g. The 802.11a or 802.11g clients get more airtime than 802.11b. The ratio is 16:4:1. 6. Click **OK**.

The following CLI commands configure airtime fairness mode:

```
(Instant AP)(config)# arm
(Instant AP)(ARM)# air-time-fairness-mode {<Default Access>| <Fair Access> | <Preferred Access>}
```

Client Match

The ARM client match feature continually monitors a client's RF neighborhood to provide ongoing client band steering and load balancing, and enhanced Instant AP reassignment for roaming mobile clients. This feature supersedes the legacy band steering and spectrum load balancing features, which unlike client match, do not trigger Instant AP changes for clients already associated to an Instant AP. In addition to this, the Client Match feature provides the smartphone handoff assist function which helps smartphones to switch between 3G and 4G networks when the Wi-Fi connectivity is poor. The Instant AP monitors the RSSI of the smartphone and checks if it remains under the threshold connectivity strength for a certain duration and deauthenticates the client.



Legacy 802.11a, 802.11b, or 802.11g access points do not support the client match feature. When client match is enabled on 802.11n-capable access points, the client match feature overrides any settings configured for the legacy band steering, station handoff assist, or load balancing feature. 802.11ac-capable access points do not support the legacy band steering, station handoff assist, or load balancing settings; so these access points must be managed using client match.

When the client match feature is enabled on an Instant AP, the Instant AP measures the RF health of its associated clients. In the current release, the client match feature is supported only within an Instant AP cluster. If any of the following trigger conditions is met, clients are moved from one Instant AP to another for better performance and client experience:

- Dynamic Load Balancing—Client match balances clients across Instant APs on different channels, based on the client load on the Instant APs and the SNR levels the client detects from an underutilized Instant AP. If an Instant AP radio can support additional clients, the Instant AP will participate in client match load balancing and clients can be directed to that Instant AP radio, subject to the predefined SNR thresholds. For better load balancing, clients are steered from busy channels to idle channels.
- Sticky Clients—The client match feature also helps mobile clients that tend to stay associated to an Instant AP despite low signal levels. Instant APs using client match continually monitor the client's RSSI as the client roams between Instant APs, and move the client to an Instant AP when a better radio match can be found. This prevents mobile clients from remaining associated to the Instant APs with less than ideal RSSI, which can cause poor connectivity and reduce performance for other clients associated with that Instant AP.
- Band Steering—Instant APs using the client match feature monitor the RSSI for clients that advertise a dual-band capability. If a client is currently associated to a 2.4 GHz radio and the Instant AP detects that the client has a good RSSI from the 5 GHz radio, the Instant AP steers the client to the 5 GHz radio, as long as the 5 GHz RSSI is not significantly worse than the 2.4 GHz RSSI, and the Instant AP retains a suitable distribution of clients on each of its radios.
- Channel Utilization—Based on the percentage of channel utilization, clients are steered from a busy channel to an idle channel.
- Client Capability Match—Based on the client capability match, clients are steered to appropriate channel, for example, HT20, HT40, or VHT80.



Starting from the Instant 6.3.1.1-4.0 release, spectrum load balancing is integrated with the client match feature. Client match allows the Instant APs in a cluster to be divided into several logical Instant AP RF neighborhood called domains, which share the same clients. The network determines the distribution of clients and balances client load across channels, regardless of whether the Instant AP is responding to the probe requests of wireless clients.

Client Match Support for Standalone Instant APs

Previously, client match keys were generated by the virtual controller key to differentiate whether or not Instant APs belonged to the same cluster. If the client match keys did not match, client match functionality failed to take effect on standalone Instant APs within the same management VLAN.

Instant 8.4.0.0 supports the client match functionality across standalone Instant APs within the same management VLAN. Client match uses the wired layer 2 protocol to synchronize information exchanged between Instant APs. Users have an option to configure the client match keys. Instant APs verify if the frames that they broadcast contain a common client match key. Instant APs that receive these frames verify if the sender belongs to same network or if the sender and receiver both have the same client match key. The receiver adds the sender's information to the client match scope. After the sender's information is added, the client match functionality takes effect for standalone Instant APs as well.

The following procedure describes how to configure client match parameters in the WebUI. When client match is enabled, the dashboard in the main window displays the **Client Match** link on selecting an Instant AP in the **Access Points** tab or a client in the **Clients** tab. Clicking this link provides a graphical representation of radio map view of an Instant AP and the client distribution on an Instant AP radio. For more information, see Client Match on page 58.

Table 152: *Configuring Client Match*

New WebUI	Old WebUI
1. For client match configuration, specify the	1. For client match configuration, specify the

New WebUI	Old WebUI
following parameters in **Configuration** > **RF** > **ARM** > **Show advanced options**: ■ **Client match** - Select **Enabled** to enable the **Client match** feature on Instant APs. When enabled, client count will be balanced among all the channels in the same band. For more information, see ARM Overview on page 369. By default, the client match feature is disabled. **NOTE:** When client match is enabled, ensure that Scanning is enabled. ■ **CM calculating interval** -Specify a value for calculating the interval of Client match. The value specified for **CM calculating interval** determines the interval at which client match is calculated. The interval is specified in seconds and the default value is 30 seconds. You can specify a value within the range of 10–600. ■ **CM neighbor matching %** - Specify a value for **CM neighbor matching %**. This number takes into account the least similarity percentage to be considered as in the same virtual RF neighborhood of client match. You can specify a percentage value within the range of 20–100. The default value is 60%. ■ **CM threshold** - Specify a value for **CM threshold**. This number takes acceptance client count difference among all the channels of client match into account. When the client load on anInstant AP reaches or exceeds the threshold, client match is enabled on that Instant AP. You can specify a value within range of 1–255. The default value is 2. ■ **SLB mode** - Select a mode from the **SLB mode** drop-down list. The SLB mode determines the balancing strategy for client match. The following options are available: a. Channel b. Radio c. Channel + Radio 2. Click **Save**.	following parameters in the **RF** > **ARM** > **Show advanced options** tab: ■ **Client match** - Select **Enabled** to enable the **Client match** feature on Instant APs. When enabled, client count will be balanced among all the channels in the same band. For more information, see ARM Overview on page 369. By default, the client match feature is disabled. **NOTE:** When client match is enabled, ensure that Scanning is enabled. ■ **CM calculating interval** -Specify a value for calculating the interval of Client match. The value specified for **CM calculating interval** determines the interval at which client match is calculated. The interval is specified in seconds and the default value is 30 seconds. You can specify a value within the range of 10–600. ■ **CM neighbor matching %** - Specify a value for **CM neighbor matching %**. This number takes into account the least similarity percentage to be considered as in the same virtual RF neighborhood of client match. You can specify a percentage value within the range of 20–100. The default value is 60%. ■ **CM threshold** - Specify a value for **CM threshold**. This number takes acceptance client count difference among all the channels of client match into account. When the client load on anInstant AP reaches or exceeds the threshold, client match is enabled on that Instant AP. You can specify a value within range of 1–255. The default value is 2. ■ **SLB mode** - Select a mode from the **SLB mode** drop-down list. The SLB mode determines the balancing strategy for client match. The following options are available: a. Channel b. Radio c. Channel + Radio 2. Click **OK**.

The following CLI commands configure Client Match:

```
(Instant AP)(config)# arm
```

```
(Instant AP)(ARM)# client-match calc-interval <seconds>
(Instant AP)(ARM)# client-match calc-threshold <threshold>
(Instant AP)(ARM)# client-match nb-matching <percentage>
(Instant AP)(ARM)# client-match slb-mode 1
```

Access Point Control

The following procedure describes how to configure access point control parameters through the WebUI.

Table 153: *Configuring Access Point Control*

New WebUI	Old WebUI
1. For **Access Point Control**, configure the following parameters in **Configuration** > **RF** > **ARM** > **Show advanced options**: ▪ **Customize valid channels** - Select this check box to customize valid channels for 2.4 GHz and 5 GHz. By default, the Instant AP uses valid channels as defined by the Country Code (regulatory domain). On selecting the **Customize valid channels** check box, a list of valid channels for both 2.4 GHz and 5 GHz are displayed. The valid channel customization feature is disabled by default. ▪ **Min transmit power** -Specify the minimum transmission power. The value specified for **Min transmit power** indicates the minimum EIRP that can range from 3 dBm to 33 dBm in 3 dBm increments. If the minimum transmission EIRP setting configured on anInstant AP is not supported by the Instant AP model, this value is reduced to the highest supported power setting. The default value for minimum transmit power is 18 dBm. ▪ **Max transmit power** - Specify the maximum transmission power. The value specified for **Max transmit power** indicates the maximum EIRP that can range from 3 dBm to 33 dBm in 3 dBm increments. If the maximum transmission EIRP configured on anInstant AP is not supported by the Instant AP model, the value is reduced to the highest supported power setting. The default value for maximum transmit power is 127 dBm. ▪ **Client aware** - When enabled, ARM does not change channels for the Instant APs with active clients, except for high-priority events such as RADAR or excessive noise.	1. For **Access Point Control**, specify the following parameters in the **RF** > **ARM** > **Show advanced options** tab: ▪ **Customize valid channels** - Select this check box to customize valid channels for 2.4 GHz and 5 GHz. By default, the Instant AP uses valid channels as defined by the Country Code (regulatory domain). On selecting the **Customize valid channels** check box, a list of valid channels for both 2.4 GHz and 5 GHz are displayed. The valid channel customization feature is disabled by default. ▪ **Min transmit power** -Specify the minimum transmission power. The value specified for **Min transmit power** indicates the minimum EIRP that can range from 3 dBm to 33 dBm in 3 dBm increments. If the minimum transmission EIRP setting configured on anInstant AP is not supported by the Instant AP model, this value is reduced to the highest supported power setting. The default value for minimum transmit power is 18 dBm. ▪ **Max transmit power** - Specify the maximum transmission power. The value specified for **Max transmit power** indicates the maximum EIRP that can range from 3 dBm to 33 dBm in 3 dBm increments. If the maximum transmission EIRP configured on anInstant AP is not supported by the Instant AP model, the value is reduced to the highest supported power setting. The default value for maximum transmit power is 127 dBm. ▪ **Client aware** - When enabled, ARM does not change channels for the Instant APs with active clients, except for high-priority events such as RADAR or excessive noise.

New WebUI	Old WebUI
This feature must be enabled in most deployments for a stable WLAN. If the Client Aware mode is set to **Disabled**, the Instant AP may change to a more optimal channel, that may disrupt the current client traffic for a while. The Client aware option is **Enabled** by default. **NOTE:** When Client aware is disabled, channels can be changed even when the clients are active on a BSSID. ▪ **Scanning** - Select **Enabled** so that the Instant AP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and reports to the Instant AP. This scanning report includes WLAN coverage, interference, and intrusion detection data. **NOTE:** For client match configuration, ensure that scanning is enabled. ▪ **Wide channel bands** - Select a band to allow the Instant APs to be placed in 40 MHz (wide band) channels. The **Wide channel bands** allows administrators to configure 40 MHz channels in the 2.4 GHz and 5 GHz bands. 40 MHz channels are two 20 MHz adjacent channels that are bonded together. A 40 MHz channel effectively doubles the frequency bandwidth available for data transmission. ▪ **80MHz support** - Enables or disables the use of 80 MHz channels on Instant APs. This feature allows ARM to assign 80 MHz channels on Instant APs with 5 GHz radios, which support a VHT. This setting is enabled by default. **NOTE:** Only the Instant APs that support 802.11ac can be configured with 80 MHz channels. 2. Click **Save**. 3. Reboot the Instant AP.	This feature must be enabled in most deployments for a stable WLAN. If the Client Aware mode is set to **Disabled**, the Instant AP may change to a more optimal channel, that may disrupt the current client traffic for a while. The Client aware option is **Enabled** by default. **NOTE:** When Client aware is disabled, channels can be changed even when the clients are active on a BSSID. ▪ **Scanning** - Select **Enabled** so that the Instant AP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and reports to the Instant AP. This scanning report includes WLAN coverage, interference, and intrusion detection data. **NOTE:** For client match configuration, ensure that scanning is enabled. ▪ **Wide channel bands** - Select a band to allow the Instant APs to be placed in 40 MHz (wide band) channels. The **Wide channel bands** allows administrators to configure 40 MHz channels in the 2.4 GHz and 5 GHz bands. 40 MHz channels are two 20 MHz adjacent channels that are bonded together. A 40 MHz channel effectively doubles the frequency bandwidth available for data transmission. ▪ **80MHz support** - Enables or disables the use of 80 MHz channels on Instant APs. This feature allows ARM to assign 80 MHz channels on Instant APs with 5 GHz radios, which support a VHT. This setting is enabled by default. **NOTE:** Only the Instant APs that support 802.11ac can be configured with 80 MHz channels. 2. Reboot the Instant AP. 3. Click **OK**.

The following CLI commands configure access point control parameters:

```
(Instant AP)(config)# arm
(Instant AP)(ARM)# a-channels <5GHz-channels>
(Instant AP)(ARM)# min-tx-power <power>
(Instant AP)(ARM)# max-tx-power <power>
(Instant AP)(ARM)# client-aware
```

```
(Instant AP)(ARM)# wide-bands {<5GHz>|<2GHz>|<All>|<None>}
(Instant AP)(ARM)# scanning
(Instant AP)(ARM)# 80mhz-support
```

For more information on these settings, see **arm** command in the *Aruba Instant 8.7.0.x CLI Reference Guide*.

Verifying ARM Configuration

The following CLI command shows ARM configuration:

```
(Instant AP)# show arm config

Minimum Transmit Power            :18
Maximum Transmit Power            :127
Band Steering Mode       :prefer-5ghz
Client Aware             :enable
Scanning                 :enable
Wide Channel Bands       :5ghz
80Mhz Support            :enable
Air Time Fairness Mode   :fair-access
Client Match             :disable
CM NB Matching Percent   :75
CM Calculating Interval  :30
CM SLB Threshold         :2
CM SLB Balancing Mode    :channel based
CM max client match req  :5
CM max adoption          :5
Custom Channels          :No
2.4 GHz Channels
----------------
Channel  Status
-------  ------
1        enable
2        disable
3        disable
4        disable
5        disable
6        enable
7        disable
8        disable
9        disable
10       disable
11       enable
12       disable
13       disable
1+       enable
2+       disable
3+       disable
4+       disable
5+       disable
6+       disable
7+       enable
5.0 GHz Channels
----------------
Channel  Status
-------  ------
36       enable
40       enable
44       enable
48       enable
52       enable
56       enable
```

```
60        enable
64        enable
149       enable
153       enable
157       enable
161       enable
165       enable
36+       enable
44+       enable
52+       disable
60+       disable
149+      enable
157+      enable
36E       enable
52E       enable
149E      enable
```

Client Match for Access Points in a Zone

When Client match is enabled, the decision to move a client from the home Instant AP to a target Instant AP is made at the radio level. However, this proves inefficient when client match is enabled on an Instant AP or SSID operating in a specific zone, it could result in the client being moved to a target Instant AP that does not have the same zone specific SSID as the home Instant AP.

Steering a client from a home Instant AP to a target Instant AP will be made at the SSID level instead of the radio level, by adding the SSID name to the client match radio database. Client Match will check if the same SSID (zone specific SSID on Home Instant AP) is available on the target Instant AP before it moves the client. This ensures that client match works as expected when zone settings are configured on the Instant AP.

Additionally, the maximum clients threshold and the current associated client number of the SSID is added to the client match radio database to prevent the clients from being moved to an SSID whose associated client number is already reached its limit.

You can use the following commands to view the SSID details stored in client match:

The **show ap client-match-ssid-table** command displays the client match SSID table for the current Instant AP and its neighboring Instant APs.

The **show ap client-match-ssid-table radio-mac <mac>** command displays the client match SSID table for a specific Instant AP denoted by its mac address.

Configuring Radio Settings

The current Radio profile is displayed as **Default**. The default profile cannot be deleted. The following procedure describes how to configure 2.4 GHz and 5 GHz radio settings for an Instant AP either using the WebUI.

Table 154: *Configuring Access Point Control*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **RF** page. 2. Click **Show advanced options** at the bottom of the page. 3. Expand **Radio**. 4. Under **2.4 GHz band**, **5 GHz band** or **Secondary 5 GHz band**, click **+**. 5. Configure the parameters listed in the Radio	1. Click the **RF** link located directly above the Search bar of the Instant main window. 2. Click **Show advanced options**. The advanced options are displayed. 3. Click the **Radio** tab. 4. Under **2.4 GHz band** or **5 GHz band**, click **New**. 5. Configure the parameters listed in the Radio

New WebUI	Old WebUI
Configuration Parameters table below. 6. Click **OK**. 7. Click **Save**.	Configuration Parameters table below. 6. Click **OK** in the **New radio profile** window. 7. Click **OK** in the RF window.
NOTE: The secondary 5 GHz radio profile can only be configured using the new WebUI and the CLI.	

Table 155: *Radio Configuration Parameters*

Parameter	Description
Name	Enter a name for the 2.4 GHz or 5 GHz radio profile.
Zone	Enter the zone name for configuration. The same zone name can be configured on a 2.4 GHz and a 5 GHz radio profile. However, the same zone name cannot be configured on two different 2.4 GHz or two different 5 GHz profiles.
Legacy only	Click the toggle switch to run the radio in non-802.11n mode. This option is disabled by default.
802.11d / 802.11h	Click the toggle switch to allow the radio to advertise its 802.11d (Country Information) and 802.11h TPC capabilities. This option is disabled by default.
Beacon interval	Enter the Beacon period for the Instant AP in milliseconds. This indicates how often the 802.11 beacon management frames are transmitted by the access point. You can specify a value within the range of 60-500. The default value is 100 milliseconds.
Interference immunity level	Select to increase the immunity level to improve performance in high-interference environments. The default immunity level is 2. ■ **Level 0**—no ANI adaptation. ■ **Level 1**—Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. ■ **Level 2**—Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. ■ **Level 3**—Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. ■ **Level 4**—Level 3 settings, and FIR immunity. At this level, the Instant AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. ■ **Level 5**—The Instant AP completely disables PHY error reporting, improving performance by eliminating the time the Instant AP would spend on PHY processing. **NOTE:** Increasing the immunity level makes the Instant AP to lose a small amount of range.
Channel switch announcement count	Specify the count to indicate the number of channel switching announcements that must be sent before switching to a new channel. This allows associated clients to recover gracefully from a channel change.

Table 155: *Radio Configuration Parameters*

Parameter	Description
Background spectrum monitoring	Click the toggle switch to allow the Instant APs in access mode to continue with normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring Instant APs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients.
Customize ARM power range	Click the toggle switch and select a minimum (**Min power**) and maximum (**Max power**) power range value for the 2.4 GHz and 5 GHz band frequencies. The default value is 3 dBm. Unlike the configuration in the ARM profile, the transmit power of all radios in the Radio profile do not share the same configuration.
Very high throughput	Ensure that this check box is selected to enable VHT on 802.11ac devices with 5 GHz radio. If VHT is enabled for the 5 GHz radio profile on anInstant AP, it is automatically enabled for all SSIDs configured on anInstant AP. By default, VHT is enabled on all SSIDs. If you want the 802.11ac Instant APs to function as 802.11n Instant APs, clear the check box to disable VHT on these devices.
Smart antenna	This value is **Disabled** by default. Select **Enabled** to allow smart antenna polarization on the IAP-335 access points support the smart antenna feature. This feature helps optimize the selection of antenna polarization values based on data collected from the training of polarization pattern combinations. This feature identifies the clients most likely to benefit from smart antenna polarization, based on the average RSSI of the received frames and the number of streams. This feature uses frame-based antenna training, which allows the Instant AP to cycle through training combinations and collect statistics without causing any impact on the client. At the end of the training sequence, the Instant AP selects the best antenna polarization based on these collected statistics. The smart antenna feature does not support optimized antenna polarization for clients using Single-User or Multi-User transmit beamforming, and will use default polarization values for these clients.
BSS Color	Configures BSS color for the BSSIDs broadcast by the radio. The value range is 0-63, where 0 configures automatic BSS coloring. The default value is 0.
ARM/WIDS Override	By default, WIDS protection is on dynamic mode. If an Instant AP is heavily loaded with client traffic and the CPU utilization exceeds the threshold limit, the WIDS processing is suspended. This causes more CPU cycles to handle the client traffic. When the CPU utilization is within the the threshold limit, the WIDS processing is resumed. When **ARM/WIDS Override** is off, the Instant AP will always process frames for WIDS purposes even when it is heavily loaded with client traffic. When **ARM/WIDS Override** on, the Instant AP will stop process frames for WIDS purposes regardless of whether the Instant AP is heavily loaded or not. The WIDS functionality will not take effect.

The following CLI commands configure 2.4 GHz radio settings:

```
(Instant AP)(config)# rf dot11g-radio-profile
(Instant AP)(RF dot11g Radio Profile)# beacon-interval <milliseconds>
(Instant AP)(RF dot11g Radio Profile)# legacy-mode
(Instant AP)(RF dot11g Radio Profile)# spectrum-monitor
(Instant AP)(RF dot11g Radio Profile)# dot11h
(Instant AP)(RF dot11g Radio Profile)# interference-immunity <level>
(Instant AP)(RF dot11g Radio Profile)# csa-count <count>
(Instant AP)(RF dot11g Radio Profile)# max-distance <count>
(Instant AP)(RF dot11g Radio Profile)# max-tx-power <db>
(Instant AP)(RF dot11g Radio Profile)# min-tx-power <db>
(Instant AP)(RF dot11g Radio Profile)# smart-antenna
```

The following CLI commands configure 5 GHz radio settings:

```
(Instant AP)(config)# rf dot11a-radio-profile
(Instant AP)(RF dot11a Radio Profile)# beacon-interval <milliseconds>
(Instant AP)(RF dot11a Radio Profile)# legacy-mode
(Instant AP)(RF dot11a Radio Profile)# spectrum-monitor
```

```
(Instant AP)(RF dot11a Radio Profile)# spectrum-band <type>
(Instant AP)(RF dot11a Radio Profile)# dot11h
(Instant AP)(RF dot11a Radio Profile)# interference-immunity <level>
(Instant AP)(RF dot11a Radio Profile)# max-distance <count>
(Instant AP)(RF dot11a Radio Profile)# max-tx-power <db>
(Instant AP)(RF dot11a Radio Profile)# min-tx-power <db>
(Instant AP)(RF dot11a Radio Profile)# smart-antenna
(Instant AP)(RF dot11a Radio Profile)# csa-count <count>
```

The following CLI commands disable VHT on a 5 GHz radio profile:

```
(Instant AP)(config)# rf dot11a-radio-profile
(Instant AP)(RF dot11a Radio Profile)# very-high-throughput-disable
```

The following CLI command shows the radio configuration:

```
(Instant AP)# show radio config

2.4 GHz:
Legacy Mode:enable
Beacon Interval:100
802.11d/802.11h:enable
Interference Immunity Level:2
Channel Switch Announcement Count:0
MAX Distance:600
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable

5.0 GHz:
Legacy Mode:enable
Beacon Interval:100
802.11d/802.11h:enable
Interference Immunity Level:2
Channel Switch Announcement Count:2
MAX Distance:600
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable
Standalone Spectrum Band:5ghz-upper
```

Configuring Cell Size Reduction using the CLI

The Cell Size Reduction feature allows you to manage dense deployments and to increase overall system performance and capacity by shrinking an Instant APs receive coverage area, thereby minimizing co-channel interference and optimizing channel reuse.

The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value.

Values from 1 dB–55 dB reduce the power level that the radio can hear by that amount. If you configure this feature to use a non-default value, you must also reduce the radio's transmission power to match its new received (Rx) power level. Failure to match a device's Tx power level to its Rx power level can result in a configuration that allows the radio to send messages to a device that it cannot hear.

The following CLI commands configure Cell Size Reduction for 2.4 GHz radio profile in the CLI:

```
(Instant AP)(config)# rf dot11g-radio-profile
(Instant AP)(RF dot11g Radio Profile)# cell-size-reduction <reduction>
```

The following CLI commands configure Cell Size Reduction for 5 GHz radio profile in the CLI:

```
(Instant AP)(config)# rf dot11a-radio-profile
(Instant AP)(RF dot11a Radio Profile)# cell-size-reduction <reduction>
```

ARM Channel Selection using the CLI

Instant APs can search for a new environment in a short span of time, so that the ARM is triggered to perform frequent scanning and selection of a valid channel for transmission.

By default, the ARM is triggered to scan all the channels every 10 seconds, and select the best channel for transmission. But when the Instant AP is in a new environment, ARM is triggered to perform frequent scanning of the non-DFS channels every 200 milliseconds, and select the best available channel for transmission. The **ap-frequent-scan** command is introduced in the CLI to enable the Instant APs to trigger frequent scanning of transmission signals on a radio profile.



Wireless connection is affected for a few seconds when the frequent scanning of non-DFS channels is ongoing. The connection is re-established after the ARM selects a valid channel. Typically, a frequent scanning session lasts for less than 10 seconds.

Perform the following checks before scanning:

- The DFS channels must be skipped (this is done to avoid delays in scanning).
- The Instant AP must be on stand-alone mode.
- The **client-aware** parameter must be disabled in the ARM profile.

The following example triggers ARM scanning on a 2.4 GHz frequency band radio profile:

```
(Instant AP)# ap-frequent-scan 2.4
```

The following CLI commands verify the status of ARM scanning:

```
(Instant AP)# show ap debug am-config
```

ARM Controls in Radio Profiles

Traditionally, the ARM settings were managed by a global ARM profile that controlled the behavior of all the AP radios. However, starting from Instant 8.7.0.0, ARM settings can be configured separately for each radio profile in addition to the ARM profile. This enables you to maximize the efficiency of the network in dense RF environments by customizing ARM settings for individual radios.



When configured, the ARM settings defined in the radio profile will take precedence over the settings defined in the ARM profile.

These settings can be configured only through the CLI and are available under **rf dot11g-radio-profile**, **rf dot11a-radio-profile**, and **rf dot11a-secondary-radio-profile** commands.

The following CLI commands configure the ARM settings for the radio profile:

```
(Instant AP)(config) rf <Radio>-radio-profile
(Instant AP)(Radio Profile)#backoff-time <secs>
(Instant AP)(Radio Profile)#channel-quality-aware-arm-disable
(Instant AP)(Radio Profile)#channel-quality-threshold <thresh>
(Instant AP)(Radio Profile)#channel-quality-wait-time <secs>
(Instant AP)(Radio Profile)#error-rate-threshold <percent>
(Instant AP)(Radio Profile)#error-rate-wait-time <secs>
(Instant AP)(Radio Profile)#ideal-coverage-index
(Instant AP)(Radio Profile)#scanning-disable
```

For more information on these settings, see the *Aruba Instant 8.7.0.x CLI Reference Guide*.

Support for channels 169 and 173 on Outdoor Instant AP

Starting from Aruba Instant 8.4.0.0, 5 GHz band on an outdoor Instant AP includes the 169 and 173 channels. These channels are currently supported only in India.

Chapter 22
DPI and Application Visibility

This chapter provides the following information:

- DPI on page 382
- Enabling Application Visibility on page 382
- Application Visibility on page 383
- Enabling URL Visibility on page 383
- Configuring ACL Rules for Application and Application Categories on page 384
- Configuring Web Policy Enforcement Service on page 387

DPI

AppRF is Aruba's custom-built Layer 7 firewall capability. It consists of an onboard DPI and a cloud-based Web Policy Enforcement service that allows creating firewall policies based on types of application. The WPE capabilities require the Instant AP to have a WPE subscription. For more information on subscription, contact the Aruba Sales Team.

Instant APs with DPI capability analyze data packets to identify applications in use and allow you to create access rules to determine client access to applications, application categories, web categories, and website URLs based on web reputation. You can also define traffic-shaping policies such as bandwidth control and QoS per application for client roles. For example, you can block bandwidth-monopolizing applications on a guest role within an enterprise.

The AppRF feature provides application visibility for analyzing client traffic flow. Instant APs support the power of both in-device packet flow identification and dynamically updated cloud-based web categorization.

Enabling Application Visibility

Enabling AppRF visibility allows you to view the AppRF statistics for an Instant AP or the clients associated with an Instant AP. Full URL visibility for HTTP sessions fed to ALE is exposed as northbound APIs which can be consumed by URL analytical engines for advanced client URL data mining and analytics.

The webcc statistics are also periodically sent to Aruba Central. This includes the URL hostname, Application ID, Application category, Web ID, and Web Reputation information. This function is currently supported only for IPv4 addresses.

The following procedure describes how to enable AppRF visibility by using the WebUI.

Table 156: *Enabling Application Visibility*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **System** > **General** section. 2. Select **All** from the **AppRF visibility** drop-down list to view both application and web categories charts or	1. Navigate to **System** > **General**. 2. Select **All** from the **AppRF visibility** drop-down list to view both application and web categories charts or select either **App** or **WebCC** to view

New WebUI	Old WebUI
select either **App** or **WebCC** to view their DPI graphs separately. 3. Click **Save**.	their DPI graphs separately. 3. Click **OK**.

The following CLI command enables AppRF visibility:

```
(Instant AP)(config)# dpi [app|webcc]
```

The following CLI command shows all the current webcc URL prefix entries:

```
(Instant AP)#show dpi webcc-url-prefix-table [referenced|unreferenced]
```

Application Visibility

The AppRF graphs are based on DPI application and Web Policy Enforcement service, which provide application traffic summary for the client devices associated with an Instant AP. The **AppRF** link above the activity panel of the dashboard is displayed only if **AppRF visibility** is enabled in the old or new WebUI.

The AppRF dashboard presents four different graph areas with data graphs on all client traffic and content filters based on App Category, Web Category, and Web Reputation. Click each category to view the real-time client traffic data or usage trend in the last 15 minutes or 1 minute.

The **permit** and **deny** monitoring tabs in the All Traffic and Web Content sections provide enforcement visibility support.

- **Permit** represents the allowed or permitted traffic on the Instant AP.
- **Deny** represents all the blocked URLs and traffic .

Application Categories Chart

The application categories chart displays details on the client traffic towards the application categories. By clicking the rectangle area, you can view the graphs and toggle between the chart and list views.

Applications Chart

The applications chart displays details on the client traffic towards the applications. By clicking the rectangular area, you can view the graphs and toggle between the chart and list views.

Web Categories Charts

The web categories chart displays details about the client traffic to the web categories. By clicking the rectangle area, you can view the graphs and toggle between the chart and list views.

Web Reputation Charts

The web reputation chart displays details about the client traffic to the URLs that are assigned security ratings. By clicking in the rectangle area, you can view the graphs and toggle between the chart and list views.

Enabling URL Visibility

Enabling URL visibility allows the Instant AP to extract the full URL information of the HTTP and HTTPS sessions and periodically log them on the ALE server. Full URL visibility for HTTP sessions fed to ALE are

exposed as Northbound APIs, and are used by URL analytical engines for advanced client URL data mining and analysis.

The following procedure describes how to enable URL visibility by using the WebUI.

Table 157: *Enabling URL Visibility*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **System** > **General** page. 2. Toggle the **URL visibility** switch to enable. 3. Click **Save**.	1. Navigate to **System** > **General**. 2. Select **Enabled** from the **URL visibility** drop-down list. 3. Click **OK**.

The following CLI command enables URL visibility:

```
(Instant AP)(config)# url-visibility
```



Instant APs extract DPI web-based URL sessions and provide the statistics to ArubaCentral. ArubaCentral compiles this information with the AppRF feed to obtain complete details.

Configuring ACL Rules for Application and Application Categories

This section describes the procedure for configuring access rules based on application and application categories. The Application and Application rules utilize the onboard DPI engine.

- For information on configuring access rules to control access to network services, see Configuring ACL Rules for Network Services on page 260.
- For information on configuring access rules based on web categories and web reputation, see Configuring Web Policy Enforcement Service on page 387.

The following procedure describes how to configure ACL rules for a user role.

Table 158: *Configuring ACL Rules for Application and Application Categories*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Security** > **Roles** section. You can also configure access rules for a wired or wireless network profile by following the steps mentioned below: a. Navigate to **Configuration** > **Networks**. b. Select the WLAN or the Wired profile and edit the profile as required. c. Go to the **Access** tab. 2. In the **Roles** section, select the role for which you want to configure the access rules. 3. In the **Access Rules for <network>** section, click **+** to add a new rule. The **New rule** window is displayed. 4. Ensure that the rule type is set to **Access control**. 5. To configure access to applications or application category, select a service from the following list:	1. Navigate to the **Security** > **Roles** tab. The **Roles** tab contents are displayed.You can also configure access rules for a wired or wireless network profile by using: a. The WLAN wizard (**Network** > **WLAN SSID** > **Edit** > **Edit WLAN** > **Access**) or b. The Wired profile (**More** > **Wired** > **Edit** > **Edit Wired Network** > **Access**) window. 2. In the **Roles** section, select the role for which you want to configure the access rules. 3. In the **Access rules** section, click **New** to add a new rule. The **New Rule** window is displayed. 4. Ensure that the rule type is set to **Access control**. 5. To configure access to applications or application category, select a service category from the

New WebUI	Old WebUI
a. Application b. Application category 6. Based on the selected service category, configure the parameters described in the Access Rule Configuration Parameters table below. 7. Click **OK**. 8. Click **Save**.	following list: 6. Application 7. Application category 8. Based on the selected service category, configure the parameters described in the Access Rule Configuration Parameters table below. 9. Click **OK** in the **New Rule** window. 10. Click **OK** in the **Roles** tab.

Table 159: *Access Rule Configuration Parameters*

Service Category	Description
Application	Select the applications to which you want to allow or deny access.
Application category	Select any of the following application categories to which you want to allow or deny access: ■ antivirus ■ authentication ■ cloud-file-storage ■ collaboration ■ encrypted ■ enterprise-apps ■ gaming ■ im-file-transfer ■ instant-messaging ■ mail-protocols ■ mobile-app-store ■ network-service ■ peer-to-peer ■ social-networking ■ standard ■ streaming ■ thin-client ■ tunneling ■ unified-communications ■ web ■ Webmail

Table 159: *Access Rule Configuration Parameters*

Service Category	Description
Application Throttling	Application throttling allows you to set a bandwidth limit for an application, application category, web category, or for sites based on their web reputation. For example, you can limit the bandwidth rate for video streaming applications such as YouTube or Netflix, or assign a low bandwidth to high-risk sites. If your Instant AP model does not support configuring access rules based on application or application category, you can create a rule based on web category or website reputation and assign bandwidth rates. This check-box is visible only when the service selected is **Application**. To specify a bandwidth limit: 1. Select the **Application Throttling** check box. 2. Specify the downstream and upstream rates in Kbps.
Action	Select any of following actions: ■ Select **Allow** to allow access to users based on the access rule. ■ Select **Deny** to deny access to users based on the access rule. ■ Select **Destination-NAT** to allow changes to destination IP address. ■ Select **Source-NAT** to allow changes to the source IP address. The destination NAT and source NAT actions apply only to the network services rules.
Destination	Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements. ■ **to all destinations**—Access is allowed or denied to all destinations. ■ **to a particular server**—Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server. ■ **except to a particular server**—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. ■ **to a network**—Access is allowed or denied to a network. After selecting this option, specify the IP address and netmask for the destination network. ■ **except to a network**—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. ■ **to domain name**—Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the **Domain Name** text box. ■ **to master IP**—Access is allowed or denied to the master IP address. ■ **to AP IP**—Access is allowed or denied to a specific AP's IP address. ■ **to AP network**—Access is allowed or denied to a specific AP network.
Log	Select this check box to create a log entry when this rule is triggered. Instant supports firewall-based logging function. Firewall logs on the Instant APs are generated as security logs.
Blacklist	Select the **Blacklist** check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified in **Auth failure blacklist time** on the Blacklisting tab of the **Security** window. For more information, see Blacklisting Clients on page 251.

Table 159: *Access Rule Configuration Parameters*

Service Category	Description
Disable scanning	Select **Disable scanning** check box to disable ARM scanning when this rule is triggered. The selection of the **Disable scanning** applies only if ARM scanning is enabled. For more information, see Configuring Radio Settings on page 377.
DSCP tag	Select the **DSCP tag** check box to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0–63. To assign a higher priority, specify a higher value.
802.1p priority	Select the **802.1p priority** check box to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value.
802.1p priority	Select the **Time Range** check box and select a time profile to apply for the rule.

The following CLI commands configure access rules:

```
(Instant AP)(config)# wlan access-rule <access-rule-name>
(Instant AP)(Access Rule <Name>)#rule <dest> <mask> <match/invert> {app <app>
{permit|deny}|appcategory <appgrp>}[<option1....option9>]
```

The following CLI example shows how to configure employee access rules:

```
(Instant AP)(config)# wlan access-rule employee
(Instant AP)(Access Rule "employee")# rule any any match app  youtube permit throttle-
downstream 256 throttle-up 256
(Instant AP)(Access Rule "employee")# rule any any match appcategory collaboration
permit
(Instant AP)(Access Rule "employee")# rule any any match any any any permit time-range
lunchtime
```

The following CLI example shows how to view the list of time profiles created on the Instant AP:

```
(Instant AP)# show time-profile
```

The following CLI example shows how to view the list of time range profiles configured on the Instant AP:

```
(Instant AP)# show time-range
```

Configuring Web Policy Enforcement Service

The following procedure describes how to configure the WPE service on an Instant AP to block certain categories of websites based on your organization specifications by defining ACL rules by using the WebUI or the CLI:

Table 160: *Configuring Web Policy Enforcement Service*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Security** > **Roles** section.	1. Navigate to **Security** > **Roles**. 2. Under **Roles** , select any WLAN SSID or wired

New WebUI	Old WebUI
2. Under **Roles** , select any WLAN SSID or wired profile role, and click **+** in the **Access Rules for <network>** section. The **New rule** window is displayed. 3. Select the rule type as **Access control**. 4. To set an access policy based on the web category: a. Under **Service**, slect the **Web category** radio button and expand the corresponding drop-down list that contains the web categories. b. Select the categories to which you want to deny or allow access. You can also search for a web category and select the required option. c. From the **Action** drop-down list, select **Allow** or **Deny** as required. d. Click **OK**. e. Click **Save**. 5. To filter access based on the security ratings of the website: a. Select **Web reputation** under **Service**. b. Move the slider to the required security rating level. Move the slider to select a specific web reputation value to deny access to websites with a reputation value lower than or equal to the configured value or to permit access to websites with a reputation value higher than or equal to the configured value. The following options are available: ▪ **Trustworthy**—These are well known sites with strong security practices and may not expose the user to security risks. There is a very low probability that the user will be exposed to malicious links or payloads. ▪ **Low risk**—These are benign sites and may not expose the user to security risks. There is a low probability that the user will be exposed to malicious links or payloads. ▪ **Moderate risk**—These are generally benign sites, but may pose a security	profile role, and click **New** in the **Access Rules for <network>** section. The **New Rule** window is displayed. 3. Select the rule type as **Access Control**. 4. To set an access policy based on the web category: a. Under **Service**, click the **Web category** radio button and expand the drop-down list that contains the web categories. b. Select the categories to which you want to deny or allow access. You can also search for a web category and select the required option. c. From the **Action** drop-down list, select **Allow** or **Deny** as required. d. Click **OK** in the **New Rule** window. e. Click **OK** in the **Roles** tab. 5. To filter access based on the security ratings of the website: a. Select **Web reputation** under **Service**. b. Move the slider to the required security rating level. Move the slider to select a specific web reputation value to deny access to websites with a reputation value lower than or equal to the configured value or to permit access to websites with a reputation value higher than or equal to the configured value. The following options are available: ▪ **Trustworthy**—These are well known sites with strong security practices and may not expose the user to security risks. There is a very low probability that the user will be exposed to malicious links or payloads. ▪ **Low risk**—These are benign sites and may not expose the user to security risks. There is a low probability that the user will be exposed to malicious links or payloads. ▪ **Moderate risk**—These are generally benign sites, but may pose a security risk. There is some probability that the

New WebUI	Old WebUI
risk. There is some probability that the user will be exposed to malicious links or payloads. ▪ **Suspicious**—These are suspicious sites. There is a higher than average probability that the user will be exposed to malicious links or payloads. ▪ **High risk**—These are high-risk sites. There is a high probability that the user will be exposed to malicious links or payloads. c. From the **Action** drop-down list, select **Allow** or **Deny** as required. **NOTE:** For a complete list of categories and information about each of these categories, visit the BrightCloud® Security Services web page at http://www.brightcloud.com/tools/change-request-url-ip.php. 6. To set a bandwidth limit based on web category or web reputation score, select the **Application Throttling** check box and specify the downstream and upstream rates in Kbps. For example, you can set a higher bandwidth for trusted sites and a low bandwidth rate for high-risk sites. 7. If required, select the following check boxes : ▪ Log ▪ Blacklist ▪ DSCP tag ▪ Disable scanning ▪ 802.1p priority 8. Click **OK**. 9. Click **Save**.	user will be exposed to malicious links or payloads. ▪ **Suspicious**—These are suspicious sites. There is a higher than average probability that the user will be exposed to malicious links or payloads. ▪ **High risk**—These are high-risk sites. There is a high probability that the user will be exposed to malicious links or payloads. c. From the **Action** drop-down list, select **Allow** or **Deny** as required. **NOTE:** For a complete list of categories and information about each of these categories, visit the BrightCloud® Security Services web page at http://www.brightcloud.com/tools/change-request-url-ip.php. 6. To set a bandwidth limit based on web category or web reputation score, select the **Application Throttling** check box and specify the downstream and upstream rates in Kbps. For example, you can set a higher bandwidth for trusted sites and a low bandwidth rate for high-risk sites. 7. If required, select the following check boxes : ▪ Log ▪ Blacklist ▪ Disable scanning ▪ DSCP tag ▪ Time Range ▪ 802.1p priority 8. Click **OK** in the **New Rule** window. 9. Click **OK** in the **Roles** tab.

The following CLI commands control access based on web categories and security ratings:

```
(Instant AP)(config)# wlan access-rule <access_rule>
(Instant AP)(Access Rule "<access-rule>")# rule <dest> <mask> <match> webcategory
<webgrp> {permit | deny}[<option1....option9>]
(Instant AP)(Access Rule "<access-rule>")# rule <dest> <mask> <match> webreputation
<webrep> {permit | deny}[<option1....option9>]
```

The following CLI example shows how to set access rules based on the web category and the web reputation:

```
(Instant AP)(config)# wlan access-rule URLFilter
(Instant AP)(Access Rule "URLFilter")# rule any any match webcategory gambling  deny
(Instant AP)(Access Rule "URLFilter")# rule any any match webcategory training-and-
tools permit
(Instant AP)(Access Rule "URLFilter")# rule any any match webreputation suspicious-
sites deny
```

This chapter explains the steps required to configure voice and video services on an Instant AP for VoIP devices, SIP, SVP, H323, SCCP, Vocera, and Alcatel NOE phones, clients running Microsoft OCS, and Apple devices running the Facetime application.

This section includes the following topics:

- WMM Traffic Management on page 391
- Media Classification for Voice and Video Calls on page 394
- Enabling Enhanced Voice Call Tracking on page 396
- Wi-Fi Calling on page 397
- Unified Communications Manager on page 397

WMM Traffic Management

WMM is a WFA specification based on the IEEE 802.11e wireless QoS standard. WMM works with 802.11a, 802.11b, 802.11g, and 802.11n physical layer standards.

WMM supports the following ACs:

- Voice
- Video
- Best effort
- Background



The bandwidth share percentage configuration for WMM traffic management is not supported on 203H Series, 203R Series, 207 Series, 340 Series, 500 Series, 510 Series, 570 Series, and AP-518 access points.

The following table shows the mapping of the WMM access categories to 802.1p priority values. The 802.1p priority value is contained in a two-byte QoS control field in the WMM data frame.

Table 161: *WMM AC to 802.1p Priority Mapping*

802.1p Priority	WMM Access Category
1	Background
2	
0	Best effort
3	

802.1p Priority	WMM Access Category
4	Video
5	
6	Voice
7	

In a non-WMM or hybrid environment, where some clients are not WMM-capable, you can configure an SSID with higher values for best effort and voice ACs, to allocate a higher bandwidth to clients transmitting best effort and voice traffic.

Configuring WMM for Wireless Clients

The following procedure describes how to configure WMM for wireless clients by using the WebUI.

Table 162: *Configuring WMM for Wireless Clients*

New WebUI	Old WebUI
1. Navigate to the WLAN wizard. ▪ Navigate to **Configuration** > **Networks** and click **+** or ▪ Navigate to **Configuration** > **Networks**, select the WLAN profile, and edit the profile as required. 2. Under **Basic**, click **Show advanced options**. 3. Under **WMM**, specify a **Share** percentage value for the following access categories, in the text box that appears before **%**. You can allocate a higher bandwidth for voice and video traffic than that for other types of traffic based on the network profile. ▪ **Background WMM**—Allocates bandwidth for background traffic such as file downloads or print jobs. ▪ **Best effort WMM**—Allocates bandwidth or best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS. ▪ **Video WMM**—Allocates bandwidth for video traffic generated from video streaming. ▪ **Voice WMM**—Allocates bandwidth for voice traffic generated from the incoming and outgoing voice communication. 4. Click **Next** until **Finish**.	1. Navigate to the WLAN wizard. ▪ Navigate to **Networks** > **New** or ▪ Navigate to **Networks**, select the WLAN profile and click **edit**. 2. Click **Show advanced options** under **WLAN Settings**. 3. In the **WMM** section, specify a percentage value for the following access categories in the corresponding **Share** text box. You can allocate a higher bandwidth for voice and video traffic than that for other types of traffic based on the network profile. ▪ **Background WMM**—Allocates bandwidth for background traffic such as file downloads or print jobs. ▪ **Best effort WMM**—Allocates bandwidth or best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS. ▪ **Video WMM**—Allocates bandwidth for video traffic generated from video streaming. ▪ **Voice WMM**—Allocates bandwidth for voice traffic generated from the incoming and outgoing voice communication. 4. Click **Next** and complete the configurations as required. 5. Click **Finish**.

The following CLI commands configure WMM traffic management for wireless clients:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# wmm-background-share <share>
(Instant AP)(SSID Profile <name>)# wmm-best-effort-share <share>
(Instant AP)(SSID Profile <name>)# wmm-video-share <share>
(Instant AP)(SSID Profile <name>)# wmm-voice-share <share>
```

Mapping WMM ACs and DSCP Tags

The IEEE 802.11e standard defines the mapping between WMM ACs and DSCP tags. You can customize the mapping values between WMM ACs and DSCP tags to prioritize various traffic types and apply these changes to a WMM-enabled SSID profile.

DSCP classifies packets based on network policies and rules. The following table shows the default WMM AC to DSCP mappings and the recommended WMM AC to DSCP mappings.

Table 163: *WMM AC-DSCP Mapping*

DSCP Value	WMM Access Category
8	Background
16	
0	Best effort
24	
32	Video
40	
48	Voice
56	

By customizing WMM AC mappings, all packets received are matched against the entries in the mapping table and prioritized accordingly. The mapping table contains information for upstream (client to Instant AP) and downstream (Instant AP to client) traffic.

The following procedure describes how to configure different WMM to DSCP mapping values for each WMM AC when configuring an SSID profile by using the WebUI.

Table 164: *Configuring WMM ACs and DSCP Tags for SSID Profiles*

New WebUI	Old WebUI
1. Navigate to the WLAN wizard. ▪ Go to **Configuration** > **Networks** and click **+** or ▪ Go to **Configuration** > **Networks**, select the WLAN profile, and edit the profile as required. 2. Under **Basic**, click **Show advanced options**. 3. Under **WMM**, specify the appropriate DSCP mapping values within a range of 0–63 for the following access categories in the text box that appears after **%**.	1. Navigate to the WLAN wizard. ▪ Navigate to **Networks** > **New** or ▪ Navigate to **Networks**, select the WLAN profile and click **edit**. 2. Click **Show advanced options** under **WLAN Settings**. 3. Click **Show advanced options**. 4. In the **WMM** section, specify the appropriate DSCP mapping values within a range of 0–63 for the following access categories in the corresponding **DSCP mapping** text box:

New WebUI	Old WebUI
▪ **Background WMM**—DSCP mapping for the background traffic. ▪ **Best effort WMM**—DSCP mapping for the best-effort traffic. ▪ **Video WMM**—DSCP mapping for the video traffic. ▪ **Voice WMM**—DSCP mapping for the voice traffic. 4. Click **Next** until **Finish**.	▪ **Background WMM**—DSCP mapping for the background traffic. ▪ **Best effort WMM**—DSCP mapping for the best-effort traffic. ▪ **Video WMM**—DSCP mapping for the video traffic. ▪ **Voice WMM**—DSCP mapping for the voice traffic. 5. Click **Next** and complete the configurations as required. 6. Click **Finish**.

The following CLI commands configure DSCP settings on an SSID:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# wmm-background-dscp <dscp>
(Instant AP)(SSID Profile <name>)# wmm-best-effort-dscp <dscp>
(Instant AP)(SSID Profile <name>)# wmm-video-dscp <dscp>
(Instant AP)(SSID Profile <name>)# wmm-voice-dscp <dscp>
```

You can configure up to 8 DSCP mappings values within the range of 0-63. You can also configure a combination of multiple values separated by a comma, for example, **wmm-voice-dscp 46,44,42,41**.

Configuring WMM U-APSD

To extend the battery life and enable power saving on WLAN clients, Instant APs support U-APSD for the clients that support WMM. The U-APSD or the WMM Power Save feature is enabled by default on all SSIDs. When configured, U-APSD enables a client station to retrieve the unicast QoS traffic buffered in the Instant AP by sending trigger frames. During the association or reassociation with the Instant AP, the station indicates the WMM Access Categories for which U-APSD is enabled. In the current release, Instant APs support U-APSD on all WMM ACs.

The following CLI commands disable U-APSD on an SSID:

```
(Instant AP)(config)# wlan ssid-profile <ssid_profile>
(Instant AP)(SSID Profile "<ssid_profile>")# wmm-uapsd-disable
```

The following CLI commands re-enable U-APSD on an SSID:

```
(Instant AP)(config)# wlan ssid-profile <ssid_profile>
(Instant AP)(SSID Profile "<ssid_profile>")# no wmm-uapsd-disable
```

Media Classification for Voice and Video Calls

Media classification and data prioritization for voice and video calls in Instant is handled automatically by the Instant AP's firewall for traffic that is allowed by wired ports and user ACLs. The firewall inspects each UDP packet, classifies it as either Voice or Video and correspondingly sets a DSCP value for the packet.

Traffic that is allowed in the network is configured using ACL rules. The Instant AP's firewall automatically allows voice and video call sessions from Skype for Business and Apple Facetime. For all other Skype for Business and Facetime applications such as desktop sharing and file transfer the corresponding ports must be opened using ACL rules.

Before media transmission, a VOIP client may initiate a Session Traversal Utilities for NAT (STUN) connectivity check and establishes a session. STUN sessions are subjected to media classification and are marked as RTP or non-RTP traffic. The RTP traffic is classified as either voice or video and re-marked with the corresponding DSCP values configured in the SSID profile, while the non-RTP traffic is forwarded without re-marking. If data packets are found to be non-compliant with the RTP parameters required in the datapath for classification, the session is marked as best effort and no flags or DSCP is set.



The default DSCP values for calls prioritized by media classification is 48 for a voice session and 40 for a video session.

If AppRF is enabled on the SSID, **alg-rtp** must be explicitly permitted in the ACL to allow voice and video traffic in the network. The following is the ACL entry to allow RTP traffic and configuring this is highly recommended:

```
(Instant AP)(VOIP-acl)# rule any any match app alg-rtp permit
```



If AppRF is enabled and alg-rtp is not allowed, no voice or video traffic will flow through the network.

When AppRF is enabled, applications must be permitted explicitly in the ACL using their app IDs for the Instant AP to allow that particular traffic to flow in the network. Allowing application traffic is necessary for establishing control sessions only after which a voice or video session is established. To obtain full inspection and control of voice and video traffic you can populate an ACL permitting particular apps. The following is a recommended ACL configuration for an SSID profile:

```
(Instant AP)(config)# wlan access-rule VOIP-acl
(Instant AP)(VOIP-acl)# rule any any match app alg-facetime permit
(Instant AP)(VOIP-acl)# rule any any match app alg-facetime-audio permit
(Instant AP)(VOIP-acl)# rule any any match app alg-ftp permit
(Instant AP)(VOIP-acl)# rule any any match app alg-h323 permit
(Instant AP)(VOIP-acl)# rule any any match app alg-jabber-audio permit
(Instant AP)(VOIP-acl)# rule any any match app alg-jabber-desktop-sharing permit
(Instant AP)(VOIP-acl)# rule any any match app alg-jabber-mc permit
(Instant AP)(VOIP-acl)# rule any any match app alg-jabber-video permit
(Instant AP)(VOIP-acl)# rule any any match app alg-noe permit
(Instant AP)(VOIP-acl)# rule any any match app alg-rtp permit
(Instant AP)(VOIP-acl)# rule any any match app alg-rtsp permit
(Instant AP)(VOIP-acl)# rule any any match app alg-sccp permit
(Instant AP)(VOIP-acl)# rule any any match app alg-sip permit
(Instant AP)(VOIP-acl)# rule any any match app alg-sip-audio permit
(Instant AP)(VOIP-acl)# rule any any match app alg-sip-video permit
(Instant AP)(VOIP-acl)# rule any any match app alg-skype4b-app-sharing permit
(Instant AP)(VOIP-acl)# rule any any match app alg-skype4b-audio permit
(Instant AP)(VOIP-acl)# rule any any match app alg-skype4b-desktop-sharing permit
(Instant AP)(VOIP-acl)# rule any any match app alg-skype4b-file-transfer permit
(Instant AP)(VOIP-acl)# rule any any match app alg-skype4b-secure permit
(Instant AP)(VOIP-acl)# rule any any match app alg-skype4b-video permit
(Instant AP)(VOIP-acl)# rule any any match app alg-svp permit
(Instant AP)(VOIP-acl)# rule any any match app alg-vocera permit
(Instant AP)(VOIP-acl)# rule any any match app alg-wifi-calling permit
(Instant AP)(VOIP-acl)# end
(Instant AP)# commit apply
```

Alternatively, users can define an higher precedence **allow-all** rule in the ACL which will allow all application, video and voice traffic in the network without having to permit them explicitly. The following is the ACL configuration to allow all traffic:

```
(Instant AP)(config)# wlan access-rule allow-all
```

```
(Instant AP)(allow-all)# rule any any match any any any permit
```

WebRTC Prioritization

The webRTC prioritization feature prioritizes the media traffic from webRTC sources. WebRTC is an open framework for the web that enables real time communication using a web browser. WebRTC includes the fundamental building blocks for high-quality communication on the web like network, audio, and video components that are used in voice, video, and chat applications.

WebRTC prioritization provides better end user experience, dashboard visibility of all WebRTC applications like voice, video, and application sharing, and call quality monitoring for audio calls using upstream and downstream RTP analysis. Ensure that you enable DPI on the AP before enabling WebRTC prioritization.

Enabling Enhanced Voice Call Tracking

Aruba Instant provides seamless support for tracking VoIP calls in the network by using SNMP to send the location details of the caller to the third-party server. This feature is currently applied for tracking Emergency 911 VoIP calls.

The Master Instant AP identifies the location from where the VoIP call was placed and sends the details of the location to the third-party SNMP server. You must configure the third-party server as an SNMP host and enable SNMP traps to activate the voice call tracking feature on the Instant AP. For more information on configuring a third-party server as an SNMP host, see Configuring SNMP on page 506.

The Master Instant AP will send the WLSXIAPVOICECLIENTLOCATIONUPDATE SNMP trap under the following scenarios:

- The VoIP call is successful.
- The VoIP client roams from one Instant AP to another during an active call, the Master Instant AP will identify the VoIP client and send out the WLSXIAPVOICECLIENTLOCATIONUPDATE trap to the emergency call server.



The trap sending feature is not supported for L3 mobility.

The WLSXIAPVOICECLIENTLOCATIONUPDATE trap contains the following information:

Table 165: *SNMP Trap Details for VoIP Calls*

Parameter	Description
wlsxTrapVcIpAddress	IP address of the VoIP client.
wlsxTrapVcMacAddress	MAC address of the VoIP client.
wlsxTrapAPMacAddress	MAC address of the Instant AP which generated the trap.
wlsxTrapAPName	Name of the Instant AP which generated the trap.

SNMP GET

In order to find the location of a particular emergency caller, the third-party SNMP server sends a query to the Master Instant AP using SNMP GET. The Master Instant AP responds back to the SNMP server

with the location (Instant AP Name) of the VoIP caller. Following are the key parameters in the response sent by the Master Instant AP:

- VoIP Client IP Address
- VoIP Client MAC Address
- Instant AP MAC Address
- Instant AP Name

Wi-Fi Calling

Wi-Fi calling service allows cellular users to make or receive calls using a Wi-Fi network instead of using the cellular network of the carrier. The users can make or receive calls, and send text messages even when they are beyond a cellular coverage but have a Wi-Fi network coverage. Most major carriers around the world support Wi-Fi calling service.

Wi-Fi Calling Operation

At a high level, this is how Wi-Fi calling operates:

1. Wi-Fi Calling-capable handset initiates a DNS query to locate the evolved Packet Data Gateway (ePDG) of the carrier.
2. The handset establishes a persistent IPsec tunnel with ePDG.
3. Calls, text, and traffic for other services offered by the carrier are carried over in this IPsec tunnel.

Some carriers use a standard FQDN format for ePDG that includes their Mobile Network Code (MNC) and Mobile Country Code (MCC). For example, T-Mobile uses ss.epdg.epc.mnc260.mcc310.pub.3gppnetwork.org. Others follow a different standard format. For example, AT&T uses epdg.epc.att.net.

Wi-Fi Calling Configuration

The Instant CLI allows you to enable the wi-fi calling service and also configure DNS patterns. The ACL in access-rules to allow IPSEC/IKE (4500 port) enables Wi-Fi calling.

The following CLI command enables Wi-Fi calling:

```
wlan access-rule rule any any match tcp 4500 4500 permit
```

The following CLI command configures DNS patterns:

```
(Instant AP)(config)# wificall-dns-pattern <dns_pattern>
```

The following CLI command shows the list of IP addresses learned by the Wi-Fi calling client during the DNS learning phase:

```
(Instant AP)# show datapath dns-ip-learning
```

Unified Communications Manager

Unified Communications Manager (UCM) is a service module introduced in Aruba Instant 8.7.0.0 that manages the prioritization of voice and video call traffic in the AP. It enables the prioritization and monitoring of voice and video applications that use SIP.

Voice and video calling applications exchange SIP control packets before establishing a voice or video session. The UCM process on the AP identifies these SIP control packets and prioritizes the corresponding session in the datapath. These sessions are tagged with default DSCP value of 48 for voice sessions and 40 for video sessions.



UCM does not support NAT

If a custom port is used for SIP other than port **5060**, the port must be added to the list of netservice ports for UCM to function. Ports can be added to the netservice list using the CLI.

The following CLI command adds a port to the list of netservice ports on the Instant AP:

```
(Instant AP)(config) #netservice svc-sip <port> <proto> <timeout>
```

Monitoring UCM operations on the Instant AP

UCM call data records and ongoing UCM datapath operations are logged in the AP. To view logs of UCM processes on the AP, UCM logging must be enabled using the CLI. The following CLI operations describe how to access logs related to UCM.

The following CLI command enables logging of UCM processes on the Instant AP:

```
(Instant AP) #ucm-logging
```

The following CLI command displays the UCM logs:

```
(Instant AP) #show log ucm
```

The following CLI command displays UCM call data records on the Instant AP:

```
(Instant AP)# show ucm cdrs
```

The following CLI command displays the datapath sessions for UCM packets:

```
(Instant AP)# show datapath session dpi
```

The datapath entries of voice and video sessions that use SIP are marked as **alg-sip-audio** and **alg-sip-video** respectively.

The following CLI command displays the UCC datapath sessions on the AP:

```
(Instant AP)# show datapath session ucc
```

Flows programmed with OpenFlow are tagged with **O** flag in the datapath session.

For more information on these commands, see *Aruba Instant 8.7.0.x CLI Reference Guide*.

Chapter 24
Services

This chapter provides information on how to configure the following services on an Instant AP:

- Configuring AirGroup on page 399
- Configuring an Instant AP for RTLS Support on page 408
- Configuring an Instant AP for ALE Support on page 410
- Clarity Live on page 411
- Deny Intra-VLAN Traffic on page 413
- Integrating an Instant AP with Palo Alto Networks Firewall on page 414
- Integrating an Instant AP with an XML API Interface on page 415
- CALEA Integration and Lawful Intercept Compliance on page 419

Configuring AirGroup

AirGroup provides a unique enterprise-class capability that leverages zero configuration networking to enable AirGroup services from mobile devices efficiently. Zero configuration networking enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. It is designed for flat, single-subnet IP networks such as wireless networking at home. The users can register their personal devices and define a group of users who can share the registered devices. Administrators can register and manage an organization's shared devices such as printers and grant global access to each device, or restrict access according to the username, role, or user location.

In large universities and enterprise networks, it is common for devices to connect to the network across VLANs. As a result, user devices on a specific VLAN cannot discover a service that resides on another VLAN. As the addresses used by the protocol are link-scope multicast addresses, each query or advertisement can only be forwarded on its respective VLAN, but not across different VLANs. Broadcast and multicast traffic are usually filtered out from a WLAN network to preserve the airtime and battery life. This inhibits the performance of AirGroup services that rely on multicast traffic. AirGroup addresses this challenge with AirGroup technology.

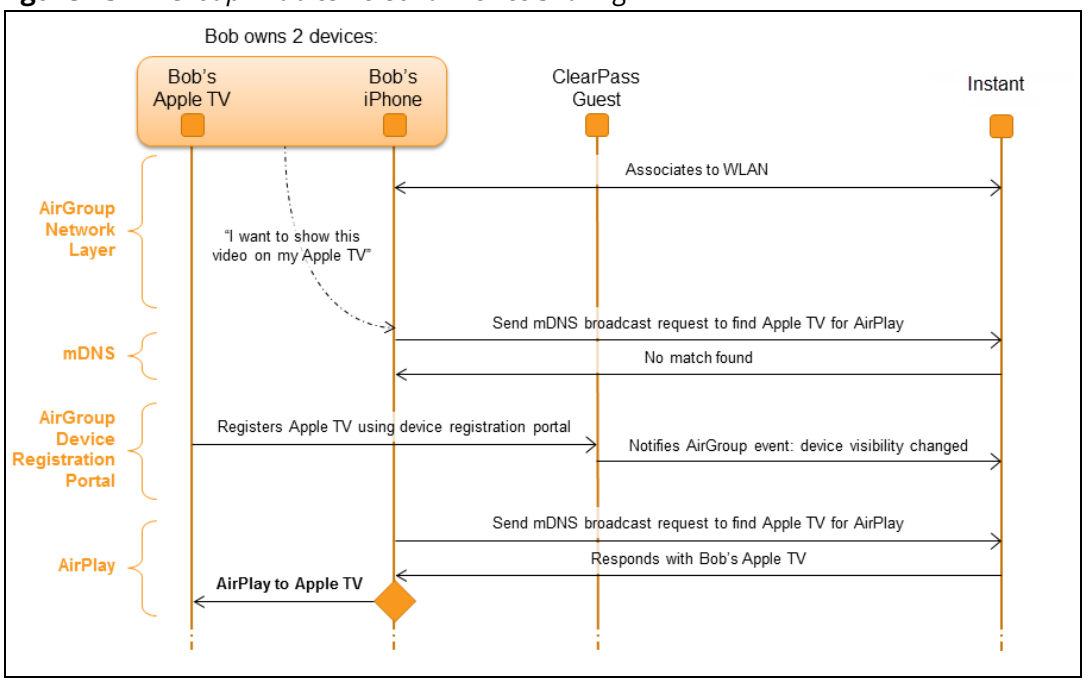
The distributed AirGroup architecture allows each Instant AP to handle mDNS and DLNA queries and responses individually instead of overloading a network with these tasks. This results in a scalable AirGroup solution.

The AirGroup solution supports both wired and wireless devices. An AirGroup device can be registered by an administrator or a guest user.

1. The AirGroup administrator gives an end user the AirGroup operator role, which authorizes the user to register the client devices on the ClearPass Policy Manager platform.
2. Instant APs maintain information for all AirGroup services. Instant AP queries ClearPass Policy Manager to map each device’s access privileges to the available services and responds to the query made by a device based on contextual data such as user role, username, and location.

The following figure illustrates how AirGroup enables personal sharing of Apple devices:

Figure 15 *AirGroup Enables Personal Device Sharing*



NOTE

AirGroup is not supported on 3G and PPPoE uplinks.

For Apple TV mirroring to work, both Apple TV and users must be on either virtual controller-assigned VLANs or network-assigned VLANs. Otherwise, Apple TV mirroring will not work.

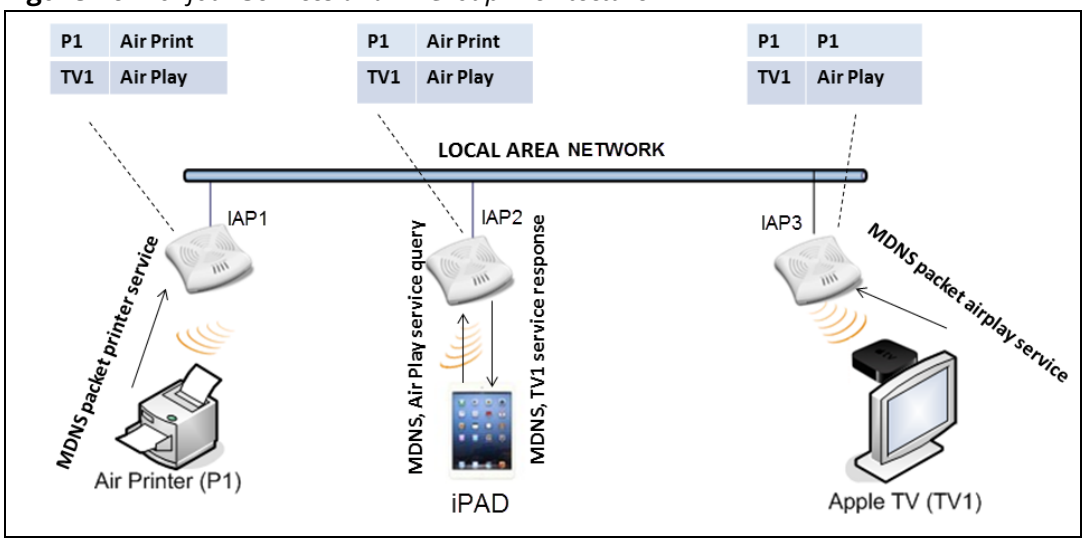
Multicast DNS and Bonjour® Services

Bonjour is the trade name for the zero configuration implementation introduced by Apple. It is supported by most of the Apple product lines, including the Mac OS X operating system, iPhone, iPod Touch, iPad, Apple TV, and AirPort Express. Apple AirPlay and AirPrint services are based on the Bonjour protocol and are essential services in campus Wi-Fi networks.

Bonjour can be installed on computers running Microsoft Windows® and is supported by the new network-capable printers. Bonjour is also included with popular software programs such as Apple iTunes, Safari, and iPhoto. Bonjour uses mDNS to locate devices and the services offered by these devices.

As shown in the following figure, the Instant AP1 discovers AirPrint (P1) and Instant AP3 discovers Apple TV (TV1). Instant AP1 advertises information about its connected P1 device to the other Instant APs that is Instant AP2 and Instant AP3. Similarly, Instant AP3 advertises TV1 device to Instant AP1 and Instant AP2. This type of distributed architecture allows any Instant AP to respond to its connected devices locally. In this example, the iPad connected to Instant AP2 obtains direct response from the same Instant AP about the other Bonjour-enabled services in the network.

Figure 16 *Bonjour Services and AirGroup Architecture*



For a list of supported Bonjour services, see AirGroup Services on page 403.

Multicast DNS Server Cache Age Out Behavior

When a mDNS wireless server disconnects abruptly from the Instant AP, the server entries and the server cache entries will be removed when the inactivity time reaches its threshold limit. The server and cache entries from other Instants in the swarm will subsequently be removed once they receive an update from the database sync messages.

Users can configure the AirGroup wireless mDNS server cache to age out timer using the following command:

```
(Instant AP)(config)# wlan ssid-profile <inactivity-timeout>
```

NOTE

This change is applicable only for wireless mDNS servers and not for DLNA servers or wired servers.

DLNA UPnP Support

In addition to the mDNS protocol, Instant APs now support UPnP, and DLNA enabled devices. DLNA is a network standard derived from UPnP, which enables devices to discover the services available in a network. DLNA also provides the ability to share data between the Windows or Android-based multimedia devices. All the features and policies applicable to mDNS are extended to DLNA to ensure full interoperability between compliant devices.

In a UPnP-based scenario, the following types of devices are available in a network:

- Controlled devices (servers)
- Control points (clients)

When a controlled device joins a network and acquires IP address, it multicasts a number of discovery messages for advertising itself, its embedded devices, and services. On the other hand, when a control point joins a network, it may multicast a search discovery message for finding interesting devices and services. The devices listening on the multicast address respond if they match the search criteria in the search message.

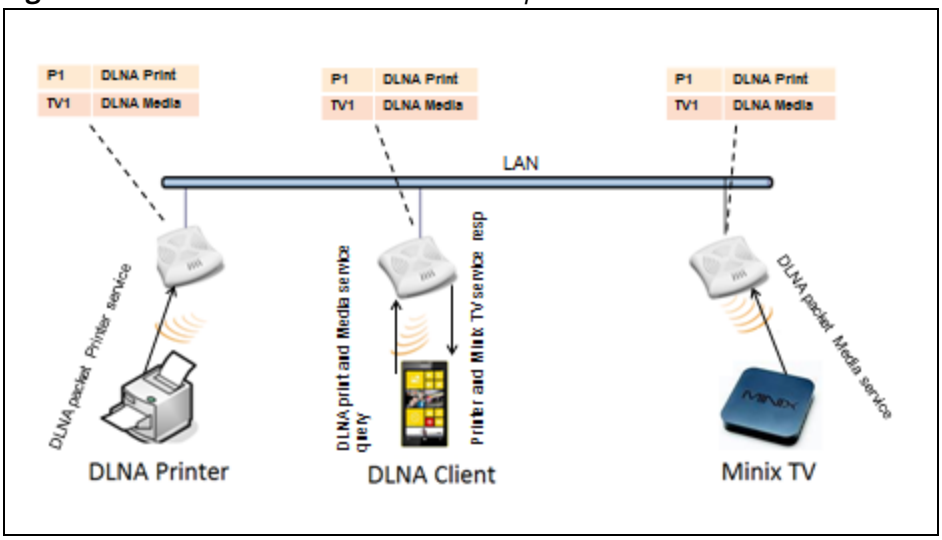
In a single Instant AP network, the Instant AP maintains a cache table containing the list of discovered services in the network. The Instant AP also enforces native policies such as disallowing roles and VLANs and the policies defined on ClearPass Policy Manager to determine the devices or services that are allowed and can be discovered in the network. Whenever a search request comes, the Instant AP looks

up its cache table and filters the cached data, based on configured policies, then builds a search response, and unicasts it to the requesting device.

In an Instant AP cluster, the Instant APs maintain a list of associated UPnP devices and allow the discovery of the associated devices.

The following figure illustrates DLNA UPnP Services and AirGroup Architecture.

Figure 17 *DLNA UPnP Services and AirGroup Architecture*



For a list of supported DLNA services, see AirGroup Services on page 403.

AirGroup Features

AirGroup supports the following features:

- Sends unicast responses to mDNS or DLNA queries and reduces the traffic footprint.
- Ensures cross-VLAN visibility and availability of AirGroup devices and services.
- Allows or blocks AirGroup services for all users.
- Allows or blocks AirGroup services based on user roles.
- Allows or blocks AirGroup services based on VLANs.
- Matches devices to their closest services such as printers.
- In a multiple cluster scenario, when a client roams from one cluster to another, allowing or blocking of a service based on the user role or the VLAN depends upon configuration settings of the new cluster. For example, a user role is not allowed to access a service on one cluster but is allowed to access the same service on another cluster. In this case, the client will receive the configuration of the new cluster in which they can access the service.

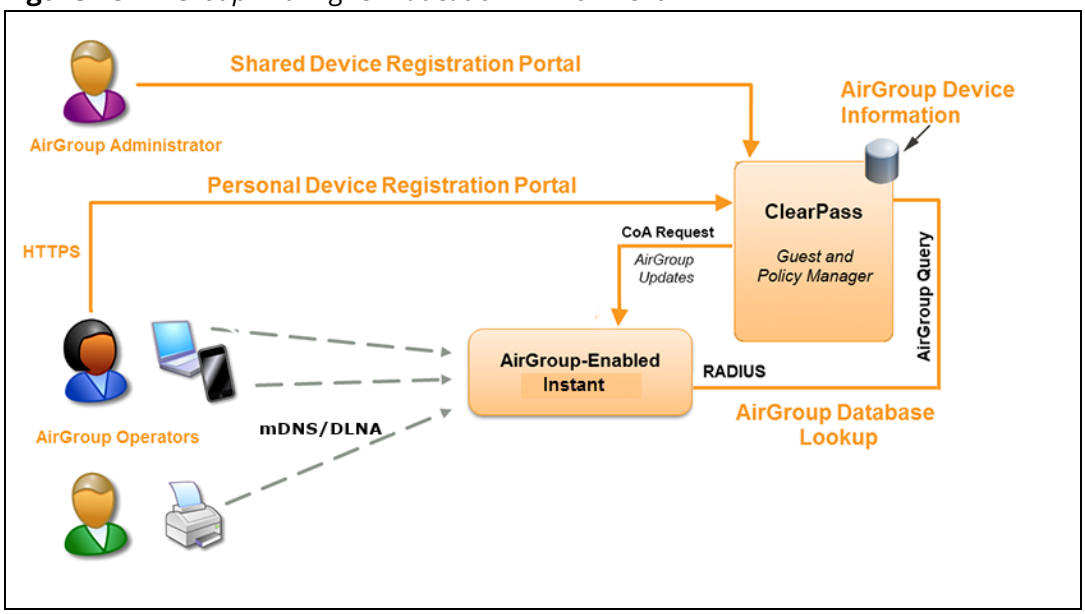
AirGroup also enables context awareness for services across the network:

- AirGroup is aware of personal and shared devices. For example, an Apple TV in a dorm room can be associated with the student who owns it or an Apple TV in a meeting room or a printer in a supply room that is available to certain users, such as the marketing department.
- AirGroup is aware of the location of services when ClearPass Policy Manager support is enabled. For example, depending on the proximity, a user would be presented with the closest printer instead of all the printers in the building.

- When configured, AirGroup enables a client to perform a location-based discovery. For example, when a client roams from one Instant cluster to another, it can discover devices available in the new cluster to which the client is currently connected.

The following figure shows an example of a higher-education environment with shared, local, and personal services available to mobile devices.

Figure 18 *AirGroup in a Higher-Education Environment*



NOTE

When AirGroup discovers a new device, it interacts with ClearPass Policy Manager to obtain the shared attributes such as shared location and role. However, the current versions of Instant APs do not support the enforcement of shared location policy.

AirGroup Services

AirGroup supports zero configuration services. The services are preconfigured and are available as part of the factory default configuration. The administrator can also enable or disable any or all services by using the WebUI or the CLI.

The following services are available for Instant AP clients:

- AirPlay™—Apple® AirPlay allows wireless streaming of music, video, and slide shows from your iOS device to Apple TV® and other devices that support the AirPlay feature.
- AirPrint™—Apple AirPrint allows you to print from an iPad®, iPhone®, or iPod® Touch directly to any AirPrint-compatible printers.
- iTunes—The iTunes service is used by iTunes Wi-Fi sync and iTunes home-sharing applications across all Apple devices.
- RemoteMgmt—The RemoteMgmt service allows remote login, remote management, and FTP utilities on Apple devices.
- Sharing—The Sharing service allows applications such as disk sharing and file sharing among Apple devices.
- ChromeCast—The ChromeCast service allows you to use a ChromeCast device to play audio or video content on a high-definition television by streaming content through Wi-Fi from the Internet or local network.

- DLNA Media—Applications such as Windows Media Player use this service to browse and play media content on a remote device.
- DLNA Print—This service is used by printers that support DLNA.



It is recommended to have a maximum of upto 80 AirGroup servers in the network.

For more information on configuring AirGroup services, see Configuring AirGroup and AirGroup Services on an Instant AP on page 405.

AirGroup Components

AirGroup leverages key elements of the Aruba solution portfolio including operating system software for Instant, ClearPass Policy Manager, and the VLAN-based or role-based filtering options offered by the AirGroup services. The components that make up the AirGroup solution include the Instant AP, ClearPass Policy Manager, and ClearPass Guest. The version requirements are described in the following table:

Table 166: *Instant AP, ClearPass Policy Manager, and ClearPass Guest Requirements*

Component	Minimum Version for mDNS Services	Minimum Version for DLNA Services
Instant Access Point	Instant 6.2.0.0-3.2.0.0	Instant 6.4.0.2-4.1.0.0
ClearPass Policy Manager software	ClearPass Policy Manager 5.2	ClearPass Policy Manager 6.2
ClearPass Guest Services plugin	ClearPass Guest 6.2.0	ClearPass Guest 6.3.0



Starting from ClearPass Policy Managerversion 6.0, the ClearPass Guest and the AirGroup Services plug-in are integrated into a single platform.

AirGroup maintains seamless connectivity between clients and services across VLANs and SSIDs. The following table summarizes the filtering options supported by Instant:

Table 167: *AirGroup Filtering Options*

Features	Instant Deployment Models	
	Integrated with ClearPass Guest	**Integrated with ClearPass Policy Manager**
Allow mDNS and DLNA traffic to propagate across subnets or VLANs	Yes	Yes
Limit mDNS and DLNA traffic on the network	Yes	Yes
VLAN-based AirGroup service policy enforcement	Yes	Yes
User-role-based AirGroup service policy enforcement	Yes	Yes

Table 167: *AirGroup Filtering Options*

Features	Instant Deployment Models	
Portal to self-register personal devices	No	Yes
Device-owner-based policy enforcement	No	Yes
Shared user-list-based policy enforcement	No	Yes
Shared role-list based-policy enforcement	No	Yes

ClearPass Policy Manager and ClearPass Guest Features

ClearPass Policy Manager and ClearPass Guest support the following features:

- Registration portal for WLAN users to register their personal devices.
- Registration portal for WLAN administrators to register shared devices.
- Operator-defined *personal* AirGroup to specify a list of other users who can share devices with the operator.
- Administrator-defined username, user role, and location attributes for shared devices.

Configuring AirGroup and AirGroup Services on an Instant AP

The following procedure describes how to configure AirGroup services by using the WebUI.

Table 168: *Configuring Dynamic DNS Updates for Clients*

New WebUI	Old WebUI
1. Go to **Configuration** > **Services**. 2. Expand **AirGroup**. 3. To enable support for Bonjour services, toggle the **Enable Bonjour** switch to enable and select the AirGroup services related to Bonjour, as required. 4. To enable DLNA support, toggle the **Enable DLNA** switch to enable and select the DLNA services. 5. To allow the users to use Bonjour services enabled in a guest VLAN, toggle the **Enable Guest Bonjour multicast** switch to enable. When enabled, the Bonjour devices are visible only in the guest VLAN and AirGroup will not discover or enforce policies in guest VLAN. 6. Toggle the **Enable AirGroup across mobility domains** switch to enable inter-cluster mobility. When enabled, the Instant AP shares the mDNS database information with the other clusters. The DNS records in the virtual controller can be shared with all the virtual controller configured for L3 Mobility. By default, this feature is disabled. To define clusters, go to **Configuration** > **System** > **L3 Mobility**. 7. Expand **AirGroup Settings**.	1. Click the **More** > **Services** link on the Instant main window. 2. Click the **AirGroup** tab. 3. To enable support for Bonjour services, select the **Enable Bonjour** check box and select the AirGroup services related to Bonjour as required. 4. To enable DLNA support, select the **Enable DLNA** check box and select the DLNA services. 5. To allow the users to use Bonjour services enabled in a guest VLAN, select **Enable Guest Bonjour multicast**. When this check box is enabled, the Bonjour devices are visible only in the guest VLAN and AirGroup will not discover or enforce policies in guest VLAN. 6. Select the **Enable AirGroup across mobility domains** check box to enable inter-cluster mobility. When enabled, the Instant AP shares the mDNS database information with the other clusters. The DNS records in the virtual controller can be shared with all the virtual controller configured for L3 Mobility. By default, this feature is disabled. To define clusters, go to the **System** > **L3 Mobility** tab. 7. Under **AirGroup Service**, ensure that the required

New WebUI	Old WebUI
8. In the **AirGroup Service** section, select the required AirGroup services. To add a service, click **+**. To allow all services, select **allowall**. If a custom service is added in the **AirGroup Service** section, you can add a corresponding service ID by clicking **+** in the **Service ID** section. **NOTE:** ▪ If anInstant AP is upgraded to the current release with the **Enable Bonjour** check box enabled, ensure that the corresponding Bonjour services are selected. ▪ Instant supports the use of up to 6 custom services.	AirGroup services are selected. To add any service, click **New** and add a service. To allow all services, select **allowall**. If a custom service is added, you can add a corresponding service ID by clicking **New** under **Service ID**. **NOTE:** ▪ If anInstant AP is upgraded to the current release with the **Enable Bonjour** check box enabled, ensure that the corresponding Bonjour services are selected. ▪ Instant supports the use of up to 6 custom services.
9. Based on the services configured, you can block any user roles from accessing an AirGroup service and restrict the AirGroup servers connected to a specific set of VLANs from being discovered . The user roles and VLANs marked as disallowed are prevented from accessing the corresponding AirGroup service. You can create a list of disallowed user roles and VLANs for all AirGroup services configured on the Instant AP. For example, ▪ If the **airPlay** service is selected, an option to edit **Disallowed roles** and **Disallowed vlans** is displayed. To block user roles from accessing an AirGroup service, click the corresponding **edit** icon and select the user roles for which you want to restrict access. By default, an AirGroup service is accessible by all user roles configured in your Instant AP cluster. ▪ Similarly, if the **sharing** service is selected, an option to edit **Disallowed roles** and **Disallowed vlans** is displayed. To block VLANs from allowing access to an AirGroup service, click the corresponding **edit** icon and select the VLANs to exclude. By default, the AirGroup services are accessible by users or devices in all VLANs configured in your Instant AP cluster.	8. Based on the services configured, you can block any user roles from accessing an AirGroup service and restrict the AirGroup servers connected to a specific set of VLANs from being discovered . The user roles and VLANs marked as disallowed are prevented from accessing the corresponding AirGroup service. You can create a list of disallowed user roles and VLANs for all AirGroup services configured on the Instant AP. For example, ▪ If the AirPlay service is selected, the **edit** links for the **airplay disallowed roles** and **airplay disallowed vlans** are displayed. To block user roles from accessing an AirGroup service, click the corresponding **edit** link and select the user roles for which you want to restrict access. By default, an AirGroup service is accessible by all user roles configured in your Instant AP cluster. ▪ Similarly, if sharing service is selected, the **edit** links for the **sharing disallowed roles** and **sharing disallowed vlans** are displayed. To block VLANs from allowing access to an AirGroup service, click the corresponding **edit** link and select the VLANs to exclude. By default, the AirGroup services are accessible by users or devices in all VLANs configured in your Instant AP cluster.
10. **ClearPass Settings**—Use this section to configure the ClearPass Policy Manager server, CoA server, and enforce ClearPass registration. ▪ **CPPM server 1**—Indicates the ClearPass Policy Manager server information for AirGroup policy.	9. **ClearPass Settings**—Use this section to configure the ClearPass Policy Manager server, CoA server, and enforce ClearPass registering. ▪ **CPPM server 1**—Indicates the ClearPass Policy Manager server information for AirGroup policy.

New WebUI	Old WebUI
▪ **Enforce ClearPass registration**—When enabled, only devices registered with ClearPass Policy Manager will be discovered by Bonjour devices, based on the ClearPass Policy Manager policy. 11. Click **Save**.	▪ **Enforce ClearPass registration**—When enabled, only devices registered with ClearPass Policy Manager will be discovered by Bonjour devices, based on the ClearPass Policy Manager policy. 10. Click **OK**.

The following CLI commands configure AirGroup:

```
(Instant AP)(config)# airgroup
(Instant AP)(airgroup)# enable [dlna-only | mdns-only]
(Instant AP)(airgroup)# cppm enforce-registration
(Instant AP)(airgroup)# cppm-server <server>
(Instant AP)(airgroup)# cppm-query-interval <interval>
(Instant AP)(airgroup)# disallow-vlan <vlan-ID>
(Instant AP)(airgroup)# enable-guest-multicast
(Instant AP)(airgroup)# multi-swarm
```

The following CLI commands enable DLNA support:

```
(Instant AP)(config)# airgroup
(Instant AP)(airgroup)# enable dlna-only
```

The following CLI commands enable support for Bonjour services:

```
(Instant AP)(config)# airgroup
(Instant AP)(config)# enable mdns-only
```

The following CLI commands configure AirGroup services:

```
(Instant AP)(config)# airgroupservice <airgroup-service>
(Instant AP)(airgroup-service)# id <airgroupservice-ID>
(Instant AP)(airgroup-service)# description <text>
(Instant AP)(airgroup-service)# disallow-role <role>
(Instant AP)(airgroup-service)# disallow-vlan <vlan-ID>
```

The following CLI command verifies the AirGroup configuration status:

```
(Instant AP)# show airgroup status
```

Configuring AirGroup and ClearPass Policy Manager Interface in Instant

Configure the Instant and ClearPass Policy Manager interface to allow an AirGroup Instant AP and ClearPass Policy Manager to exchange information regarding device sharing, and location. The configuration options define the RADIUS server that is used by the AirGroup RADIUS client.

The AirGroup configuration with ClearPass Policy Manager involves the following steps:

1. Create a RADIUS Server
2. Assign a Server to AirGroup
3. Configure ClearPass Policy Manager to Enforce Registration
4. Configuring CoA

Creating a RADIUS Server

The following procedure describes how to create a RADIUS server in the **AirGroup** window of the WebUI.

Table 169: *Configuring a RADIUS Server*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Services** > **AirGroup**.	1. Navigate to **More** > **Services** > **AirGroup**.

New WebUI	Old WebUI
2. To add a new RADIUS server, go to the **ClearPass Settings** section and click **+** beside the **CPPM server 1** drop-down list. If you want to choose from a list of available servers, select a server from the **CPPM server 1** drop-down list. 3. To create a new RADIUS server, click **+** and configure the parameters are required. 4. Click **OK**. 5. Click **Save**.	2. In the **ClearPass Settings** section, select **New** from the **CPPM server 1** drop-down list. 3. Configure the parameters are required. 4. Click **OK**.

You can configure an external RADIUS Security window. For more information on configuring ClearPass Policy Manager server, see External RADIUS Server on page 231.

Assigning a Server to AirGroup

To associate the ClearPass Policy Manager server with AirGroup, select the ClearPass Policy Manager server from the **CPPM Server 1** drop-down list of the old WebUI.



If two ClearPass Policy Manager servers are configured, the CPPM server 1 acts as a primary server and the CPPM server 2 acts as a backup server.

After the configuration is complete, this particular server will be displayed in the **CPPM server 1** drop-down list. To view this server, go to **More** > **Services** > **AirGroup** > **ClearPass Settings** > **CPPM server 1** in the old WebUI.

To view this server in the new WebUI, go to **Configuration** > **Services** > **AirGroup** > **ClearPass Settings** > **CPPM server 1** or **CPPM server 2**.

Configuring ClearPass Policy Manager to Enforce Registration

When ClearPass Policy Manager registration is enforced, the devices registered with ClearPass Policy Manager will be discovered by Bonjour devices, based on the ClearPass Policy Manager policy.

Configuring CoA

When a RADIUS server is configured with CoA with the ClearPass Policy Manager server, the guest users are allowed to register their devices. For more information on configuring RADIUS server with CoA , see External RADIUS Server on page 231.

Configuring an Instant AP for RTLS Support

Instant supports the real-time tracking of devices when integrated with the AMP or a third-party RTLS server such as Aeroscout RTLS server. With the help of the RTLS, the devices can be monitored in real time or through history.

The following procedure describes how to configure RTLS by using the WebUI or the CLI.

Table 170: *Configuring RTLS Support*

New WebUI	Old WebUI
To configure Aruba RTLS: 1. Go to the **Configuration** > **Services** page. 2. Expand **RTLS**. 3. Under **Instant**, toggle the **RTLS** switch to enable to	To configure Aruba RTLS: 1. Click the **More** > **Services** link on the Instant main window. 2. Click the **RTLS** tab.

New WebUI	Old WebUI
integrate Instant with the AMP or Ekahau RTLS server. 4. In the **IP/FQDN** field, specify the IP address or domain name of the RTLS server. 5. In the **Port** field, enter the port number to which the location reports must be sent. 6. Specify the shared secret key in the **Passphrase** text box. 7. In the **Update** text box, specify the frequency at which the virtual controller can send updates to the RTLS server. You can specify a value within the range of 5–3600 seconds. The default value is 30 seconds. 8. Toggle the **Include unassociated stations** switch to enable to send reports to the RTLS server about the stations that are not associated to any Instant AP. 9. Click **Save**.	3. Under **Aruba**, select the **RTLS** check box to integrate Instant with the AMP or Ekahau RTLS server. 4. Specify the IP address and port to which the location reports must be sent. 5. Specify the shared secret key in the **Passphrase** text box. 6. In the **Update** text box, specify the frequency at which the virtual controller can send updates to the RTLS server. You can specify a value within the range of 5–3600 seconds. The default value is 30 seconds. 7. Select the **Include unassociated stations** check box to send reports to the RTLS server about the stations that are not associated to any Instant AP. 8. Click **OK**.
To configure third-party RTLS such as Aeroscout: 1. Under **3rd party**, toggle the **Aeroscout** switch to send the RFID tag information to an AeroScout RTLS. 2. In the **IP/FQDN** field, specify the IP address or domain name of the Aeroscout RTLS server. 3. In the **Port** field, enter the port number of the AeroScout server to which location reports must be sent. 4. Toggle the **Include unassociated stations** switch to enable to send reports on the stations that are not associated to any Instant AP to the Aeroscout RTLS server. 5. Click **Save**.	To configure third-party RTLS such as Aeroscout: 1. Under **3rd party**, select the **Aeroscout** check box to send the RFID tag information to an AeroScout RTLS. 2. Specify the IP address and port number of the AeroScout server to which location reports must be sent. 3. Select the **Include unassociated stations** check box to send reports on the stations that are not associated to any Instant AP to the Aeroscout RTLS server. 4. Click **OK**.

The following CLI command configures AirWave RTLS:

```
(Instant AP)(config)# airwave-rtls <server> <port> <passphrase> <seconds> include-unassoc-sta
```

The following CLI command configures Aeroscout RTLS:

```
(Instant AP)(config)# aeroscout-rtls <server> <port> include-unassoc-sta
```

Support RTLS Tags with Aruba Central

Starting from Aruba Instant 8.4.0.0, Instant APs are capable of sending data from RTLS tags to Central thereby facilitating WLAN deployments that use an inbuilt RTLS protocol. With the help of Central, you can now track the location of an asset without the use of an RTLS server.

Reporting RTLS Tags to Aruba Central

The Instant AP maintains a dynamic list of the RTLS tags. When the Instant AP listens to a new chirp signal from a tag, it overrides the previous chirp signal and reports the latest data to Central. The list of

RTLS tags is then erased and the Instant AP prepares to maintain a new list of RTLS tags. You can also configure a specific interval during which the data from the RTLS tags should be reported to Central.

You can configure an Instant AP to send RTLS tags to Central using the Instant CLI. Additonaly, you can view the list of RTLS tags and the debug logs for RTLS.

The following CLI command enables reporting RTLS tags to Central:

```
(Instant AP)(config)# report-rtls-to-central
```

The following CLI command sets an interval for reporting RTLS tags to Central:

```
(Instant AP)(config)# report-rtls-to-central-interval <interval>
```

The following CLI command shows the list of RTLS tags:

```
(Instant AP)# show rtls-tags
```

The following CLI command displays the debug logs for the RTLS tags:

```
(Instant AP)# debug-rtls-logs
```

The following CLI command shows all RTLS related logs:

```
(Instant AP)# show rtls-logs
```

The following CLI command shows the RTLS logs from the Instant AP to Central:

```
(Instant AP)# show log rtls-to-cloud
```

Configuring an Instant AP for ALE Support

The ALE is designed to gather client information from the network, process it, and share it through a standard API. The client information gathered by ALE can be used for business purposes by analyzing a client's Internet behavior such as shopping preferences.

ALE includes a location engine that calculates the associated and unassociated device location every 30 seconds by default. For every device on the network, ALE provides the following information through the Northbound API:

- Client username
- IP address
- MAC address
- Device type
- Application firewall data showing the destinations and applications used by associated devices
- Current location
- Historical location

ALE requires the Instant AP placement data to be able to calculate location for the devices in a network.

ALE with Instant

The Instant 6.3.1.1-4.0.0.0 release supports ALE. The ALE server acts as a primary interface to all third-party applications and the Instant AP sends client information and all status information to the ALE server.

To integrate Instant AP with ALE, the ALE server address must be configured on an Instant AP. If the ALE sever is configured with a host name, the virtual controller performs a mutual certificated-based authentication with the ALE server before sending any information.

Enabling ALE Support on an Instant AP

The following procedure describes how to configure an Instant AP for ALE support by using the WebUI.

Table 171: *Configuring ALE Support*

New WebUI	Old WebUI
1. Click **Configuration** > **Services**. 2. Click **RTLS**. 3. In the **Instant** section, toggle the **Analytics & Location Engine** switch to enable. 4. In the **Auth Server** text box, specify the ALE server name or IP address. 5. In the **Report interval** text box, specify the reporting interval within the range of 6–60 seconds. The Instant AP sends messages to the ALE server at the specified interval. The default interval is 30 seconds. 6. Click **Save**.	1. Click **More** > **Services**. 2. Click the **RTLS** tab. 3. Under **Aruba**, select the **Analytics & Location Engine** check box. 4. In the **Server** text box, specify the ALE server name or IP address. 5. In the **Report interval** text box, specify the reporting interval within the range of 6–60 seconds. The Instant AP sends messages to the ALE server at the specified interval. The default interval is 30 seconds. 6. Click **OK**.

The following CLI commands enable Instant AP integration with the ALE server:

```
(Instant AP)(config)# ale-server <server-name | IP-address>
(Instant AP)(config)# ale-report-interval <seconds>
```

Verifying ALE Configuration on an Instant AP

The following CLI command shows the configuration details:

```
(Instant AP)# show ale config
```

The following CLI command verifies the configuration status:

```
(Instant AP)# show ale status
```

Clarity Live

Instant AP provides support for Inline Monitoring support using Clarity Live to identify client connectivity issues and sends user debug data to AirWave. The client connectivity issues can be a problem with the client, Radius Authentication, DHCP, DNS, or it can be delay in the network. Clarity Live is used to identify the root cause of the problem, this feature can be used.

Inline Monitoring

This functionality of Clarity Live helps diagnose client connectivity issues. It provides the network administrator or engineers with more information regarding the exact stage at which the client connectivity fails or provides data where the dhcp or radius server is slow.

The Instant AP collects all information related to user transitions like association, authentication, and dhcp. Then, the Instant AP sends these records to a management server like AirWave. The management server analyzes the data and concludes which dhcp or radius server was not working efficiently causing user connectivity issues. This enhancement allows the management server to isolate WLAN issues caused by external servers such as dhcp or radius.

HTTPS is the data transport protocol used to communicate basic statistics or state changes to AirWave. Inline Monitoring makes use of HTTPS to send the statistics to AirWave too.

The following events are used by Instant AP to send inline monitoring (Clarity Live) updates to AirWave:

- Authentication Failure Events—The statistics or updates shared as part of this event are related to the management frame. These frames are processed by STM and are collected in the user space.

- DHCP Failure Events—In scenarios where the DHCP Server does not respond, information about the failure of the event can be collected by the Instant AP with the help of Clarity Live and sent to AirWave. This functionality receives client DHCP transactions from the control plane.
- DNS Failure Events—The Instant AP measures the responsiveness of each DNS server with the help of Clarity Live. The monitoring includes minimum, maximum, and average response time of each DNS server. A maximum of 16 DNS servers can be monitored at a time and a maximum of 16 DNS server entries are made in the DNS table. If there are no queries from a particular DNS server for a long period of time, the DNS server entry can be removed and replaced with a new DNS server entry. The statistical data collected for the DNS server will be pushed to AirWave before the entry is replaced by a new DNS entry.
- STA Failure Events—The station passive monitor statistic is generated when enabled on the Instant AP. The Instant AP generate the data periodically for every 60 seconds and sends it to AirWave.



All of the above clarity configurations must be enabled or disabled at the same time whether if it is by the WebUI or the CLI. AirWave will drop the message even if one of the four stats is disabled.

The following procedure describes how to configure an Instant AP to generate inline monitoring statistics by using the WebUI.

Table 172: *Configuring Clarity Live*

New WebUI	Old WebUI
1. Go to **Configuration** > **Services**. 2. Expand **Clarity**. The configuration options for the Clarity group are displayed. 3. Toggle the **Inline DHCP stats** switch to enable the Instant AP to generate statistics and update messages for DHCP Failure Events. 4. Toggle the **Inline Sta stats** switch to enable the Instant AP to generate statistics and update messages for STA Failure Events. 5. Toggle the **Inline Auth stats** switch to enable the Instant AP to generate statistics and update messages for Authentication Failure Events. 6. Toggle the **Inline DNS stats** switch to enable the Instant AP to generate statistics and update messages for DNS Failure Events. 7. Click **Save**.	1. Click **More** > **Services**. 2. Click **Clarity**. The configuration options for the Clarity group are displayed. 3. Select the **Inline DHCP stats** check box to enable the Instant AP to generate statistics and update messages for DHCP Failure Events. 4. Select the **Inline Sta stats** check box to enable the Instant AP to generate statistics and update messages for STA Failure Events. 5. Select the **Inline Auth stats** check box to enable the Instant AP to generate statistics and update messages for Authentication Failure Events. 6. Select the **Inline DNS stats** check box to enable the Instant AP to generate statistics and update messages for DNS Failure Events. 7. Click **OK**.

The following CLI commands configure inline monitoring statistics using the CLI:

```
(Instant AP)(config)# clarity
(Instant AP)(clarity)# inline-auth-stats
(Instant AP)(clarity)# inline-dhcp-stats
(Instant AP)(clarity)# inline-dns-stats
(Instant AP)(clarity)# inline-sta-stats
```

Verify Clarity Configuration on Instant AP

The following CLI command shows the status of the Inline Monitoring events:

```
(Instant AP)# show clarity config
```

The following CLI command shows the history of the authentication events:

```
(Instant AP)# show clarity history auth
```

The following CLI command shows the history of the DHCP events:

```
(Instant AP)# show clarity history dhcp
```

The following CLI command shows the history of the DNS events:

```
(Instant AP)# show clarity history dns
```

Deny Intra-VLAN Traffic

Deny Intra-VLAN Traffic feature isolates clients from one another and disables all communication between peers in the VLAN network. Enable this feature to disable all peer-to-peer communication and only allow traffic from client to gateway and whitelisted servers to flow in the network. By doing so all other traffic will be dropped by the Instant AP. This will enhance the security of the network and protects it from vulnerabilities.

When Deny Intra-VLAN Traffic is configured, the Instant AP learns the IP, Subnet Mask, MAC, and other essential information of the gateway and the DNS server and logs it in a subnet of whitelisted destinations. The destination MAC of data packets sent by the client is validated against this subnet table and only those destined to addresses in the subnet table are forwarded by the Instant AP. To add servers in the network, their IP or MAC address must be added to the Intra-VLAN Traffic Whitelist table to serve clients.

Deny Intra-VLAN Traffic feature has the following limitations:

1. This feature is supported only in IPv4 networks.
2. This feature does not support AirGroup functionalities and affects Chromecast and Airplay services.

Aruba recommends that both Deny Intra VLAN Traffic and ARP poison check be configured for enhanced security. To configure ARP poison check, read Configuring Firewall Settings for Protection from ARP Attacks.

The following procedure describes how to configure Deny Intra-VLAN Traffic using the WebUI.

1. Navigate to the **Configuration > Networks** page.
2. Select a network you want to configure Deny Intra-VLAN Traffic and click on **edit**.
3. Click on **Show Advanced Options** and select **Miscellaneous**(for wireless profiles).
4. Toggle the **Deny intra VLAN traffic** switch to enable or disable the feature. When enabled, the **Intra VLAN Traffic Whitelist** option appears.

   For servers to serve the network they must be added to the Intra-VLAN Traffic Whitelist table. The Intra-VLAN Traffic Whitelist is a global whitelist for all WLAN SSIDs and wired networks configured with the feature. Servers are added to this whitelist using its IP or MAC address. To manage the whitelist, click on **Intra VLAN Traffic Whitelist**
5. To add a server to the whitelist, click on **Add** in the Wired Server IP or Wired Server MAC and enter the IP or MAC address of the wired server and click **OK**.
6. To delete a server from the whitelist, select the server entry from the Wired Server IP or Wired Server MAC list and click **Delete**.
7. Click **OK** and save your changes.

The following CLI commands enable Deny Intra VLAN Traffic:

For WLAN SSID profiles

```
(Instant AP)(config) # wlan ssid-profile <profile name>
(Instant AP)(SSID Profile "<profile name>") # deny-intra-vlan-traffic
```

For Wired network profiles

```
(Instant AP)(config) # wired-port-profile <profile name>
```

```
(Instant AP)(wired ap profile "<profile name>") # deny-intra-vlan-traffic
```

Following the above syntax use the **no deny-intra-vlan traffic** command to disable Deny Intra-VLAN Traffic.

The following CLI commands add wired servers to the whitelist:

```
(Instant AP)(config) # intra-vlan-traffic-profile
(Instant AP)(intra-vlan-traffic) # wired-server-ip <ip>
(Instant AP)(intra-vlan-traffic) # wired-server-mac <mac>
```

The following CLI command shows the Intra-VLAN Traffic Whitelist of the network:

```
(Instant AP)(config)# show datapath subnet
```

The following CLI command clears all entries in the datapath subnet table:

```
(Instant AP)# clear datapath subnet all
```

The following CLI command clears all datapath subnet entries of a specific VLAN:

```
(Instant AP)# clear datapath subnet vlan <id>
```

The following CLI command clears a specific ip entry in a specific vlan of the datapath subnet table:

```
(Instant AP)# clear datapath subnet vlan <id> ip <ip>
```

Integrating an Instant AP with Palo Alto Networks Firewall

Palo Alto Networks next-generation firewall offers contextual security for all users for safe enabling of applications. A simple firewall beyond basic IP address or TCP port numbers only provides a subset of the enhanced security required for enterprises to secure their networks. In the context of businesses using social networking sites, legacy firewalls are not able to differentiate valid authorized users from casual social networking users.

The Palo Alto next-generation firewall is based on user ID, which provides many methods for connecting the users to sources of identity information and associating them with firewall policy rules. For example, it provides an option to gather user information from Active Directory or LDAP server.

Integration with Instant

The functionality provided by the Palo Alto Networks firewall based on user ID requires the collection of information from the network. Instant AP maintains the network (such as mapping IP address) and user information for its clients in the network and can provide the required information for the user ID on Palo Alto Networks firewall. Before sending the user-ID mapping information to the Palo Alto Networks firewall, the Instant AP must retrieve an API key that will be used for authentication for all APIs.

Instant AP provides the User ID mapping information to the Palo Alto Networks firewall for integration. The client user id for authentication will not be sent to the Palo Alto Networks firewall unless it has a domain prefix. The Instant AP checks for the domain information in the client username for all login and logout requests sent to the Palo Alto Networks firewall. If the user id already has a domain prefix, Instant AP forwards the request to the Palo Alto Networks firewall. Otherwise, the static client domain configured in the Palo Alto Networks firewall profile will be prefixed to the user id and then sent to the Palo Alto Networks firewall.

Instant AP and Palo Alto Networks firewall integration can be seamless with the XML-API that is available with Palo Alto Networks-OS 5.0 or later.

To integrate an Instant AP with Palo Alto Networks user ID, a global profile is added. This profile can be configured on an Instant AP with Palo Alto Networks firewall information such as IP address, port, username, password, firewall-enabled or firewall-disabled status.

The Instant AP sends messages to Palo Alto Networks based on the type of authentication and client status:

- After a client completes the authentication and is assigned an IP address, Instant AP sends the **login** message.
- After a client is disconnected or dissociated from the Instant AP, the Instant AP sends a **logout** message.

Configuring an Instant AP for PAN integration

The following procedure describes how to configure an Instant AP for Palo Alto Networks firewall integration by using the WebUI.

Table 173: *Configuring Palo Alto Networks Firewall*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Services**. 2. Expand **Network Integration**. The Palo Alto Networks firewall configuration options are displayed. 3. Toggle the **Enable** switch to enable Palo Alto Networks firewall. 4. Provide the user credentials of the Palo Alto Networks firewall administrator in the **Username** and **Password** text boxes. 5. Enter the Palo Alto Networks firewall IP address in the **IP address** field. 6. In the **Port** text box, enter the port number within the range of 1–65,535. The default port is 443. 7. Specify the static **Client domain** to be mapped to the client User IDs that do not have a domain name of its own. 8. Click **Save**.	1. Click **More** > **Services**. 2. Click **Network Integration**. The Palo Alto Networks firewall configuration options are displayed. 3. Select the **Enable** check box to enable Palo Alto Networks firewall. 4. Provide the user credentials of the Palo Alto Networks firewall administrator in the **Username** and **Password** text boxes. 5. Enter the Palo Alto Networks firewall IP address. 6. In the **Port** text box, enter the port number within the range of 1–65,535. The default port is 443. 7. Specify the static **Client domain** to be mapped to the client User IDs that do not have a domain name of its own. 8. Click **OK**.

The following CLI commands enable Palo Alto Networks firewall integration with the Instant AP:

```
(Instant AP)(config)# firewall-external-enforcement pan
(Instant AP)(firewall-external-enforcement pan)# enable
(Instant AP)(firewall-external-enforcement pan)# domain-name <name>
(Instant AP)(firewall-external-enforcement pan)# ip <ip-address>
(Instant AP)(firewall-external-enforcement pan)# port <port>
(Instant AP)(firewall-external-enforcement pan)# user <name> <password>
```

Integrating an Instant AP with an XML API Interface

The XML API interface provides options to create and execute user management operations seamlessly on behalf of the clients or users.

Integration with Instant

The XML API interface allows you to send specific XML commands to an Instant AP from an external server. These XML commands can be used to customize Instant AP client entries. You can use the XML API interface to add, delete, authenticate, query, or blacklist a user or a client.



The user authentication is supported only for users authenticated by captive portal authentication and not for the dot1x-authentication users.

The user add operation performed by the XML API interface is only used to modify the role of an existing user and not to create a new user.

You can now use HTTP or HTTPS to post commands to Instant AP. The communication process using the XML API Interface is as follows:

- An API command is issued in XML format from the server to the virtual controller.
- The virtual controller processes the XML request and identifies where the client is and sends the command to the correct slave Instant AP.
- Once the operation is completed, the virtual controller sends the XML response to the XML server.
- Users can use the response and take appropriate action to suit their requirements. The response from the virtual controller is returned using the predefined formats.

Configuring an Instant AP for XML API integration

The following procedure describes how to configure an Instant AP for XML API integration by using the WebUI. Instant AP supports the configuration of up to 8 XML API server entries.

Table 174: *Configuring XML API Integration*

New WebUI	Old WebUI
1. Go to **Configuration** > **Services**. 2. Expand **Network Integration**. 3. To add an XML API server, click **+** in the **XML API Server Configuration** section. 4. Enter a name for the XML API Server in the **Name** text box. 5. Enter the subnet of the XML API Server in the **Subnet** text box. 6. Enter the subnet mask of the XML API Server in the **Mask** text box. 7. Enter a passcode in the **Passphrase** text box, to enable authorized access to the XML API Server. 8. Re-enter the passcode in the **Retype** box. 9. To add multiple entries, repeat the procedure. 10. Click **OK**. 11. Click **Save**. 12. To edit or delete server entries, use the corresponding icons.	1. Click **More** > **Services**. 2. Click **Network Integration**. 3. To add an XML API server, click **New**. The **New XML API Server** window is displayed. 4. Enter a name for the XML API Server in the **Name** text box. 5. Enter the subnet of the XML API Server in the **Subnet** text box. 6. Enter the subnet mask of the XML API Server in the **Mask** text box. 7. Enter a passcode in the **Passphrase** text box, to enable authorized access to the XML API Server. 8. Re-enter the passcode in the **Retype** box. 9. To add multiple entries, repeat the procedure. 10. Click **OK**. 11. To edit or delete the server entries, use the **Edit** and **Delete** buttons, respectively.

The following CLI commands enable XML API integration with the Instant AP:

```
(Instant AP)(config)# xml-api-server <xml_api_server_profile>
(Instant AP)(xml-api-server <profile-name>)# ip <subnet> [mask <mask>]
(Instant AP)(xml-api-server)# key <key>
```

Creating an XML API Request

You can now create an XML request with an appropriate authentication command and send it to the virtual controller through HTTPS post. The format of the URL to send the XML request is:

```
https://<virtualcontroller-ip/auth/command.xml>
```

- **virtualcontroller-ip**: The IP address of the virtual controller that will receive the XML API request
- **command.xml** : The XML request that contains the XML API command.

The format of the XML API request is:

```
xml=<aruba command="<XML API command>">
<options>Value</options>
...
<options>Value</options>
</aruba>
```

You can specify any of the following commands in the XML request:

Table 175: *XML API Command*

Parameter	Description
user_add	If the user entry is already present in the user table, the command will modify the entry with the values defined in the XML request. For an existing user, this command will update any value that is supplied, with an exception of IP and MAC address. Session time-out is only applicable to captive portal users.
user_delete	This command deletes an existing user from the user table of the virtual controller. **NOTE:** Do not use the **user_delete** command if the intention is to clear the association from the virtual controller user table. If the client is dual-stack, it re-inherits the authentication state from the IPv6 address. If not dual-stack, the client reverts to the initial role.
user_authenticate	This command authenticates against the server group defined in the captive portal profile. This is only applicable to captive portal users.
user_blacklist	This command blacklists a user from connecting to your network. This command uses the default blacklist timeout of 3600 seconds. There is no corresponding clear command.
user_query	This command fetches the status and details of a user connected to your network. A dual-stack client can be queried by any of its IPv4 or IPv6 addresses, but only the queried IP address is displayed in the output.

Each XML API command requires certain mandatory options to successfully execute the task. The list of all available options are:

Table 176: *XML API Command Options*

Parameter	Description	Range / Defaults
ipaddr	IP address of the user in IPv4 or IPv6 format.	—
macaddr	MAC address of the user in aa:bb:cc:dd:ee:ff format.	Enter MAC address with colon.
user	Name of the user.	64-character string

Parameter	Description	Range / Defaults
role	This option is used to change the role of an existing user. This option applies to user_add and user_ delete commands only.	64-character string
password	The password of the user for authentication.	—
session_timeout	The role will be changed to a pre-auto role after session timeout.	—
authentication	Authentication method used to authenticate the message and the sender. You can use any of MD5, SHA-1 or clear text methods of authentication. This option is ignored if shared secret is not configured. It is, however, mandatory if it is configured.	
key	This is the encoded MD5 or SHA-1 hash of shared secret or plain text shared secret. This option is ignored if shared secret is not configured on the switch. The actual MD5 or SHA-1 hash is 16/20 bytes and consists of binary data. It must be encoded as an ASCII-based HEX string before sending. It must be present when the virtual controller is configured with an xml API key for the server. Encoded hash length is 32/40 bytes for MD5 or SHA-1.	
version	The version of the XML API interface available in the virtual controller. This is mandatory in all XML API requests.	Current version is XML API 1.0

SES-imagotag ESL System

Starting from Aruba Instant 8.4.0.0, Instant APs provide support for SES-imagotag's Electronic Shelf Label system. Electronic Shelf Label is used by various retailers to display the price of the products kept on retail shelves. SES-imagotag's Electronic Shelf Label system enables Instant APs to configure ESL-Radio, ESL-Server, label, and client software. The ESL-Radio is a USB dongle that works on 2.4 GHz frequency band. The ESL-Server is a management system that controls product labeling and client software is the control center for all ESL-Servers. These centers help in controlling and executing various tasks such as changing images to labels, assigning tags, resetting labels, refreshing displays, switching to preloaded pages, and so on. By enabling and using ESL system, retail labeling becomes easier and efficient. Aruba Instant APs integrated with SES-imagotag enable access to Wi-Fi and Electronic Shelf Label services simultaneously.



This functionality is supported only on AP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, IAP-335, AP-344, AP-345, AP-514, and AP-515 access points.

The hotplug of Electronic Shelf Label Dongle is supported only on the following platforms: AP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 access points.

The following CLI command configures SES-imagotag's Electronic Shelf Label (ESL) system details:

```
(Instant AP)# sesimagotag-esl-profile
```

The following CLI command shows the status of SES-imagotag's Electronic Shelf Label configuration for an Instant AP:

```
(Instant AP)# show esl status
```

The following CLI command shows the status of Electronic Shelf Label Radio's (USB dongle) traffic:

```
(Instant AP)# show esl-radio status [name]
```

The following CLI command shows the status of the serial communication daemon process:

```
(Instant AP)# show log scd [count]
```

CALEA Integration and Lawful Intercept Compliance

LI allows the Law Enforcement Agencies to perform an authorized electronic surveillance. Depending on the country of operation, the service providers are required to support LI in their respective networks.

In the United States, service providers are required to ensure LI compliance based on CALEA specifications.

Instant supports CALEA integration in a hierarchical and flat topology, mesh Instant AP network, the wired and wireless networks.



Enable this feature only if LI is authorized by a law enforcement agency.

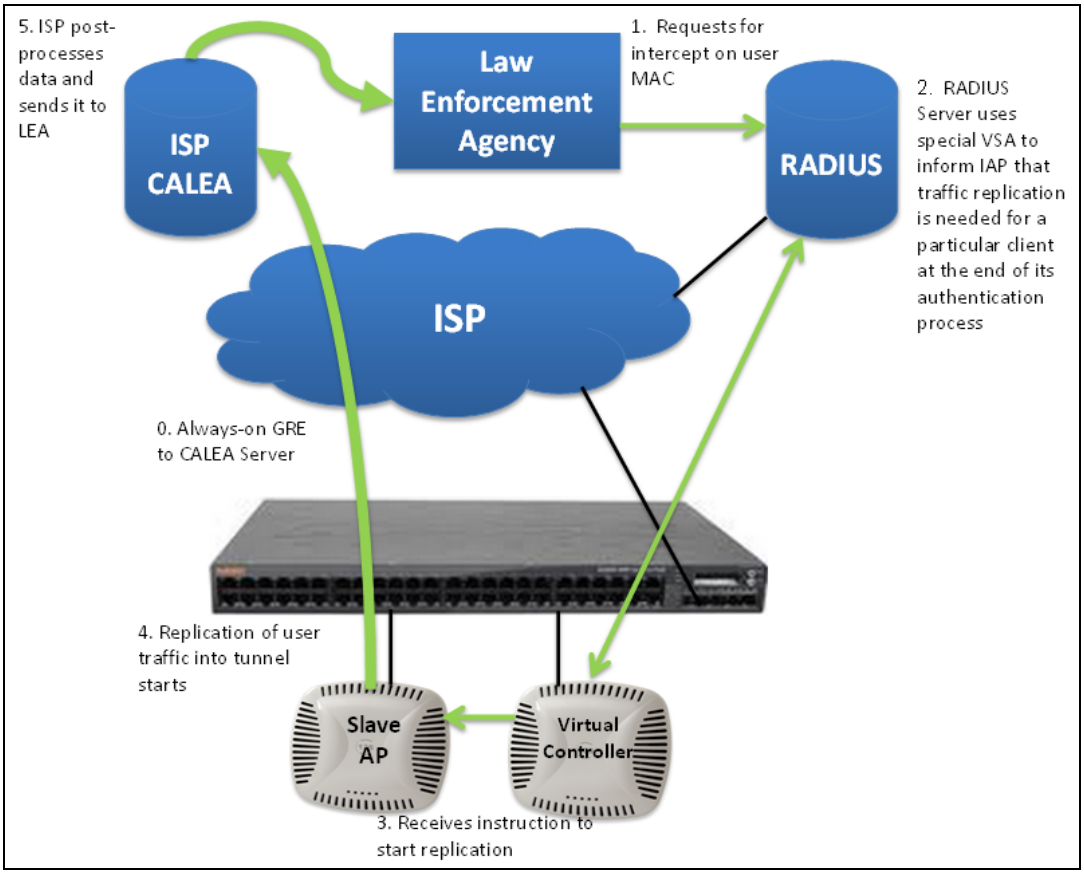
CALEA Server Integration

To support CALEA integration and ensure LI compliance, you can configure the Instant APs to replicate a specific or selected client traffic and send it to a remote CALEA server.

Traffic Flow from Instant AP to CALEA Server

You can configure an Instant AP to send GRE-encapsulated packets to the CALEA server and replicate client traffic within the GRE tunnel. Each Instant AP sends GRE encapsulated packets only for its associated or connected clients. The following figure illustrates the traffic flow from the Instant AP to the CALEA server.

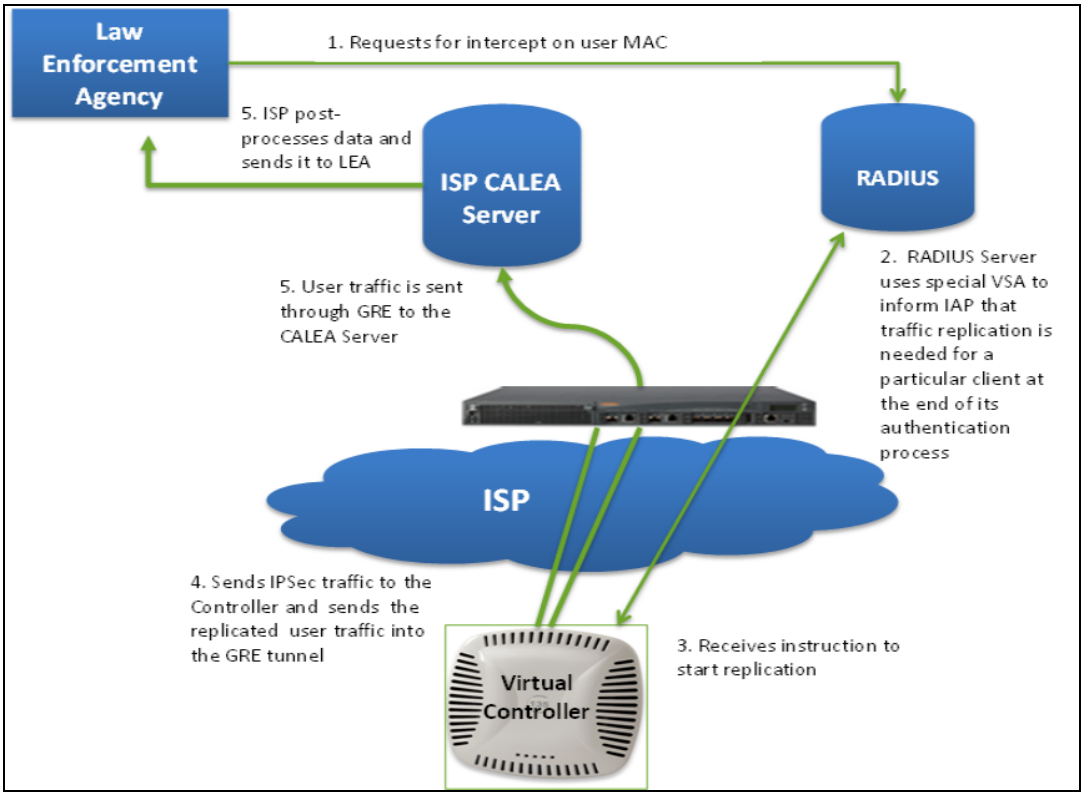
Figure 19 *IAP to CALEA Server*



Traffic Flow from Instant AP to CALEA Server through VPN

You can also deploy the CALEA server with the controller and configure an additional IPsec tunnel for corporate access. When CALEA server is configured with the controller, the client traffic is replicated by the slave Instant AP and client data is encapsulated by GRE on slave, and routed to the master Instant AP. The master Instant AP sends the IPsec client traffic to the controller. The controller handles the IPsec client traffic while GRE data is routed to the CALEA server. The following figure illustrates the traffic flow from Instant AP to the CALEA server through VPN.

Figure 20 *Instant AP to CALEA Server through VPN*



Ensure that IPsec tunnel is configured if the client data has to be routed to the ISP or CALEA server through VPN. For more information on configuring IPsec, see Configuring an IPsec Tunnel on page 319.

Client Traffic Replication

Client traffic is replicated in the following ways:

- Through RADIUS VSA—In this method, the client traffic is replicated by using the RADIUS VSA to assign clients to a CALEA-related user role. To enable role assignment to clients, you need to create a user role and a CALEA access rule, and then assign the CALEA rule to the user role. Whenever a client that is configured to use a CALEA rule connects, a replication role is assigned.
- Through CoA—In this method, a user session can start without replication. When the network administrator triggers a CoA from the RADIUS server, the user session is replicated. The replication is stopped when the user disconnects or by sending a CoA to change the replication role.

As the client information is shared between multiple Instant APs in a cluster, the replication rules persist when clients roam within the cluster.

Configuring an Instant AP for CALEA integration

To enable CALEA server integration, perform the following steps:

1. Create a CALEA profile.
2. If a replication role must be assigned through the RADIUS VSA, create an access rule and assign the access rule to a WLAN SSID or wired profile.
3. Verify the configuration.

Creating a CALEA Profile

The following procedure describes how to create a CALEA profile by using the WebUI.

Table 177: *Creating CALEA Profile*

New WebUI	Old WebUI
1. Go to **Configuration** > **Services**. 2. Expand **CALEA**. 3. Specify the following parameters: 4. **IP address**—Specify the IP address of the CALEA server. 5. **Encapsulation type**—Select the encapsulation type. The current release of Instant supports GRE only. 6. **GRE type**—Specify the GRE type. 7. **MTU**—Specify a size for the MTU within the range of 68–1500. After GRE encapsulation, if packet length exceeds the configured MTU, IP fragmentation occurs. The default MTU size is 1500. 8. Click **Save**.	1. Click **More** > **Services** link on the Instant main window. 2. Click **CALEA**. 3. Specify the following parameters: 4. **IP address**—Specify the IP address of the CALEA server. 5. **Encapsulation type**—Select the encapsulation type. The current release of Instant supports GRE only. 6. **GRE type**—Specify the GRE type. 7. **MTU**—Specify a size for the MTU within the range of 68–1500. After GRE encapsulation, if packet length exceeds the configured MTU, IP fragmentation occurs. The default MTU size is 1500. 8. Click **OK**.

The following CLI commands create a CALEA profile:

```
(Instant AP)(config)# calea
(Instant AP)(calea)# ip <IP-address>
(Instant AP)(calea)# ip mtu <size>
(Instant AP)(calea)# encapsulation-type <gre>
(Instant AP)(calea)# gre-type <type>
```

Creating an Access Rule for CALEA

The following procedure describes how to create an access rule for CALEA by using the WebUI.

Table 178: *Creating Access Rules for CALEA*

New WebUI	Old WebUI
1. To add a CALEA access rule to an existing profile, select an existing wireless or wired network under **Configuration** > **Networks** and click **Edit**. 2. To add an access rule to a new profile, click **+** under the **Configuration** > **Networks** tab and create a WLAN or wired profile. 3. In the **Access** tab, select the role for which you want create the access rule. 4. Under **Access Rules for <network>**, click **+**. The **New Rule** window is displayed. 5. Select **CALEA** as the **Rule type**. 6. Click **OK**. 7. Create a role assignment rule, if required. 8. Click **Finish**.	1. To add a CALEA access rule to an existing profile, Select an existing wireless network under **Networks** and click **edit** or select a Wired profile in **More** > **Wired** and click **edit**. 2. To add an access rule to a new profile, click **New** under the **Networks** tab and create a WLAN profile or click **More** > **Wired** > **New** and create a wired port profile. 3. In the **Access** tab, select the role for which you want create the access rule. 4. Under **Access Rules**, click **New**. The **New Rule** window is displayed. 5. Select **CALEA** as the **Rule type**. 6. Click **OK**. 7. Create a role assignment rule, if required. 8. Click **Finish**.

The following CLI commands create a CALEA access rule:

```
(Instant AP)(config)# wlan access-rule <name>
```

```
(Instant AP)(Access Rule <name>)# calea
```

The following CLI commands assign the CALEA rule to a user role:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# set-role <attribute>{{equals | not-equals | starts-
with| ends-with | contains}<operator><role> | value-of}
```

The following CLI commands associate the access rule with a wired profile:

```
(Instant AP)(config)# wired-port-profile <name>
(Instant AP)(Wired ap profile <name>)# access-rule-name <name>
```

Verifying the configuration

The following CLI command shows the CALEA configuration:

```
(Instant AP)# show calea config
```

The following CLI command shows the tunnel encapsulation statistics:

```
(Instant AP)# show calea statistics
```

The following example shows how to configure CALEA

To enable CALEA integration:

```
(Instant AP)(config)# calea
```

To enable a CALE access rule:

```
(Instant AP)(config)# wlan access-rule ProfileCalea
(Instant AP)(Access Rule "ProfileCalea")# calea
```

To assign the CALEA rule to user role:

```
(Instant AP)(config)# wlan ssid-profile Calea-Test
(Instant AP)(SSID Profile"Calea-Test")# enable
(Instant AP)(SSID Profile"Calea-Test")# index 0
(Instant AP)(SSID Profile"Calea-Test")# type employee
(Instant AP)(SSID Profile"Calea-Test")# essid QA-Calea-Test
(Instant AP)(SSID Profile"Calea-Test")# opmode wpa2-aes
(Instant AP)(SSID Profile"Calea-Test")# max-authentication-failures 0
(Instant AP)(SSID Profile"Calea-Test")# auth-server server1
(Instant AP)(SSID Profile"Calea-Test")# set-role Filter-Id equals 123456 calea-test
(Instant AP)(SSID Profile"Calea-Test")# rf-band 5.0
(Instant AP)(SSID Profile"Calea-Test")# captive-portal disable
(Instant AP)(SSID Profile"Calea-Test")# dtim-period 1
(Instant AP)(SSID Profile"Calea-Test")# inactivity-timeout 1000
(Instant AP)(SSID Profile"Calea-Test")# broadcast-filter none
(Instant AP)(SSID Profile"Calea-Test")# dmo-channel-utilization-threshold 90
(Instant AP)(SSID Profile"Calea-Test")# local-probe-req-thresh 0
(Instant AP)(SSID Profile"Calea-Test")# max-clients-threshold 64
```

To verify the configuration:

```
(Instant AP)# show calea config

calea-ip :10.0.0.5
encapsulation-type :gre
gre-type :25944
ip mtu : 150
```

To view the tunnel encapsulation statistics:

```
(Instant AP)# show calea statistics

Rt resolve fail : 0
Dst resolve fail: 0
Alloc failure   : 0
Fragged packets : 0
Jumbo   packets : 263
Total Tx fail   : 0
Total Tx ok     : 263
```

BLE IoT for Data Communication

Aruba Instant supports IoT applications through BLE which includes transport mechanisms (such as HTTPS POSTs, WebSockets, and UDP), payload encoding (such as JSON, Protobuf), payload content, and periodicity of information updates.

The APB reports data comprising advertisement and scan response frames from scanned IoT or BLE devices to the BLE daemon (BD) process that runs on an Instant AP. BD classifies the incoming messages based on the signature of known device types. Advertisement and scan response frames for unknown devices are stored in raw format, that is, the payload for each frame type is stored as a hexadecimal string, along with the RSSI value. BD maintains a database of IoT devices with attributes populated for known or classified devices and complete advertisement or scan frames for unclassified devices.

Aruba Instant 8.4.0.0 introduces two new standardized endpoints—Telemetry HTTPS and Telemetry Websocket. The message payload for these two standardized endpoints are constructed based on a published Telemetry JSON schema file and Protobuf format respectively. Additionally, Instant supports two new device classes from EnOcean. With these new endpoints provide the capability of choosing multiple payload content from various device classes in the existing IoT transport profile.

- **Endpoint**—The following IoT endpoints are currently supported:
  - Telemetry HTTPS
  - Telemetry WebSocket
  - Authentication URL—JWT with Bearer, Cell Size, Threshold Attributes, and Age Out filter
  - Meridian Beacon Management
  - Meridian Asset Tracking
  - UID-Namespace Filter for Eddystone beacon protocol
  - URL Filter for Eddystone beacon protocol
  - ZF Openmatics.
- **Payload Content**—The payload content is the list of the classified devices that is sent to the endpoints.
  - Ability Smart Sensor
  - Managed beacons—Contains the attributes that are recognized by Aruba-specific APB. Typically, these attributes are communicated to the Meridian Editor.
  - Managed Tags—Contains the asset tag MAC address, RSSI, MAC address of observer or APB and timestamp.
  - Eddystone
  - EnOcean Sensors
  - EnOcean Switches
  - iBeacon—Filter Attributes for iBeacon UUID
  - ZF Tags—Contains the attributes that are recognized for the ZF tags.
  - Wiliot
  - Mysphera
  - sBeacon
  - Wi-Fi Association Station
  - Wi-Fi Unassociation Station
  - Wi-Fi Tags
  - Exposure Notification

- Unclassified
- Zigbee Socket Device
- Serial Data

- **Payload Encoding**—The BLE daemon packages the payload to send to a particular endpoint.
  - JSON encoding for beacon management data
  - Protobuf encoding for asset tag data
- **Transport interval** : This indicates the time interval during which the data is sent from the BLE daemon to the BLE relay. The intervals are:
  - Asset tag RSSI data that occurs every 4 seconds from each Instant AP to Meridian.
  - The Aruba beacon management data that is Telemetry HTTPS, Telemetry WebSocket every 1800 seconds (30 minutes) as the data is mostly static.
- **Filter Attributes**—The filter attributes are used to configure a list of UUIDs as a beacon whitelist. All beacons with a UUID in the configured list are reported and others are ignored.
- **Cell Size**—The cell size defines a scanning scope, in meters, for the APB. The cell size does not have a default value. When the cell size is set a specific value and a beacon is observed outside the cell, the beacon is ignored.
- **Threshold Attributes**—The threshold attributes are used to track the movement inside the cell size. If a BLE device that is inside the cell size moves a distance that is less than the change threshold, then the device status is not updated to the server. However, if the BLE device moves a distance that is more than the change threshold, then the device status is reported to the server. With the right threshold value, you can benefit from avoiding unstable event reporting caused by RSSI dithering.
- **Vendor Filter**—The vendor filter is either the vendor name or the vendor ID of the IoT device. The vendor ID is a 2-byte hexadecimal value preceding with 0x in 0xABCD format. The vendor name is a string that can be either a full vendor name (example: Aruba) or a substring of the actual vendor name (example: Aru) and can be case-insensitive. Configure the vendor filter in the IoT transport profile. The vendor filter accepts up to five combinations of vendor names or vendor IDs separated by commas, for example:
  - Aruba, Favendo, HanVit, SoluM, ABB
  - 0xABCD, 0xBCDE, 0xCDEF, 0xDEF0, 0xEF01
  - Aruba, 0xABCD, Favendo, 0xBCDE, HanVit

If more than one vendor name or vendor ID is configured, then any of the matching vendor names or vendor IDs in the vendor filter is applied. A vendor filter is reported only if the vendor data or vendor name is not empty and matches the vendor information configured in the IoT transport profile. If the vendor field is not populated for the IoT devices, the IoT devices are reported because there is not matching vendor filter in the IoT transport profile.

- **Out of Range Timeout**—The Instant AP maintains an IoT or BLE device table for all the scanned tags. When a tag is within the scan range of an Instant AP, the Instant AP observes the tag, and the tag periodically broadcasts updates information like RSSI of the tag. If the tag loses its power and no longer broadcasts information, then the tag is aged out. When an Instant AP does not observe a tag for a period exceeding the timeout value (default value is 120 seconds), the Instant AP performs the following:
  - When the tag is within the cell size and not heard within timeout value, then the Instant AP reports the tag as out of range.
  - When the tag is not heard within 10 minutes, then the Instant AP deletes the tag from the IoT BLE device table.

Starting from Instant 8.4.0.0, administrators can identify Instant APs in Meridian applications based on their names as it is easier to associate an Instant AP's name with its location.

Configuring IoT Transport Profile

The following procedure describes how to configure IoT Transport profiles by using the WebUI.

Table 179: *Configuring IoT Transport Profile*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **Services** > **IoT**. 2. Under the **Transport Streams** section, click **+**. The **New** window will be displayed. 3. Update the **Name**, **Server Type**, **State**, **Server URL**, **Device classes**, **Proxy**, and **Authentication** fields to create a new transport profile. 4. Click **OK**. 5. Click **Save**.	1. Navigate to **More** > **Services** > **IoT**. 2. Under the **IoT Endpoints** section, click **New**. The **New** window will be displayed. 3. Update the **Name**, **Server Type**, **State**, **Server URL**, **Device classes**, **Proxy**, and **Authentication** fields to create a new transport profile. 4. Click **OK**.

The following CLI command configures the IoT transport profile:

```
(Instant AP) (config) # iot transportProfile <name>
```

The following CLI command sets the IoT profile application:

```
(Instant AP) (config) # iot useTransportProfile <Profile>
```

The following CLI command shows the IoT profile status:

```
(Instant AP)# show iot transportProfile
```

Proxy Server

The proxy server configuration in an IoT transport profile allows you to send IoT data to a proxy server that can in turn relay the IoT data to its final destination. This is useful when you cannot establish a direct link with a server that is hosted in the cloud. The proxy server configuration includes the IP address and port number of the proxy sever and the optional username and password to log in to the proxy server.

The following CLI commands configure a proxy server:

```
(Instant AP) (config) # iot transportProfile <name>
(Instant AP) (IoT Transport Profile <name>) # proxyserver <host> <port>
[<username>|<password>]
```

SES-imagotag ESL System

Starting from ArubaInstant 8.4.0.0, Instant APs provide support for SES-imagotag's Electronic Shelf Label system. Electronic Shelf Label is used by various retailers to display the price of the products kept on retail shelves. SES-imagotag's Electronic Shelf Label system enables Instant APs to configure ESL-Radio, ESL-Server, label, and client software. The ESL-Radio is a USB dongle that works on 2.4 GHz frequency band. The ESL-Server is a management system that controls product labeling and client software is the control center for all ESL-Servers. These centers help in controlling and executing various tasks such as changing images to labels, assigning tags, resetting labels, refreshing displays, switching to preloaded pages, and so on. By enabling and using ESL system, retail labeling becomes easier and efficient. ArubaInstant APs integrated with SES-imagotag enable access to Wi-Fi and Electronic Shelf Label services simultaneously.

This functionality is supported only on AP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, IAP-335, AP-344, AP-345, AP-514, and AP-515 access points.

The hotplug of Electronic Shelf Label Dongle is supported only on the following platforms: AP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 access points.

Execute the following commands in the Instant CLI to configure sesimagotag's Electronic Shelf Label services.

The following CLI command configures SES-imagotag's Electronic Shelf Label (ESL) system details:

```
(Instant AP)# sesimagotag-esl-profile
```

The following CLI command shows the status of SES-imagotag's Electronic Shelf Label configuration for an Instant AP:

```
(Instant AP)# show esl status
```

The following CLI command shows the status of Electronic Shelf Label Radio's (USB dongle) traffic:

```
(Instant AP)# show esl-radio status [name]
```

The following CLI command shows the status of the serial communication daemon process:

```
(Instant AP)# show log scd [count]
```

Support for SES-Imagotag Cloud TLS Authentication

Aruba Instant allows an AP with ESL USB dongle to connect to the SES cloud by using TLS authentication. This allows you to configure and update the ESL through the SES cloud. Configure either an IP address or domain name in the SES profile in the managed device.

The AP initiates a TLS authentication with the SES cloud using an Aruba certificate. After successful authentication, the AP and SES cloud use a session key to communicate with each other. If a ESL USB dongle is unplugged from the AP or the IP address or the domain name is deleted, the session between the AP with ESL USB dongle and the ESL cloud is terminated.

To allow SES-imagotag cloud TLS authentication, configure the SES-Imagotag server name or SES-Imagotag server IP address the AP system profile. The SES-Imagotag server name accepts an FQDN while the SES-Imagotag server IP address accepts an IP address. If both are configured, the SES-Imagotag server name takes higher priority and the SES-Imagotag server IP address does not take effect. If the SES-Imagotag server name is deleted, the SES-Imagotag server IP address takes effect. To disable SES-Imagotag, delete both the SES-Imagotag server name and SES-Imagotag server IP address.

The following CLI command configures an SES-Imagotag server name:

```
(Instant AP)("sesimagotag-esl-profile") #sesimagotag-esl-server <name>
```

The following CLI command configures a SES-Imagotag server IP address:

```
(Instant AP)("sesimagotag-esl-profile") #sesimagotag-esl-serverip <ip_address>
```

The following CLI command deletes a SES-Imagotag server name:

```
(Instant AP)("sesimagotag-esl-profile") #no sesimagotag-esl-server
```

The following CLI command deletes a SES-Imagotag server IP address:

```
(Instant AP)("sesimagotag-esl-profile") #no sesimagotag-esl-serverip
```

Support for MySphera Tag

MySphera is a leading provider of BLE-based asset tracking tags and services. When a MySphera BLE tag broadcasts an advertisement, an AP obtains the RSSI information, computes the location of the tag, and relays the location information to a destination server. A new device class filter, MySphera that matches the server type Telemetry-HTTPS and Telemetry-Websocket to configure the MySphera data in the IoT transport profile.

Support for AmberBox Sensor

Aruba Instant supports AmberBox detectors and gateways that connect to a USB port in an AP. The AP relays the traffic from the detector or gateway to the destination server.

Support for ABB Sensor

Aruba Instant supports the following ABB ability smart sensors and forwards the IoT data from these sensors over Telemetry-HTTPS and Telemetry-websocket server types:

- Motor sensor
- Pump sensor
- Bearing sensor
- Ambient sensor
- ECM drive sensor
- CoMo sensor

Wi-Fi RTLS and BLE Telemetry Streams

The Wi-Fi RTLS and BLE telemetry streams in Aruba Instant are combined into a single telemetry stream in the IoT transport profile. This optimizes the integration of telemetry streams with third party location engines. Three new device class filters, Wi-Fi RTLS tags, Wi-Fi associated stations, and Wi-Fi unassociated stations are introduced in the IoT transport profile. If required, define a MAC address filter for filtering the RTLS tags based on the destination address. If required, enable Wi-Fi client count to send counts instead of the actual device data.



Only aggregated client count per AP for the Meridian Beacons Management server type is sent. Device data is not split based on radio type (2.4 GHz or 5 GHz).

IoT and Third Party Server Integration

Aruba Instant 8.4.0.0 introduces the integration of built-in IoT BLE messages with third party servers. This integration provides a flexible interface for users to build their own endpoint and service without meridian support. Controllers send messages received from Instant AP to the endpoints.

Instant APs send messages and ensure that these messages from multiple Instant APs arrive within the desired frame. The location engine needs only the latest set of messages from the Instant AP.

Instant APs send JSON encoded messages every minute after which, a clean-up of the messages is not required.

Instant APs maintain the current list of BLE or IoT devices. When Instant APs detect a new sound from a beacon or an IoT device, they override the previous sound information in order to send only the latest sound information to the endpoint.

Universal Unique Identifier (UUID) Configuration

A universal unique identifier is a 128-bit number used to uniquely identify an object or an entity on the Internet. Instant enables users to configure universal unique identifiers and these identifiers are used as beacon whitelists. All beacons with the universal unique identifier in the configured list are reported to the endpoints. The remaining beacons are ignored. You can use a separate login message with a configurable username and password to perform authentication for the ignored beacons.

The following CLI commands configure UUID for the IoT profile:

```
(Instant AP) (config) # iot transportProfile <name>
(Instant AP) (IoT Transport Profile "name") # uuidFilter <filter>
```

Configuring a VLAN ID for IoT Telemetry

The IoT telemetry data is transported to multiple users using BLE. The telemetry data is parsed and sent to the server through WSS or HTTPS protocols. To ensure the telemetry data is seamlessly transported to the server, the telemetry traffic should be isolated to a client specific VLAN. and must not reside on

the same VLAN used for the AP management traffic. Follow these steps to configure a client specific VLAN:

The following CLI commands create an interface vlan:

```
(Instant AP)(config)# interface vlan <vlan-id>
(Instant AP)("Interface VLAN <vlan-id>") ip <ip address or domain name>
```

The following CLI command configures a VLAN ID on the IoT Transport Profile:

```
(Instant AP)(config)# iot transportProfile <profile>
(Instant AP)("IoT Transport Profile <profile>")# vlan <vlan-id>
```

Chapter 25
SDN

SDN is an architecture that uses OpenFlow. It enables software programs to manipulate the flow of packets in a network, and manages the traffic to suit the requirements of an application. OpenFlow enables an SDN controller by allowing dynamic manipulation of a forwarding plane of controllers and routers. In an Instant deployment scenario, OpenFlow runs on every master and slave Instant AP. The Instant APs can connect and communicate with the OpenFlow controller over a TCP channel. However encryption between the OpenFlow agent and OpenFlow controller takes place through TLS.

Listed below are the topics included in this chapter:

- OpenFlow for WLAN on page 430
- Clickstream Analysis on page 432
- Wildcard ACL Support on page 432

Functionalities of SDN

Interoperability

With SDN and OpenFlow, it is possible to interoperate with, control, and manage third party devices in the network.

Customization or Programmability

SDN enables network programmability. This flexibility enables customers to build applications that can control and manage network traffic to suit their needs.

OpenFlow for WLAN

Every Instant AP interacts directly with an OpenFlow controller. An Instant AP makes wireless clients connected to the OpenFlow enabled port appear on the OpenFlow controller. When the Instant AP learns about a client connected to the port, the Instant AP sends a gratuitous ARP packet (enclosed in an OpenFlow protocol message) to the OpenFlow controller. Prior to this, the Instant AP exposes all WLAN ports and OpenFlow SSIDs as a logical port to the Openflow controller. This way, OpenFlow controller learns about the hosts on some ports of the Instant AP. When an OpenFlow controller pushes the flow of clients to an Instant AP, it can find out the right Instant AP to which the flow needs to be pushed.

Heuristics and RTPA Support

When OpenFlow agent is enabled, Instant APs can send heuristics and RTP analysis data to the OpenFlow controller. The controller runs as either Service Controller or as Central.

With the current release of Central, heuristics data is supported only for Skype for Business. When heuristics data is sent to Central, it either allows or denies the RTP session. Instant APs send RTP downstream analysis data that includes jitters, delay, packet loss, and RTP count. This information comes directly from the driver for each Instant AP type.

SDN Skype

When an OpenFlow connection is established between Instant APs and Central, and when clients connected to an Instant AP make a Skype call, the Skype server sends the call details to Central. Based on call details received from the Skype server, Central sends OpenFlow enabled flows to the Instant APs. This way, Skype calls initiated by Instant AP clients are given higher precedence and can experience better call quality. Central contains information about the call details and the call quality.

When a Skype call is terminated, its corresponding sessions gradually ageout.



OpenFlow is supported on AP-303P, 303 Series, 318 Series, AP-374, AP-375, AP-377, AP-344, AP-345, AP-203H, AP-303H, AP-365, AP-367, AP-203R, AP-203RP, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, IAP-335, IAP-207, IAP-304, and IAP-305, platforms.

OpenFlow is not supported on Layer-3 mobility profiles and wired profiles.

The following procedure describes how to configure OpenFlow configuration by using the WebUI:

Table 180: *ConfiguringOpenFlow*

New WebUI	Old WebUI
To enable OpenFlow SSID: 1. Go to **Configuration** > **Networks** and click **+** or select a profie from the list of networks and click **Edit**. 2. Under **Basic**, enter a name that uniquely identifies a WLAN network in the **Name** text box. 3. Click **Show advanced options**. 4. Under miscellaneous, toggle the **Openflow** switch to enable.	To enable OpenFlow SSID: 1. On the **Networks** tab of the Instant main window, click the **New** link. The **New WLAN** window is displayed. 2. Enter a name that uniquely identifies a WLAN network in the **Name** text box. 3. Click **Show advanced options**. 4. Select the **Openflow**checkbox.
To enable OpenFlow TLS authentication: 1. Go to **Configuration** > **Services**. 2. Expand **Openflow**. 3. Update the controller IP address in the **OFC IP/FQDN** textbox. 4. Update the port address in the **Port** text box. 5. Toggle the **TLS** switch to enable. 6. Click **Save**.	To enable OpenFlow TLS authentication: 1. Click the **Services** link under **More** on the Instant main window. The **Services** window is displayed. 2. Click the **Openflow** tab. 3. Update the controller IP address in the **OFC IP/FQDN** textbox. 4. Update the port address in the **Port** text box. 5. Select the **TLS** checkbox. 6. Click **OK**.

The following CLI commands configure an OpenFlow enabled SSID in a WLAN profile:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# openflow-enable
```

The following CLI command enables OpenFlow through TCP and TLS channels:

```
(Instant AP)(config)# openflow-server {host <addr> tcp-port <port> | tls-enable}
```

Wired Port Support

Starting from Aruba Instant 8.4.0.0, all clients connected to a wired port will be listed on ACP through the same packet_in method used for wireless ports. For trusted ports, all packets will be sent to ACP through the packet_in method if the packet matches the flow installed using the OpenFlow ACL104. This allows learning of all AirGroup devices connected upstream to ACP.

Clickstream Analysis

Clickstream is a record of user activity on the Internet. Clickstream data is very useful as it helps understand the Internet customer's behavior. Clickstream data is collected either in the form of website log files or in the form of direct decoding of the Internet request data payload.

When customers require HTTP payload related information of the user's web traffic, data is fed to their clickstream analytics engine through Central. To support this, Instant APs use OpenFlow as the SDN protocol to transfer clickstream data from the access point infrastructure to Central.

An Instant AP datapath extracts clickstream data of the HTTP session of every client, and sends it to the OpenFlow agent through a socket. The OpenFlow agent maintains this data in a ring buffer and dumps it into the OpenFlow controller either on a full buffer basis or on a periodic timeout basis. On receiving this message, OpenFlow controller segregates the data based on the flow type and forwards it to the clickstream application for further processing.

The Instant AP datapath can extract six TCP segments for an HTTP POST message. However, it can extract only two TCP segments for other HTTP methods such as GET, HEAD, PUT, PATCH, and DELETE. Instant does not support the extraction of HTTP methods such as TRACE, CONNECT, and OPTIONS.

You can obtain details about a clickstream data feed by executing the **show openflow clickstream-statistics** command on the Instant CLI.



The ring buffer size of clickstream data is modified according to the requirements of the Central deployments.

Wildcard ACL Support

Wildcard ACLs enable ARP requests or responses to match with the ARP flow. The wildcard flow installed by OFC can be programmed to have any of the five tuple information—source IP address, destination IP address, source port, destination port, or protocol. This flow is used to either allow, deny, or send packet count to the Openflow controller.

Wildcard ACL support introduces the following:

- Support for New Openflow Wildcard ACL on page 432
- Wireless Client ARP Handling on page 432
- Packet Out Implementation for mDNS on page 432

Support for New Openflow Wildcard ACL

The OpenFlow wildcard ACL in datapath is 104. When OpenFlow is enabled on an SSID, packets are subjected to ACL 104 in the slow path. Depending on the packet type, the packet is copied to the user space OFALD process. The user space then sends the data in the packet_in format to the OFC.

Wireless Client ARP Handling

OFC installs a wildcard ACL flow that allows matching ARP requests and responses. Accordingly if the ARP request or response matches the ARP flow, a copy of the ARP packet is sent via PACKET_IN to OFC.

Packet Out Implementation for mDNS

When the ARP cache times out on the OFC after 8 minutes, it sends out an ARP request to the Instant AP using the packet out protocol option. When Instant AP receives the packet out, it removes the OpenFlow headers and sends out the ARP packet request to its downstream clients. If the client is still connected

to the SSID, it responds with an ARP response that is in turn sent to the OFC using the packet_in method.

Chapter 26
Cluster Security

Cluster security is a communication protocol that secures control plane messages between Instant access points. Control plane messages such as configuration, cluster join, and other messages distributed between the devices in a cluster are secured using this protocol. Cluster security operates on the UDP port 4434 and uses DTLS protocol to secure messages.

This chapter describes cluster security and the procedure for configuring cluster security DTLS for secure communication. It includes the following topics:

- Enabling Cluster Security on page 435
- ZTP with Cluster Security on page 435
- Low Assurance Devices on page 436
- Cluster Security Debugging Logs on page 437
- Verifying the Configuration on page 438

Cluster Security Using DTLS

Cluster security provides secure communication using DTLS. A DTLS connection is established between the Instant APs communicating with each other in the cluster.

Following are some of the advantages of using DTLS for cluster security:

- Mutual authentication is done between the Instant APs in a cluster using device certificate.
- Peer MAC address validation against **AP whitelist** can be enabled in the configuration.
- Control plane messages between cluster members are transmitted securely using the DTLS connection established.



If auto-join is enabled, backward compatibility and recovery of Instant APs is allowed on ARUBA UDP port 8211. Messages required for image synchronization and cluster security DTLS state synchronization are the only messages allowed.

If auto-join is disabled, the MAC address of a peer Instant AP is verified against the **AP whitelist** during device certificate validation.

Locked Mode Slave Instant AP

A slave Instant AP with non-factory default configuration and DTLS enabled in that configuration is considered to be in locked mode of operation. These slave Instant APs will not be able to join the existing non-DTLS cluster as backward compatibility and recovery is not allowed. This is done for security reasons.

To recover the slave Instant APs in locked mode:

- Execute the **disable-cluster-security-dtls** action command on the slave Instant AP , or
- Factory reset the slave Instant AP.

Enabling Cluster Security

The following procedure describes how to enable cluster security using the WebUI. Ensure that the following pre-requisites are satisfied:

Table 181: *Configuring Cluster Security*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **System** > **General**. 2. Toggle the **Cluster security** switch to enable. 3. Click **Save**.	1. Navigate to **System** > **General**. 2. Select **Enabled** from the **Cluster security** drop-down list. 3. Click **OK**.
NOTE: Reboot all the Instant APs in the swarm for the configuration to take effect.	

Pre-requisites

1. NTP server must be reachable—If internet is reachable, pool.ntp.org will be used by default, otherwise a static NTP server needs to be configured.
2. UDP port 4434 should be permitted.

The following CLI commands enable cluster security:

```
(Instant AP)(config)# cluster-security
(Instant AP)(cluster-security)# dtls
```

The following CLI commands disable cluster security DTLS:

```
(Instant AP)(config)# cluster-security
(Instant AP)(cluster-security)# no dtls
```

The following CLI command changes per module logging level of cluster security:

```
(Instant AP)# cluster-security logging module <module_name> log-level <level>
```

The following CLI command sets individual log level for each module:

```
(Instant AP)# cluster-security logging module <module_name> log-level-individual <level>
```



After enabling or disabling the cluster security option, ensure that the Config Sync Status is TRUE in the output of the show summary command, before rebooting the cluster.

Cluster security is not supported for L3 mobility.

ZTP with Cluster Security

In the earlier versions of Aruba Instant, it was a criteria to disable DTLS on a cluster before provisioning Instant APs through ZTP. The user had to enable DTLS on the cluster once again after ZTP was complete, which proved to be a slightly cumbersome process. A slave Instant AP operating on an image that does not support DTLS could not join the cluster through ZTP. Starting from Aruba Instant 8.4.0.0, certain

enhancements have been made to allow a DTLS disabled slave Instant AP to join a DTLS enabled cluster through ZTP.

Adding Slave Instant APs to DTLS Enabled Clusters

In order for ZTP to succeed when auto-join is disabled, the Instant AP should be added to the list of whitelist APs by Central or AirWave before it joins the cluster.

The following procedure describes how to allow slaves to join a DTLS enabled cluster by using the Instant AP WebUI:

Table 182: *Adding Slave APs to DTLS Enabled Cluster*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **System** > **General** . 2. Click **Show advanced options**. 3. Select **Allow** from the **Non-DTLS Slaves** drop-down list. 4. Click **Save**.	1. Navigate to **System** > **General** . 2. Select **Allow** from the Non-DTLS Slaves drop-down list. 3. Click **OK**.

The following commands allows a slave Instant AP to join a DTLS enabled cluster:

```
(Instant AP)(config)# cluster-security
(Instant AP)(cluster-security)# no disallow-non-dtls-slaves
```

The following CLI commands prevent a DTLS disabled slave Instant AP from joining a DTLS enabled cluster:

```
(Instant AP)(config)# cluster-security
(Instant AP)(cluster-security)# disallow-non-dtls-slaves
```

The following CLI command checks if non-DTLS slave Instant APs are allowed to join a DTLS enabled cluster:

```
(Instant AP)# show cluster-security
```

Low Assurance Devices

Most of the Aruba devices contain a TPM chip that securely stores keys and performs cryptographic operations. However, some devices do not have a TPM chip. So, the unique private keys for those devices are stored in flash. Therefore, the level of protection for the device reduces.

To overcome this challenge, Instant has introduced a new PKI which issues device certificates to non-TPM devices. The device certificates consist of a policy OID indicating that they are issued by the PKI. Non-TPM devices are low assurance devices.

The following new features are introduced in the new PKI:

- SHA-256 is supported.
- Non-TPM devices can be listed in the policy server.
- Policies of new non-TPM Instant APs can be updated

A 256-bit random number generated by non-TPM devices is used to encrypt a private key that is unique to each device. The keys is encrypted by AES encryption. Non-TPM devices compress and store the encrypted private key file and the certificate files in Flash.The private key is maintained in an encrypted format. APIs are provided to applications that use the private key.

The following procedure describes how to allow low assurance devices by using the WebUI:

Table 183: *Allowing Low Assurance Devices to join the Cluster*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **System** > **General**. 2. Click **Show advanced options**. 3. Toggle the **Cluster security** switch to enable. 4. Select **Allow** from the **Low assurance PKI** drop-down list. 5. Click **Save**.	1. Navigate to **System** > **General**. 2. Click **Show advanced options**. 3. Select **Enabled** from the **Cluster security** drop-down list. 4. Select **Allow** from the **Low assurance PKI** drop-down list. 5. Click **OK**.

The following CLI commands allows low assurance devices to join the cluster:

```
(Instant AP)(config)# cluster-security
(Instant AP)(cluster-security)# allow-low-assurance-devices
```



When a DTLS connection is denied to low assurance Instant APs, the connection will not be allowed even if the Instant AP is in the allowed Instant AP whitelist.

If a mixed mode cluster (combination of non-TPM Instant APs and regular Instant APs) is preferred, ensure to set the **low assurance devices** parameter to **allow**.

Zeroization of TPM Keys

Zeroization is a process that involves the erasing of sensitive parameters (electronically stored data, cryptographic keys, and critical security parameters) to prevent their disclosure when a device is compromised.

Instant 8.4.0.0 introduces zeroization of TPM keys in FIPS-based Instant APs under circumstances that present a threat to their integrity such as unauthorized removal of FIPS-based Instant APs, evidence of tampering, and so on.

The following CLI command zeroises TPM keys:

```
(Instant AP)# zeroize-tpm-keys
```

Cluster Security Debugging Logs

Cluster security logging is organized into modules based on functionality. The following are the core modules which are useful and should be used for debugging:

- **peer**—The peer module is used to log connection initiation, renegotiation, collision and active connection updates. The log-level should be set to **debug** level while debugging any issues.
- **conn**—The connection module is used to log connection creation, establishment, data transfer and maintenance updates. The log-level should be set to **debug** level for debugging DTLS connection issues.
- **mcap**—The module capture module is used to log messages sent and received to the socket. Set log-level to **debug** to log only control messages. Set log-level to **debug1** to log control and data messages.

The following CLI command sets per module logging level:

```
(Instant AP)# cluster-security logging module <module_name> log-level <level>
```

Once the log-level is set, logs can be viewed using:

```
(Instant AP)# show log papi-handler
```

Verifying the Configuration

The following CLI command shows current cluster security Configuration and running state

```
(Instant AP)# show cluster-security
```

The following CLI command shows the cluster security statistics:

```
(Instant AP)# show cluster-security stats
```

The following CLI command shows the cluster security connection table:

```
(Instant AP)# show cluster-security connections
```

The following CLI command shows the cluster security peers:

```
(Instant AP)# show cluster-security peers
```

The following CLI command shows the message handler process logs:

```
(Instant AP) # show log papi-handler <count>
```

This chapter provides information on provisioning, managing and monitoring Instant APs from the following management servers:

- Managing an Instant AP from AirWave on page 439
- Managing Instant AP from Aruba Central on page 449
- WebSocket Connection on page 452
- Support for REST API on page 453

Managing an Instant AP from AirWave

AirWave is a powerful platform and easy-to-use network operations system that manages Aruba wireless, wired, and remote access networks, as well as wired and wireless infrastructures from a wide range of third-party manufacturers. With its easy-to-use interface, AirWave provides real-time monitoring, proactive alerts, historical reporting, as well as fast and efficient troubleshooting. It also offers tools that manage RF coverage, strengthen wireless security, and demonstrate regulatory compliance.

AirWave can be used to provision, manage, and monitor a multi-site deployment of Instant networks. For example,if you have 100 retail offices that require Instant to provide WLAN connectivity at each office, AirWave can be used to provision all the 100 offices from a central site. AirWave also provides the administrator with the ability to monitor these geographically dispersed Instant networks using an AirWave server depending on the scalability recommendations for AirWave.

The Instant APs communicate with AirWave using the HTTPS, XML, or Websocket protocol. This allows an AirWave server to be deployed in the cloud across a NAT device, such as a router.

The AirWave features available in the Instant network are described in the following sections:

Image Management

AirWave allows you to manage firmware updates on WLAN devices by defining a minimum acceptable firmware version for each make and model of a device. It remotely distributes the firmware image to the WLAN devices that require updates, and it schedules the firmware updates such that updating is completed without requiring you to manually monitor the devices.

The following models can be used to upgrade the firmware:

- Automatic—In this model, the virtual controller periodically checks for newer updates from a configured URL and automatically initiates upgrade of the network.
- Manual—In this model, the user can manually start a firmware upgrade for each virtual controller or set the desired firmware preference per group of devices.

Resetting an Instant AP

A virtual controller is added to the AirWave database either on management mode or monitor mode based on the AirWave configuration.

An Instant AP device can be reset through AirWave in the **Managed** mode:

1. In the **Modify Devices** section, select the Instant AP devices you want to reset to factory-default by selecting the check box beside it.
2. From the **Change Device Group Folder** drop-down list, select **Factory Reset selected devices**.
3. Click the **Factory Reset** tab.

NOTE

On resetting the Instant AP device from AirWave, all the configuration values will be set to default except for the **per-ap-settings** and **VC Key** value.

Instant AP and Client Monitoring

AirWave allows you to find any Instant AP or client on the wireless network and to see real-time monitoring views. These monitoring views can be used to aggregate critical information and high-end monitoring information.

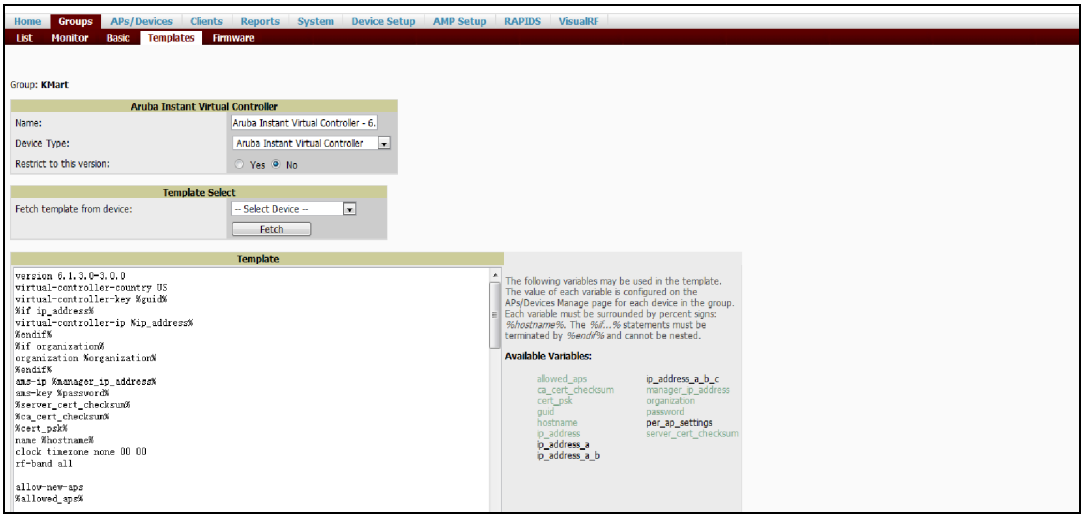
In the AirWave UI, you can select either **Manage Read/Write** or **Monitor-only+Firmware Upgrades** as management modes. When the AirWave Management level is set to **Manage Read/Write**, the WebUI is in read-only mode. When the AirWave Management level is set to **Monitor-only+Firmware Upgrades**, the WebUI changes to the read-write mode.

With the latest version of AirWave, a new option in the AMP is available to put the Instant AP in config-only mode. In this mode, the Instant AP will receive the firmware upgrades and configurations, but will not send any statistics for monitoring. The load is reduced on Instant AP and AirWave and this assists in scaling AirWave effectively.

Template-Based Configuration

AirWave automatically creates a configuration template based on any of the existing Instant APs, and it applies that template across the network as shown in the following figure. It audits every device on an ongoing basis to ensure that configurations never vary from the enterprise policies. It alerts you whenever a violation is detected and automatically repairs the incorrectly configured devices.

Figure 21 *Template-Based Configuration*



Trending Reports

AirWave saves up to 14 months of actionable information, including network performance data and user roaming patterns, so you can analyze how network usage and performance trends have changed

over time. It also provides detailed capacity reports with which you can plan the capacity and appropriate strategies for your organization.

IDS

AirWave provides advanced, rules-based rogue classification. It automatically detects rogue APs irrespective of their location in the network and prevents authorized APs from being detected as rogue APs. It tracks and correlates the IDS events to provide a complete picture of network security.

WIDS Event Reporting to AirWave

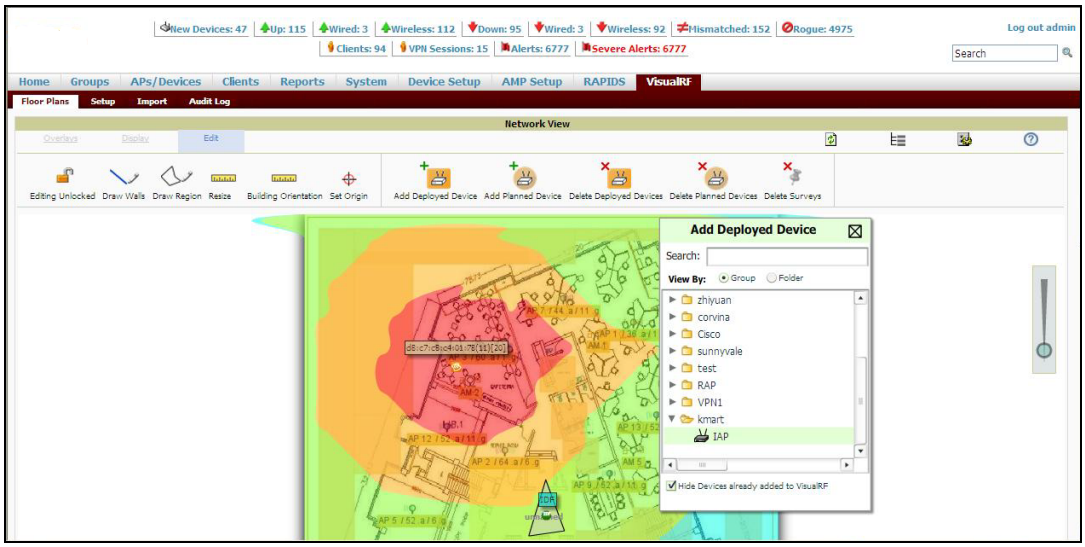
AirWave supports WIDS Event Reporting, which is provided by Instant. This includes WIDS classification integration with the RAPIDS module. RAPIDS is a powerful and easy-to-use tool for automatic detection of unauthorized wireless devices. It supports multiple methods of rogue detection and uses authorized wireless Instant APs to report other devices within range.

The WIDS report cites the number of IDS events for devices that have experienced the most instances in the prior 24 hours and provides links to support additional analysis or configuration in response.

RF Visualization Support for Instant

AirWave supports RF visualization for Instant. The VRF module provides a real-time picture of the actual radio environment of your wireless network and the ability to plan the wireless coverage of new sites. VRF uses sophisticated RF fingerprinting to accurately display coverage patterns and calculate the location of every Instant device in range. VRF provides graphical access to floor plans, client location, and RF visualization for floors, buildings, and campuses that host your network.

Figure 22 *Adding an Instant AP in VRF*



PSK-Based and Certificate-Based Authentication

The PSK-Based and Certificate-Based Authentication are determined by the AMP configuration field.

For a PSK-based authentication, the AMS-IP and PSK must be configured in the Instant AP. The virtual controller attempts to use the login message to initiate a connection.

For a Certificate-based authentication, the AMS-IP and the PSK or just the AMS hostname must be configured in the Instant AP. The Instant APsends a login message to the AMP. The AMP responds with a

randomly generated string. The Instant AP signs the string with its private key and certificate, and sends it back to the AMP. The AMP verifies if the certificate and signature are valid.

A virtual controller is approved based on the status of the Whitelist database:

- When Whitelist is enabled, the AMP verifies if the MAC address and serial number in the login message of the virtual controller and the whitelist database match. If they match, a virtual controller is created and approved. If they do not match, no virtual controller is created.
- When Whitelist is disabled, the virtual controller is created based on the following conditions:
  - Presence of other virtual controller with the same organization string and PSK in the AMP.
  - Approval of atleast one of the virtual controller in the AMP.

Configurable Port for Instant AP and AirWave Management Server Communication

You can now customize the port number of the AMP server through the **server_host:server_port** format, for example, **amp.aruba.com:4343**.

The following example shows how to configure the port number of the AMP server:

```
24:de:c6:cf:63:60 (config) # ams-ip 10.65.182.15:65535
```

Configuring Organization String

The Organization string is a set of colon-separated strings created by the AirWave administrator to accurately represent the deployment of each Instant AP. This string is defined by the installation personnel on the site.

You can use any of the following strings:

- AMP Role—"Org Admin" (initially disabled)
- AMP User—"Org Admin" (assigned to the role "Org Admin")
- Folder—"Org" (under the Top folder in AMP)
- Configuration Group—"Org"

You can also assign additional strings to create a hierarchy of subfolders under the folder named "Org". For example:

- subfolder1 for a folder under the "Org" folder
- subfolder2 for a folder under subfolder1

Shared Key

The Shared Secret key is an optional key used by the administrator to manually authorize the first virtual controller for an organization. Any string is acceptable.

The AirWave administrator can use a shared key to manually authorize the first virtual controller for an organization. Any string is acceptable, but this string must be the same for all devices in your organization.

The AirWave administrator sends the shared secret key, Organization String and the AirWave IP address to the on-site installer setting up the virtual controller and other Instant devices on the network. The AirWave administrator then manually authorizes the virtual controller shared secret key when it appears in the **APs/Devices** > **New list**. After the virtual controller has been validated, other Instant devices using that shared key will automatically be sent to the AirWave server, and appear in the **APs/Devices** > **New list**.

Configuring AirWave Information

The following procedure describes how to configure AirWave information by using the WebUI.

1. Click the AirWave **Set Up Now** link of the main window. The **System** window is displayed with the AirWave parameters on the **Admin** tab.
2. Enter the name of your organization in the **Organization name** text box. The name defined for the organization is displayed under the **Groups** tab in the AirWave UI.
3. Enter the IP address or domain name of the AirWave server in the **AirWave server** text box.
4. Enter the IP address or domain name of a backup AirWave server in the **AirWave backup server** text box. The backup server provides connectivity when the primary server is down. If the Instant AP cannot send data to the primary server, the virtual controller switches to the backup server automatically.
5. Enter the shared key in the **Shared key** text box and reconfirm. This shared key is used for configuring the first Instant AP in the Instant network.
6. Click **OK**.

The following CLI commands configure AirWave information:

```
(Instant AP)(config)# organization <name>
(Instant AP)(config)# ams-ip <IP-address or domain name>
(Instant AP)(config)# ams-backup-ip <IP-address or domain name>
(Instant AP)(config)# ams-key <key>
```

Configuring for AirWave Discovery Through DHCP

AirWave can be discovered through the DHCP server. You can configure this only if AirWave was not configured earlier or if you have deleted the precedent configuration.

On the DHCP server, the format for option 60 is "**ArubaInstantAP**". The two formats for option 43 are "**<organization>,<ams-ip>,<ams-key>**" and "**<organization>,<ams-domain>**" wherein you can configure any domain name.

If you use the **<organization>,<ams-ip>,<ams-key>** format, the PSK-based authentication is used to access the AMP server.

If you use the **<organization>,<ams-domain>** format, the Instant AP resolves the domain name into two IP addresses—AirWave Primary and AirWave Backup.



For option 43, when you choose to enter the domain name, the IP address and key are not available.

Enabling DNS-Based Discovery of the Provisioning AMP Server

Instant APs can now automatically discover the provisioning AMP server if the DHCP option 43 and Activate cannot perform ZTP and transfer the AirWave configuration to the Instant AP.

When a domain option **xxx** is included in the DHCP configuration, the Instant AP will search the DNS server records for **aruba-airwave.xxx**. When there is no domain option, the Instant AP will search only the server records for **aruba-airwave**.



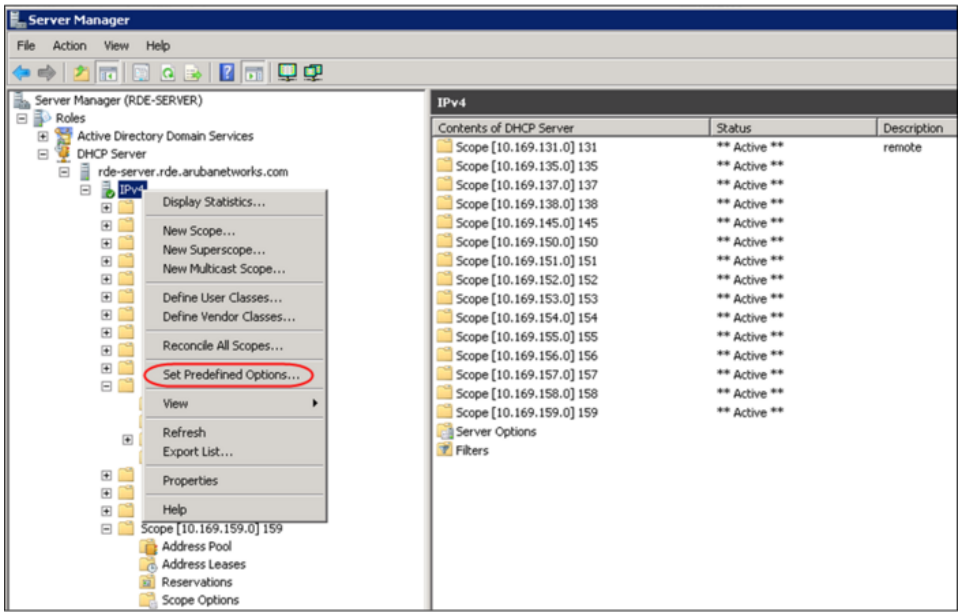
To enable Instant APs to automatically discover the AMP server, create a DNS record for **aruba-airwave.xxx** or **aruba-airwave** in the DNS server. To use this feature on the AirWave side, enable certificate-based login. For information on how to enable certificate-based login, see PSK-Based and Certificate-Based Authentication on page 441.

Standard DHCP Options 60 and 43 on Windows Server 2008

In networks that are not using DHCP options 60 and 43, it is easy to use the standard DHCP options 60 and 43 for an Instant AP or AP. For APs, these options can be used to indicate the master controller or the local controller. For Instant APs, these options can be used to define the AirWave IP, group, password, and domain name.

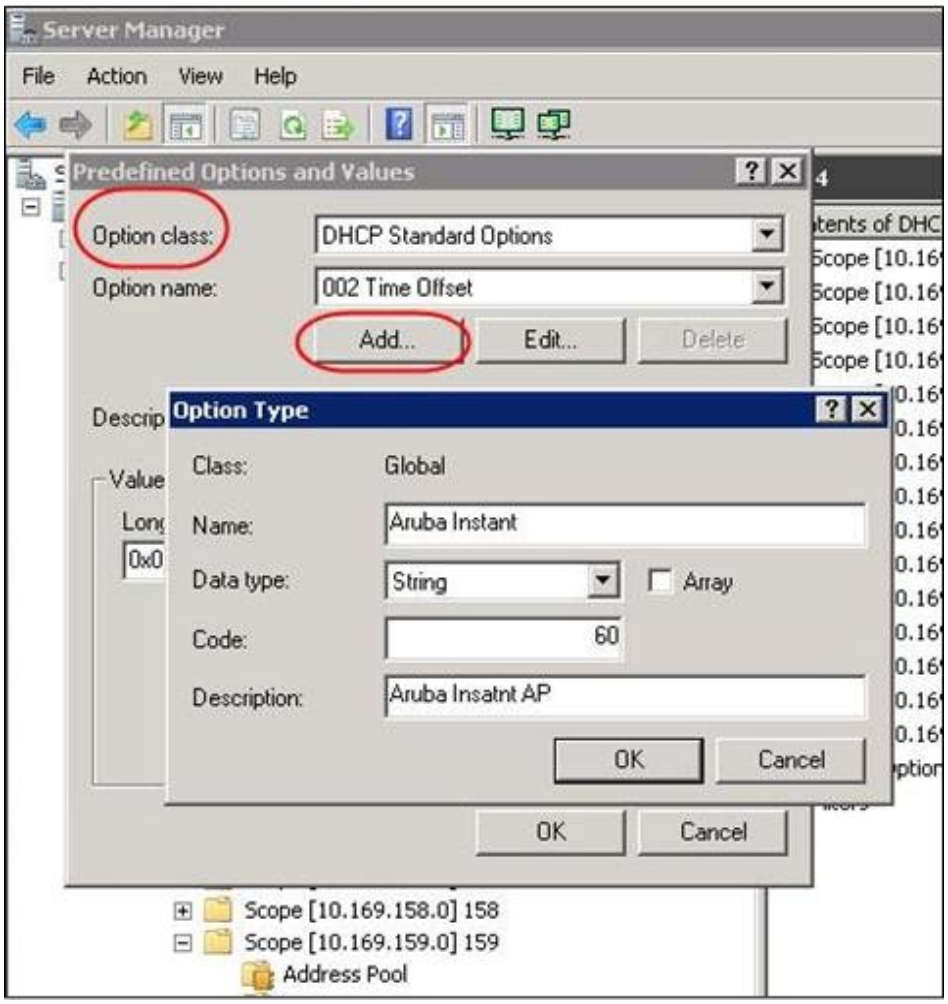
1. From a server running Windows Server 2008, navigate to **Server Manager > Roles > DHCP sever > domain > DHCP Server > IPv4**.
2. Right-click **IPv4** and select **Set Predefined Options.**

Figure 23 *Instant and DHCP options for AirWave: Set Predefined Options*



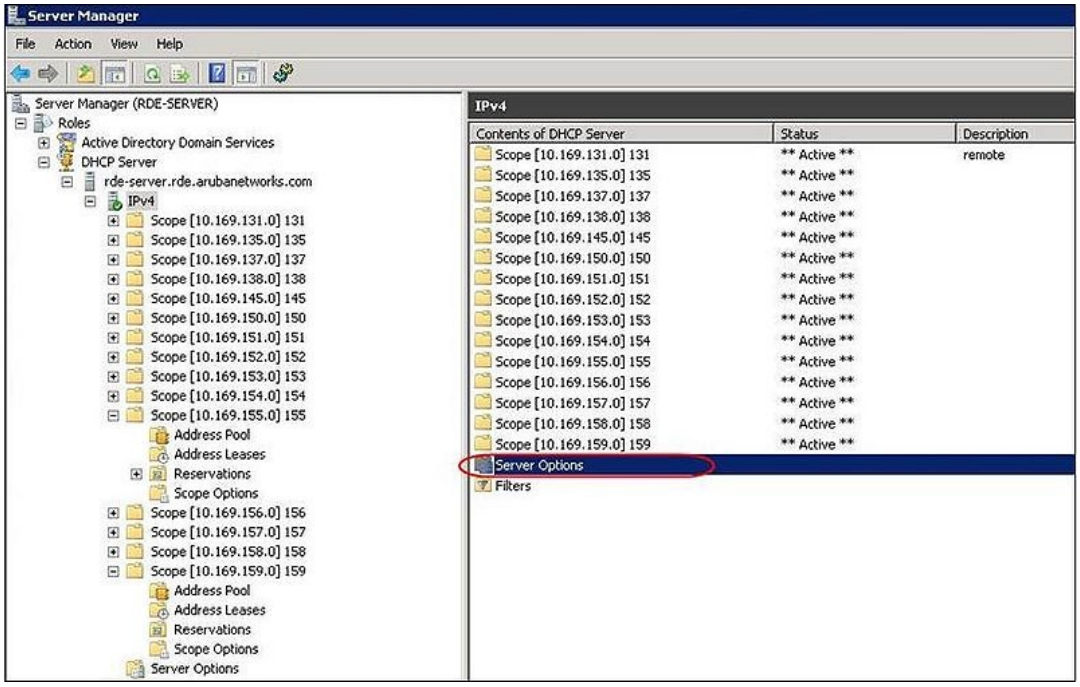
1. Select **DHCP Standard Options** in the **Option class** drop-down list and then click **Add**.
2. Enter the following information:
   - Name—Instant
   - Data Type—String
   - Code—60
   - Description—Instant AP

Figure 24 *Instant and DHCP options for AirWave: Predefined Options and Values*



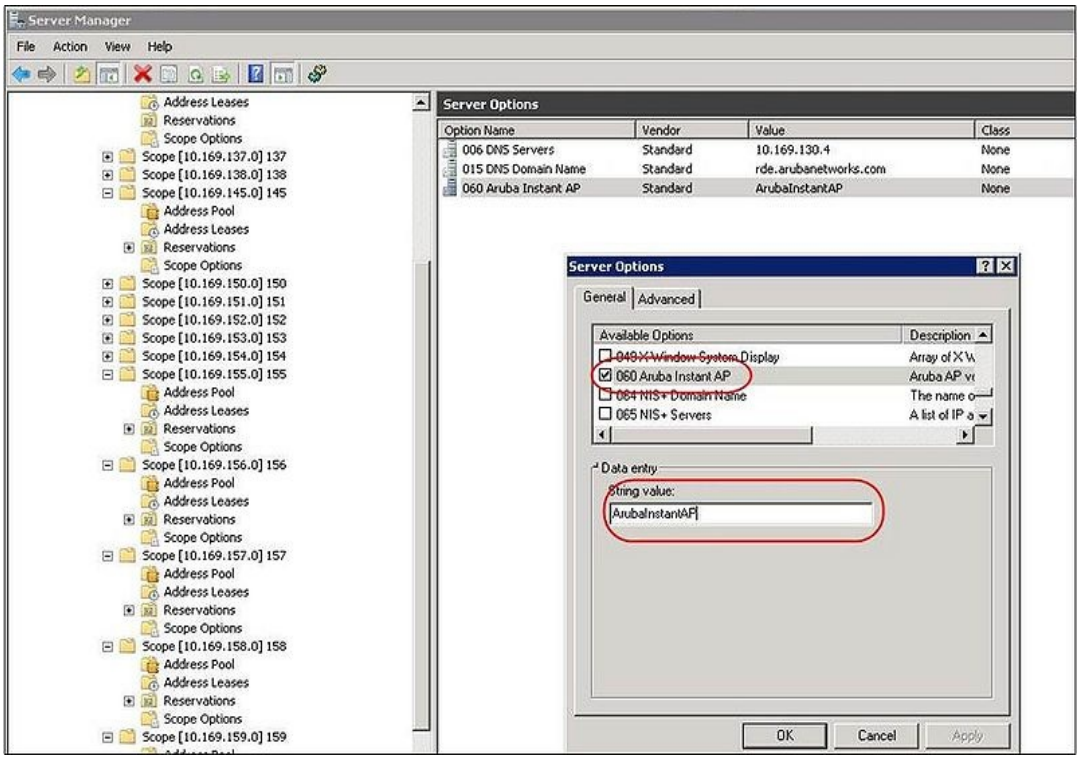
3. Navigate to **Server Manager** and select **Server Options** in the **IPv4** window. This sets the value globally. Use options on a per-scope basis to override the global options.
4. Right-click **Server Options** and select the configuration options.

Figure 25 *Instant and DHCP options for AirWave: Server Options*



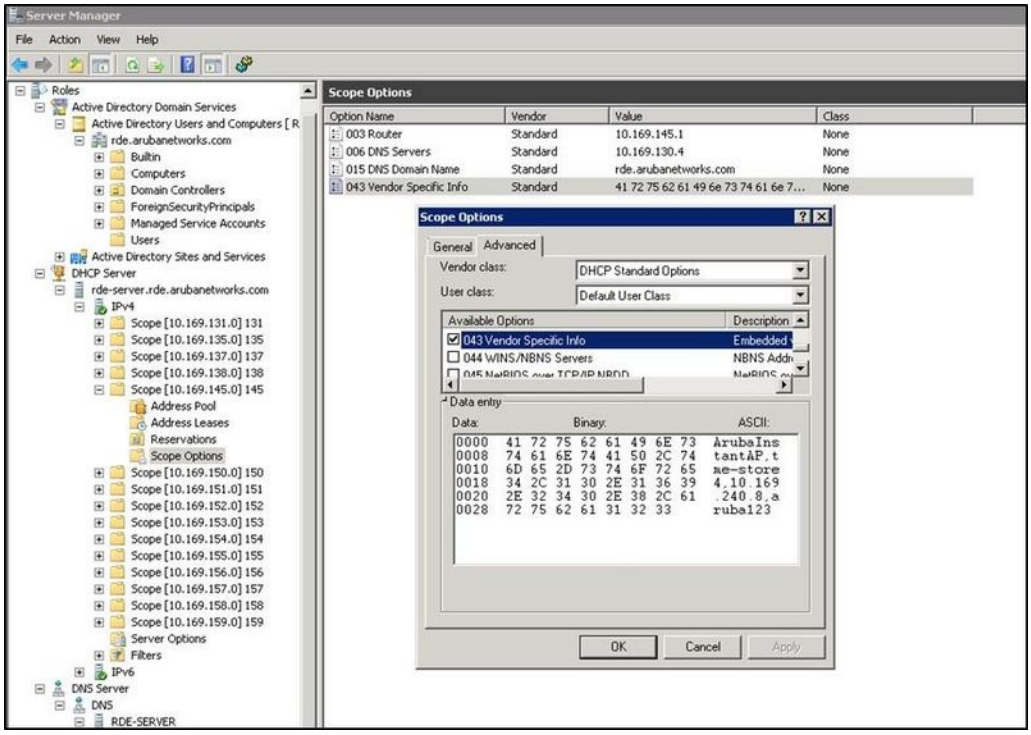
5. Select **060 Aruba Instant AP** in the **Server Options** window and enter **ArubaInstantAP** in the **String value** text box.

Figure 26 *Instant and DHCP options for AirWave—060 Instant AP in Server Options*



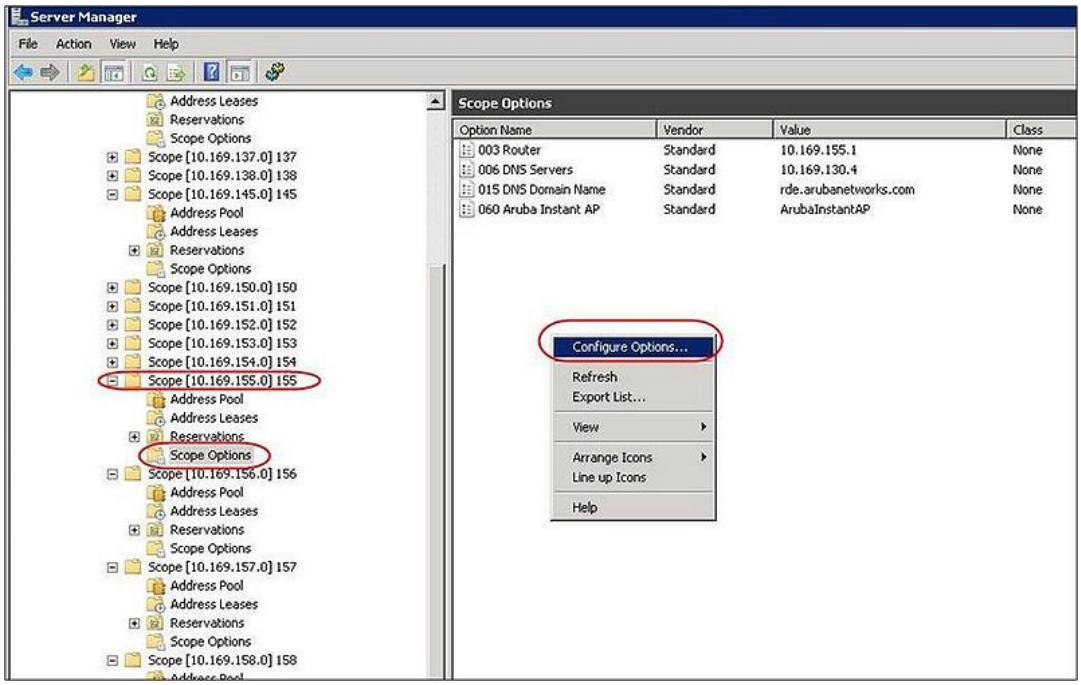
6. Select **043 Vendor Specific Info** and enter a value for either of the following in the ASCII text box:
   - **airwave-orgn, airwave-ip, airwave-key**; for example: Aruba,192.0.2.20, 12344567
   - **airwave-orgn, airwave-domain**; for example: Aruba, aruba.support.com

Figure 27 *Instant and DHCP options for—043 Vendor-Specific Info*



This creates DHCP options 60 and 43 on a global basis. You can do the same on a per-scope basis. The per-scope option overrides the global option.

Figure 28 *Instant and DHCP options for AirWave: Scope Options*



Alternate Method for Defining Vendor-Specific DHCP Options

This section describes how to add vendor-specific DHCP options for Instant APs in a network that already uses DHCP options 60 and 43 for other services. Some networks use DHCP standard options 60 and 43 to provide the DHCP clients information about certain services such as PXE. In such an environment, the standard DHCP options 60 and 43 cannot be used for Instant APs.

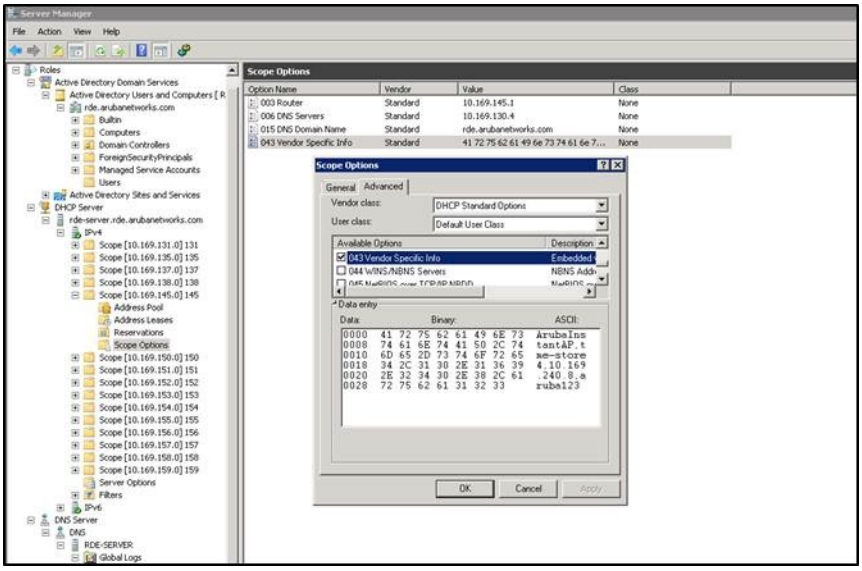
This method describes how to set up a DHCP server to send option 43 with AirWave information to the Instant AP. This section assumes that option 43 is sent per scope, because option 60 is being shared by other devices as well.



The DHCP scope must be specific to Instant, and the PXE devices that use options 60 and 43 must not connect to the subnet defined by this scope. This is because you can specify only one option 43 for a scope, and if other devices that use option 43 connect to this subnet, they are presented with the information specific to the Instant AP.

1. In Windows Server 2008, navigate to **Server Manager > Roles > DHCP Server > Domain DHCP Server > IPv4**.
2. Select a scope [subnet]. Scope [10.169.145.0]145 is selected in the example shown in the figure below.
3. Right-click and select **Advanced,** and then specify the following options:
   - Vendor class—DHCP Standard Options
   - User class—Default User Class
   - Available options—Select 043 Vendor-Specific Info
   - String Value—ArubaInstantAP, tme-store4, 10.169.240.8, Aruba123 (which is the Instant AP description, organization string, AirWave IP address or domain name, PSK, for AirWave)

Figure 29 *Vendor-Specific DHCP options*



Upon completion, the Instant AP shows up as a new device in AirWave, and a new group called **tme-store4** is created. Navigate to **APs/Devices > New > Group** to view this group.

Figure 30 *AirWave—New Group*

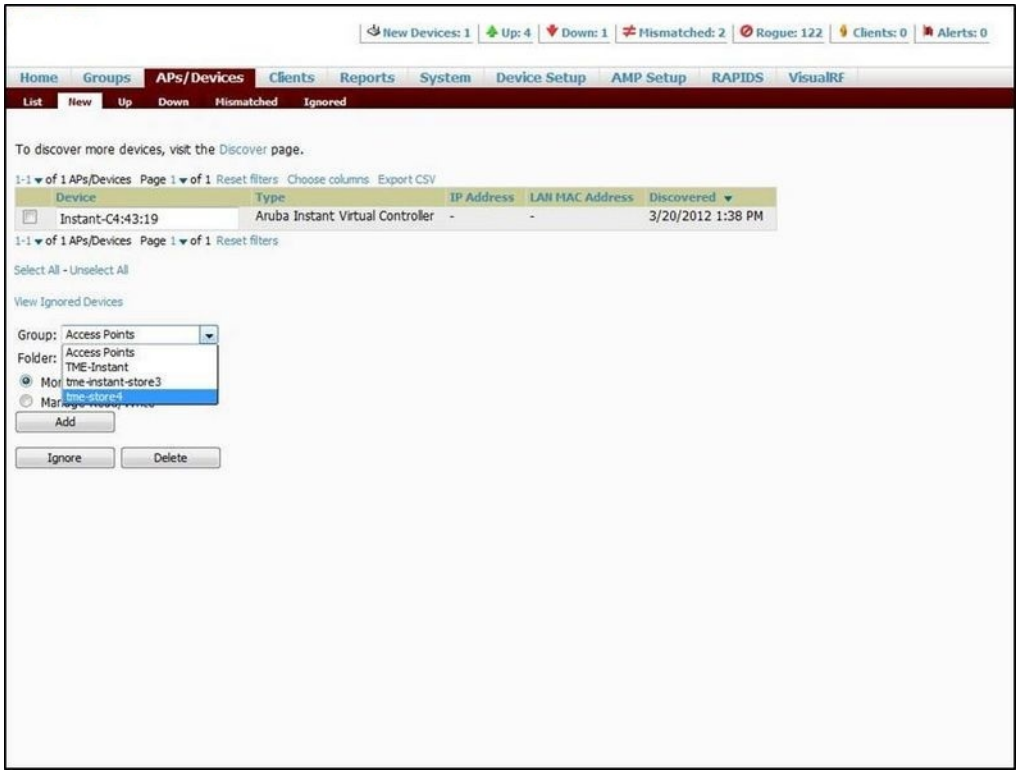
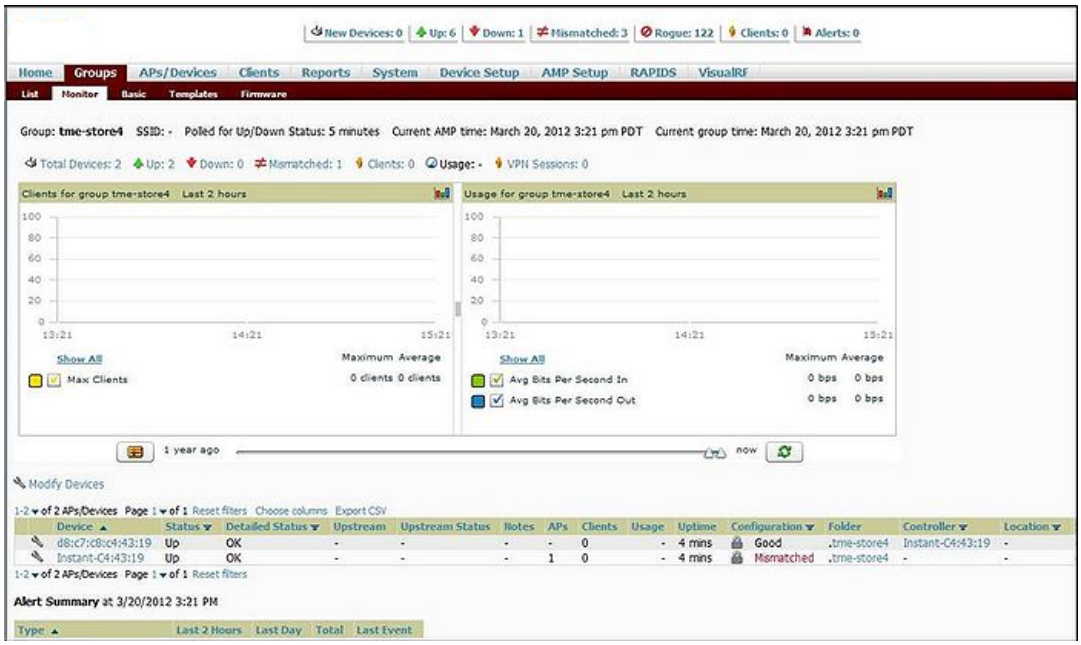


Figure 31 *AirWave—Monitor*



For more information on provisioning, managing, and monitoring the Instant APs from AirWave, refer to the *AirWave Aruba Instant Deployment Guide*.

Managing Instant AP from Aruba Central

Central uses a secure HTTPs connection and provides a strong mutual authentication mechanism using certificates for all communication with Instant APs. These certificates ensure the highest level of protection.

Provisioning an Instant AP using Aruba Central

Accessing Central

After you subscribe and register an Instant AP, log in to the Central dashboard to manage your Instant AP using the following URL: http://www.arubanetworks.com/iap-motd

The Aruba Central WebUI is categorized into the following sections:

1. Monitoring
2. Configuration
3. Reporting
4. Maintenance

These sections are layered under groups. The configuration details of the Instant APs are defined at a group level.

Instant AP Provisioning

Obtaining Cloud Activation Key

The Instant APs obtain the cloud activation key from the Aruba Central Activate server in the following scenarios:

- During reboot, if the Virtual Controller has the Aruba Central URL stored, it will connect directly to Aruba Central using the activation key obtained from the Aruba Central Activate server. If there is no URL stored, the Virtual Controller tries to establish a connection with the Activate server every 5 minutes, until a successful SSL connection is established and the activation key is obtained.
- If the Instant AP Virtual Controller has a Aruba Central URL stored, but fails to establish a connection to Aruba Central in three attempts, the Virtual Controller reconnects to the Activate server to obtain a new activation key.

The cloud activation key obtained from the Activate server is valid for 10 days. To obtain a new activation key, Instant APs reconnect to the Activate server after the initially assigned key expires.

Managing Subscriptions

Central maintains a subscription list for the Instant APs. If an Instant AP is not included in this list, Central identifies it as an unauthorized Instant AP and prevents it from joining the network. The service providers use Central to track the subscription of each Instant AP based on its serial number and MAC address.

The following types of subscription status are listed for the Instant APs:

- Active—Central allows the Instant AP to join the network.
- Expired—Central denies the Instant AP from joining the network.



If the status of a master Instant AP changes from active to expired, it retains its configuration and the local WebUI comes up. The master Instant AP does not reload upon Central subscription expiry.

If the status of a slave Instant AP changes from active to expired, the Virtual Controller sets the slave Instant AP to factory defaults and reboots the Instant AP.

Slave Instant APs can connect to Central through WebSocket.

- Unknown—Central does not allow the Instant AP to join the network. However, it gives an option to retry the connection.

The list maintained by Central is different from the list maintained by the end users. Therefore, Central can prevent an Instant AP from joining the network when the subscription expires, even if the Instant AP is present in the subscription list maintained by the end user.



The subscription list is dynamic and gets updated each time an Instant AP is included in Central.

Firmware Management

For a multiclass Instant AP network, ensure that the Instant AP can download software images from the Aruba Cloud-Based Image Service. You may also need to configure HTTP proxy settings on the Instant AP if they are required for Internet access in your network. For more information about image upgrade and HTTP proxy configuration, refer to the *Aruba Instant Release Notes*.

Instant AP Configuration

Any Instant AP joining a group inherits the configuration defined for the group. After you create a group, navigate to the Wireless Configuration section and create a new SSID. Aruba Central supports ZTP, which allows the network administrators to configure the Instant APs even before the hardware arrives.

After you turn on the Instant AP and connect to the uplink port, the Instant AP is displayed under the default group in the Central UI. You can choose to move the Instant AP to a different group that you created. The configuration defined in this group is automatically applied to the Instant AP.



Starting from ArubaInstant 8.3.0.0, Instant AP allows ArubaCentral to override the routing settings on Instant AP and have some control over the way Central-related traffic is routed.

Recovery Mechanism in the Event of Central Connection Failure

Instant APs managed by Aruba Central require a connection with the Central server for network operations. In the event of a connection loss with Central, the AP tries to reach Central server using the IP address stored in its flash or by retrieving the Central server IP address from the Activate server. When Instant APs configured with a static IP address fail to reach Central, the AP initiates a self recovery mechanism and switches to local DHCP management in an attempt to connect to Central.

The switch from static IP to local DHCP will only be triggered if all of the following conditions are met:

- The AP loses connectivity with Central for more than 10 minutes.
- The AP is unable to reach the default gateway using ARP ping.
- The AP encounters TCP, SSL, or DNS error with both Activate and Central connections.
- A DHCP server responds to DHCP probe requests sent by the AP.

Once the AP establishes connection with Central, it will receive configurations from Central and reboot with the original static IP configuration.

To view the status of recovery mechanism, use the **show recover status** command. It displays the status of the recovery mechanism and cause for recovery trigger.

```
(Instant AP)(config)# show recover status
```

To view static IP address stored in the AP, use the **show ap-env** command.

```
(Instant AP)(config)# show ap-env
```

For more information on these commands, refer to the *Aruba Instant 8.x CLI Reference Guide*.

Changes to the Subscription Model

Starting from Aruba Instant 8.4.0.0, a new subscription model is introduced as a basic interface between Instant AP and Central. The subscription model uses a programmable telemetry interface to subscribe or unsubscribe Instant APs from Central.

Following are some of the key features of the new subscription model:

- Instant APs no longer require a firmware upgrade when
  - Central adds or removes subscribed data
  - A new client requests data
  - Central dynamically manages data feed operations such as start, pause, resume, or unsubscribe.
- The subscribed data is published periodically during an assigned interval.
- Any changes made to the subscribed data is immediately published to the Instant AP.
- The new subscription model follows the distributed module, where Central communicates with each device to gather reports on device monitoring, configuration, and upgrade status specific to the device.

Subscription for Periodic Updates

The telemetry interface in the new subscription model can be programmed to send periodic updates using the Instant CLI. The following CLI command initiates the subscription for periodic updates from Central:

```
(Instant AP)(config)# stats-update-interval
```

WebSocket Connection

WebSocket is a protocol based on which the virtual controllers and the slave Instant APs can establish and maintain a connection with the AirWave and Central servers. A WebSocket support is more efficient because the server does not depend on a client request to respond to an Instant AP. When a WebSocket connection is established, all the access points including virtual controllers and slaves can communicate with the server at any time. Virtual controllers can communicate with the AirWave or Central management server. Slave Instant APs can communicate with application level components.

A new WebSocket capable Instant AP connects to a server through the HTTPS post. If a server supports WebSocket, it will send an HTTP redirect message to the Instant AP. The Instant AP closes the existing HTTPS connection and connects to the server through WebSocket. If the server does not support WebSocket, it will ignore the header and Instant APs will continue using HTTPS and XML to communicate with the server.

The following CLI command shows the websocket status between Instant APs and AirWave:

```
(Instant AP)# show ap debug airwave
```

Support for REST API

Starting from Aruba Instant 8.5.0.0, you can configure and monitor Instant APs using REST APIs. This feature is supported by Instant on both cluster and standalone modes. For more information, see *Aruba Instant8.5.0.x REST API Guide*.

This chapter provides the following information:

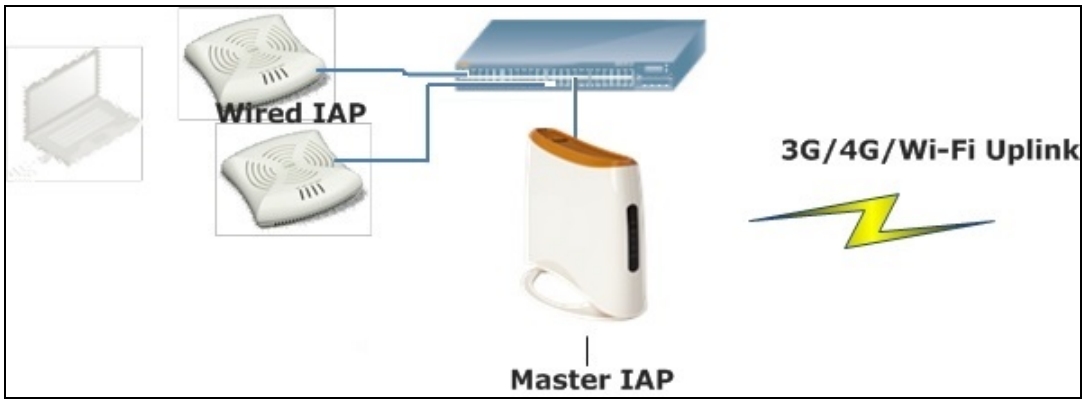
- Uplink Interfaces on page 454
- Uplink Preferences and Switching on page 462

Uplink Interfaces

Instant network supports Ethernet, 3G and 4G USB modems, and the Wi-Fi uplink to provide access to the corporate Instant network. The 3G/4G USB modems and the Wi-Fi uplink can be used to extend the connectivity to places where an Ethernet uplink cannot be configured. It also provides a reliable backup link for the Ethernet-based Instant network.

The following figure illustrates a scenario in which the Instant APs join the virtual controller as slave Instant APs through a wired or mesh Wi-Fi uplink:

Figure 32 *Uplink Types*



The following types of uplinks are supported on Instant:

- Ethernet Uplink
- Cellular Uplink
- Wi-Fi Uplink

Ethernet Uplink

The Eth0 port on an Instant AP is enabled as an uplink port by default. You can view the type of uplink and the status of uplink of an Instant APin the **Info** tab on selecting a client.

Ethernet uplink supports the following types of configuration:

- PPPoE
- DHCP
- Static IP

You can use PPPoE for your uplink connectivity in both Instant AP and IAP-VPN deployments. PPPoE is supported only in a single Instant AP deployment.



Uplink redundancy with the PPPoE link is not supported.

When the Ethernet link is up, it is used as a PPPoE or DHCP uplink. After the PPPoE settings are configured, PPPoE has the highest priority for the uplink connections. The Instant AP can establish a PPPoE session with a PPPoE server at the ISP and get authenticated using PAP or CHAP. Depending upon the request from the PPPoE server, either the PAP or the CHAP credentials are used for authentication. After configuring PPPoE, reboot the Instant AP for the configuration to take effect. The PPPoE connection is dialed after the Instant AP comes up. The PPPoE configuration is checked during Instant AP boot and if the configuration is correct, Ethernet is used for the uplink connection.



When PPPoE is used, do not configure Dynamic RADIUS Proxy and IP address of the virtual controller. An SSID created with default VLAN is not supported with PPPoE uplink.

You can also configure an alternate Ethernet uplink to enable uplink failover when an Ethernet port fails.

Configuring PPPoE Uplink Profile

The following procedure describes how to configure PPPoE settings from the WebUI.

Table 184: *Configuring PPPoE Uplink Profile*

New WebUI	Old WebUI
1. Go to **Configuration** > **System** > **Show advanced options**. 2. Expand **Uplink**. 3. Under **PPPoE** perform the following steps: a. Enter the PPPoE service name provided by your service provider in the **Service name** text box. b. Enter the username for the PPPoE connection in the **User** text box. c. Enter the secret key used for CHAP authentication in the **CHAP secret** and **Retype** text boxes. You can use a maximum of 34 characters for the CHAP secret key. d. Enter a password for the PPPoE connection and confirm the password in the **Password** and **Retype** text boxes. 4. Select a value from the **Local interface** drop-down list to set a local interface for the PPPoE uplink connections. The selected DHCP scope will be used as a local interface on the PPPoE interface and the Local L3 DHCP gateway IP address as its local IP address. When configured, the local interface acts as an unnumbered PPPoE interface and allows the entire Local L3 DHCP subnet to be allocated to clients.	1. Click the **System** link on the Instant main window. 2. Click the **Show advanced options** link. 3. Go to the **Uplink** tab. 4. Perform the following steps in the **PPPoE** section: a. Enter the PPPoE service name provided by your service provider in the **Service name** text box. b. Enter the secret key used for CHAP authentication in the **CHAP secret** and **Retype** text boxes. You can use a maximum of 34 characters for the CHAP secret key. c. Enter the username for the PPPoE connection in the **User** text box. d. Enter a password for the PPPoE connection and confirm the password in the **Password** and **Retype** text boxes. 5. Select a value from the **Local interface** drop-down list to set a local interface for the PPPoE uplink connections. The selected DHCP scope will be used as a local interface on the PPPoE interface and the Local L3 DHCP gateway IP address as its local IP address. When configured, the local interface acts as an unnumbered PPPoE interface and allows the entire Local L3 DHCP subnet to be allocated to clients.

New WebUI	Old WebUI
NOTE: The options in the **Local interface** drop-down list are displayed only if a Local L3 DHCP scope is configured on the Instant AP. 5. Click **Save**. 6. Reboot the Instant AP for the configuration to take effect.	**NOTE:** The options in the **Local interface** drop-down list are displayed only if a Local L3 DHCP scope is configured on the Instant AP. 6. Click **OK**. 7. Reboot the Instant AP for the configuration to take effect.

The following CLI commands configure a PPPoE uplink connection:

```
(Instant AP)(config) # pppoe-uplink-profile
(Instant AP)(pppoe-uplink-profile)# pppoe-svcname <service-name>
(Instant AP)(pppoe-uplink-profile)# pppoe-username <username>
(Instant AP)(pppoe-uplink-profile)# pppoe-passwd <password>
(Instant AP)(pppoe-uplink-profile)# pppoe-chapsecret <password>
(Instant AP)(pppoe-uplink-profile)# pppoe-unnumbered-local-l3-dhcp-profile <dhcp-
profile>
```

The following CLI command shows the PPPoE configuration:

```
(Instant AP)# show pppoe config

PPPoE Configuration
-------------------
Type                    Value
----                    -----
User                    testUser
Password                3c28ec1b82d3eef0e65371da2f39c4d49803e5b2bc88be0c
Service name            internet03
CHAP secret             8e87644deda9364100719e017f88ebce
Unnumbered dhcp profile  dhcpProfile1
```

The following CLI command shows the PPPoE status:

```
(Instant AP)# show pppoe status
pppoe uplink state:Suppressed.
```

Configuring Preferred Uplink for AP-318 and 370 Series Access Points

Starting from Instant 8.5.0.3, AP-318 and 370 Series access points will have both eth1 and eth0 ports as default uplink ports. The eth1 port as the primary Ethernet uplink and eth0 as the backup Ethernet uplink by default. The primary Ethernet uplink can be configured using the **preferred-uplink** command. When eth0 port is configured as the primary Ethernet uplink, the eth1 port assumes the role of backup Ethernet uplink and vice versa.

The eth1 port cannot be configured as a downlink port whereas, if required, the eth0 port can be configured as a downlink port by enabling **enet0-bridging**. When enet0-bridging is enabled on the AP, the eth0 port assumes the downlink role irrespective of the preferred uplink configuration.

The following conditions apply to AP-318 and 370 Series access points:

- The downlink parameters configured in the wired port profile will not take effect.
- If LACP is configured, enet0-bridging cannot be enforced.
- In Mesh scenarios, the mesh point change will only occur if uplink is down for both eth0 and eth1 ports.

Configuring Primary Ethernet Uplink Port

The primary Ethernet uplink for , AP-318 and 370 Series access points can be configured using the **preferred-uplink** command. When configured, the primary Ethernet uplink port will be used for uplink and the backup Ethernet uplink will only be used if the primary Ethernet uplink is down. The uplink for these AP platforms will fall back to a different uplink, defined in the uplink priority list, only if both the primary and backup Ethernet link is down.

The preferred uplink command is a per-AP setting. The following CLI command configures the preferred uplink:

```
(Instant AP)# preferred-uplink <0,1>
```

Configuring Downlink Port

The eth0 port of AP-318 and 370 Series access points can be configured as a downlink port by enabling **enet0-bridging**. Only the eth0 port of these access points can be configured as a downlink port. If eth0 is configured as the primary Ethernet uplink and enet0 bridging is enabled, the eth0 port will become a downlink port and eth1 will become the primary uplink port.

The enet0-bridging is a per-AP setting, The following CLI command configures enet0-bridging:

```
(Instant AP)# enet0-bridging
```

Viewing Ethernet Uplink Status

The **show ap-env** command displays the status of preferred uplink configuration:

```
(Instant AP)# show ap-env
Antenna Type: Internal
Need usb field:No
uap_controller_less:1
preferred_uplink:eth1
```

Cellular Uplink

Instant supports the use of 3G and 4G USB modems to provide the Internet backhaul to an Instant network. The 3G or 4G USB modems can be used to extend client connectivity to places where an Ethernet uplink cannot be configured. This enables the Instant APs to automatically choose the available network in a specific region.



When UML290 runs in auto-detect mode, the modem can switch from 4G network to 3G network or vice-versa based on the signal strength. To configure the UML290 for the 3G network only, manually set the USB type to **pantech-3g**. To configure the UML290 for the 4G network only, manually set the 4G USB type to **pantech-lte**.

Configuring Cellular Uplink Profiles

The following procedure describes how to configure 3G or 4G uplinks by using the WebUI.

Table 185: *Configuring Cellular Uplink Profiles*

New WebUI	Old WebUI
1. Go to **Configuration** > **System** > **show advanced settings**. 2. Expand **Uplink**. 3. In the **3G/4G** section, select the options from the **Country** and **ISP** drop-down lists, as required.	1. Click the **System** link on the Instant main window. 2. Click the **show advanced settings** link. 3. Click the **Uplink** tab. 4. In the **3G/4G** section, select the options from the

New WebUI	Old WebUI
4. Click **Save**. 5. Reboot the Instant AP for changes to take effect.	**Country** and **ISP** drop-down lists, as required. 5. Click **OK**. 6. Reboot the Instant AP for changes to take effect.

The following CLI commands configure 3G/4G uplink manually:

```
(Instant AP)(config) # cellular-uplink-profile
(Instant AP)(cellular-uplink-profile)# usb-type <3G-usb-type>
(Instant AP)(cellular-uplink-profile)# 4g-usb-type <4g-usb>
(Instant AP)(cellular-uplink-profile)# modem-country <country>
(Instant AP)(cellular-uplink-profile)# modem-isp <service-provider-name>
(Instant AP)(cellular-uplink-profile)# usb-auth-type <usb-authentication_type>
(Instant AP)(cellular-uplink-profile)# usb-user <username>
(Instant AP)(cellular-uplink-profile)# usb-passwd <password>
(Instant AP)(cellular-uplink-profile)# usb-dev <device-ID>
(Instant AP)(cellular-uplink-profile)# usb-tty <tty-port>
(Instant AP)(cellular-uplink-profile)# usb-init <Initialization-parameter>
(Instant AP)(cellular-uplink-profile)# usb-dial <dial-parameter>
(Instant AP)(cellular-uplink-profile)# usb-modeswitch <usb-modem>
```

The following CLI command switches a modem from the storage mode to modem mode:

```
(Instant AP)(cellular-uplink-profile)# usb-modeswitch <usb-modem>
```

The following CLI command shows the cellular configuration:

```
(Instant AP)# show cellular config
```

Managing Cellular SIM PIN

Instant APs now support the SIM PIN management functions such as locking, unlocking, and renewing the SIM PIN of the 3G/4G modems. In the current release, these functions can be configured only through the Instant AP CLI.

To prevent any fradulent use of 3G/4G modems connected to an Instant AP, you can enable locking of the SIM PIN of the modems. When enabled, if an incorrect PIN code is provided in the three consecutive attempts, the SIM PIN is locked. To unlock the PIN, the users must use the Personal Unblocking Code code provided by your ISP.



After enabling SIM PIN lock, reboot the Instant AP to apply the SIM PIN lock configuration changes.

The following CLI command enables SIM PIN lock:

```
(Instant AP)# pin-enable <pin_current_used>
```

The following CLI command disables SIM PIN locking:

```
(Instant AP)# no pin-enable <pin_current_used>
```

The following CLI command unlocks a PIN with the PUK code provided by the operator:

```
(Instant AP)# pin-puk <pin_puk> <pin_new>
```

The following CLI command renews the PIN:

```
(Instant AP)# pin-renew <pin_current> <pin_new>
```

Cellular Uplink Preemption

Instant 8.4.0.0 introduces a preemption enhancement method for IAP-VPN wherein Instant APs can detect the reachability of a primary VPN over the Ethernet uplink by simultaneously keeping the secondary 3G/4G uplink stable.

Users can set two Internet failover IP addresses; one for Ethernet uplink and another for cellular 3G/4G uplink. When the cellular uplink IP address is not set, it takes the IP address of the Ethernet uplink.

When the current uplink is Ethernet, the Internet failover IP address is used to detect Internet reachability of Ethernet. When the current uplink is cellular, the cellular Internet failover IP address is used to detect Internet reachability of cellular 3G/4G. In the background, the Internet failover IP address detects Internet reachability of Ethernet and determines whether or not a preemption must take place.

The following CLI commands configure the Internet failover IP address for a cellular 3G/4G uplink:

```
(Instant AP)(config)# uplink
(Instant AP)(uplink)# failover-internet-ip-for-cellular-uplink
```

Wi-Fi Uplink

Instant supports the use of Wi-Fi as uplink to provide internet backhaul for the Instant network. Wi-Fi uplink allows you to connect to SSIDs with open, CCMP, TKIP, PSK-CCMP, and PSK-TKIP encryption. When Wi-Fi uplink is used, the Instant AP uses MAC Address Translation (MAT) to bridge traffic between wireless and wired users of the AP and the uplink network. To enable or disable Wi-Fi uplink on the AP, the AP must be rebooted.



Wi-Fi Uplink is not supported on 340 Series access points.

Wi-Fi Uplink is not supported on AP-555 access points when split 5 GHz mode is enabled.

Configuration Guidelines

- For single-radio Instant APs, the radio serves wireless clients and the Wi-Fi uplink and for dual-radio Instant APs, both radios can be used to serve clients but only one of them can be used for the Wi-Fi uplink.
- The Wi-Fi uplink configuration only takes effect on the Master Instant AP in cluster configurations.
- To bridge traffic for Wi-Fi uplink, the access port VLAN must be the same as Wi-Fi uplink's native VLAN and Client IP assignment should be Network Assigned. To configure the uplink VLAN of the Instant AP, see Configuring Uplink VLAN for an Instant AP.
- 802.1X Authentication is not supported in 802.11n AP platforms.
- Mesh configuration is not supported when Wi-Fi uplink is configured on the 5 GHz band. If Wi-Fi Uplink is enabled on the 5 GHz band, Mesh is disabled.
- Mesh configuration is supported when Wi-Fi uplink is configured on the 2.4 GHz band. When Wi-Fi uplink is configured on the 2.4 GHz radio of an Instant AP in a mesh, that AP automatically assumes the role of mesh portal.
- To connect an Instant AP using Wi-Fi uplink to an Instant-based WLAN, the host controller must run Instant 6.2.1.0 or later for 802.11n AP platforms and Instant 8.5.0.0 or later for 802.11ac AP platforms.
- When Wi-Fi uplink is enabled, IP assignment for clients can either be Virtual Controller managed or Network assigned. To configure client IP assignment, see Configuring VLAN Settings for a WLAN SSID Profile.

NOTE

In Mesh deployments, the configurations made on the Master AP/ Mesh portal is synced across all devices in the mesh cluster. In order to enable Wi-Fi uplink only on the Master AP/ Mesh Portal use the **disable-on-mesh-point** command to disable uplink on mesh points.

Configuring Wi-Fi Uplink

The following procedure describes how to provision an Instant AP with the Wi-Fi uplink using the WebUI.

Table 186: *Configuring Wi-Fi Uplink*

New WebUI	Old WebUI
1. If you are configuring a Wi-Fi uplink after restoring factory settings on anInstant AP, connect the Instant AP to an Ethernet cable to allow the Instant AP to get the IP address. Otherwise, go to step 2. 2. Go to **Configuration** > **System** > **Show advanced options**. 3. Expand **Uplink**. 4. In the **Wifi** section, enter the name of the wireless network that is used for the Wi-Fi uplink in the **Name (SSID)** text box. 5. Select the type of key for uplink encryption and authentication from the **Key management** drop-down list. If the uplink wireless router uses mixed encryption, WPA2 is recommended for the Wi-Fi uplink. 6. Select the band in which the virtual controller currently operates, from the **Band** drop-down list. The following options are available: ▪ 2.4 GHz (default) ▪ 5 GHz 7. Select a passphrase format from the **Passphrase format** drop-down list. The following options are available: ▪ 8–63 alphanumeric characters ▪ 64 hexadecimal characters 8. Enter a PSK passphrase in the **Passphrase** text box and click **Save**. 9. When **WPA2 Enterprise** or **WPA Enterprise** key management type is selected the 802.1X authentication parameters are available for configuration. In the **AP1X type** drop down list box, specify the 802.1X authentication protocol to be used or choose **None** to disable 802.1X authentication. ▪ If **TLS** authentication type is selected, specify the certificate type to be used in the **Certificate type** drop down list. Select **User** from the drop-down.	1. If you are configuring Wi-Fi uplink after restoring factory settings on anInstant AP, connect the Instant AP to an Ethernet cable to allow the Instant AP to get the IP address. Otherwise, go to step 2. 2. Click the **System** link on the Instant main window. 3. Click the **Show advanced options** link. The advanced options are displayed. 4. Click the **Uplink** tab. 5. Under **Wi-Fi**, enter the name of the wireless network that is used for the Wi-Fi uplink in the **Name (SSID)** text box. 6. Select the type of key for uplink encryption and authentication from the **Key management** drop-down list. If the uplink wireless router uses mixed encryption, WPA2 is recommended for the Wi-Fi uplink. 7. Select the band in which the virtual controller currently operates, from the **Band** drop-down list. The following options are available: ▪ 2.4 GHz (default) ▪ 5 GHz 8. When **WPA Personal**or**WPA2 Personal**key management type is selected, the passphrase options are available for configuration. Select a passphrase format from the **Passphrase format** drop-down list. The following passphrase formats are available: ▪ 8–63 alphanumeric characters ▪ 64 hexadecimal characters 9. Enter a PSK passphrase in the **Passphrase** text box and click **OK**. 10. When **WPA2 Enterprise** or **WPA Enterprise** key management type is selected, the 802.1X authentication parameters are available for configuration. In the **AP1X type** drop down list box, specify the 802.1X authentication protocol to be used or choose **None** to disable 802.1X authentication.

New WebUI	Old WebUI
▪ If **PEAP** authentication type is selected, enter the user credentials in the **Username** and **Password** text box. 10. Toggle the **Validate server** button to enable or disable server certificate verification by the AP. **NOTE:** Ensure that the hexadecimal password string is exactly 64 digits in length. **NOTE:** If User certificate type is selected or Validate Server is enabled, the respective certificates must be uploaded to the Instant AP, See Uploading Certificates. 11. Navigate to **System** > **General** > **Show advanced options** and disable the **Extended SSID** toggle switch. 12. Click **Save**. 13. Reboot the Instant AP to apply the changes. After the Instant AP reboots, the Wi-Fi and mesh links are automatically enabled.	▪ If **TLS** authentication type is selected, specify the certificate type to be used in the **Certificate type** drop down list. Select **User** from the drop-down. ▪ If **PEAP** authentication type is selected, enter the user credentials in the **Username** and **Password** text box. 11. Toggle the **Validate server** button to enable or disable server certificate verification by the AP. 12. Click **OK**. **NOTE:** Ensure that the hexadecimal password string is exactly 64 digits in length. **NOTE:** If User certificate type is selected or Validate Server is enabled, the respective certificates must be uploaded to the Instant AP, See Uploading Certificates. 13. Navigate to **System** > **General** > **Show advanced options** and set the **Extended SSID** parameter to **Disabled**. 14. Click **OK**. 15. Reboot the Instant AP to apply the changes. After the Instant AP reboots, the Wi-Fi and mesh links are automatically enabled.

The following CLI commands configure Wi-Fi uplink with open, WPA personal and WPA2 personal authentication:

```
(Instant AP)(config) # wlan sta-profile
(Instant AP)(sta uplink)# cipher-suite<clear | wpa-tkip-psk | wpa2-ccmp-psk>
(Instant AP)(sta uplink)# essid <essid>
(Instant AP)(sta uplink)# uplink-band <dot11a/dot11g>
(Instant AP)(sta uplink)# wpa-passphrase <key>
```

The following CLI commands configure Wi-Fi uplink with 802.1X authentication:

```
(Instant AP)(config) # wlan sta-profile
(Instant AP)(sta uplink)# cipher-suite <wpa-tkip | wpa2-ccmp>
(Instant AP)(sta uplink)# essid <essid>
(Instant AP)(sta uplink)# uplink-band <dot11a/dot11g>
(Instant AP)(sta uplink)# wifi1x {peap <username> <password> | tls <user>}
(Instant AP)(sta uplink)# wifi1x-eap-server <validate-server>
```

The following CLI commands configure uplink VLAN for Wi-Fi Uplink use the following syntax:

```
(Instant AP)# uplink-vlan <vlan id>
```

Troubleshooting Wi-Fi Uplink

The following CLI command shows the Wi-Fi uplink status:

```
(Instant AP)# show wifi-uplink status
configured     :NO
```

```
The following CLI command shows the configuration of Wi-Fi uplink:
(Instant AP)# show wifi-uplink config

ESSID           :wifi
Cipher Suite    :wpa2-ccmp-psk
Passphrase      :******
Band            :dot11a
```

The following CLI command shows the authentication log for Wi-Fi uplink:

```
(Instant AP)# show wifi-uplink auth
-------------------------------------------------------------------
wifi uplink auth log:
-------------------------------------------------------------------
[1116]2000-01-01 00:00:45.625: Global control interface '/tmp/supp_gbl'
```

The following CLI command shows the 802.1X client cert and server ca cert:

```
(Instant AP)# show ap1xcert
```

The following CLI command shows the MAT table maintained for Wi-Fi uplink:

```
(Instant AP)# show wifi-uplink mat-table
```

Uplink Preferences and Switching

This topic describes the following procedures:

- Enforcing Uplinks on page 462
- Setting an Uplink Priority on page 463
- Enabling Uplink Preemption on page 464
- (Instant AP)(uplink)# preemption on page 464
- Viewing Uplink Status and Configuration on page 467

Enforcing Uplinks

The following configuration conditions apply to the uplink enforcement:

- When an uplink is enforced, the Instant AP uses the specified uplink as the primary uplink regardless of uplink preemption configuration and the current uplink status.
- When an uplink is enforced and multiple Ethernet ports are configured ,and if the uplink is enabled on the wired profiles, the Instant AP tries to find an alternate Ethernet link based on the priority configured.
- When no uplink is enforced and preemption is not enabled, and if the current uplink fails, the Instant AP tries to find an available uplink based on the priority configured. The uplink with the highest priority is used as the primary uplink. For example, if Wi-Fi-sta has the highest priority, it is used as the primary uplink.
- When no uplink is enforced and preemption is enabled, and if the current uplink fails, the Instant AP tries to find an available uplink based on the priority configured. If current uplink is active, the Instant AP periodically tries to use a higher-priority uplink and switches to the higher-priority uplink even if the current uplink is active.

You can enforce a specific uplink on an Instant AP by using the WebUI or the CLI.

In the Old WebUI

To enforce an uplink:

1. Go to **System** > **Show advanced options** > **Uplink**.
2. Under **Management**, select the type of uplink from the **Enforce uplink** drop-down list. If the Ethernet uplink is selected, the **Port** text box is displayed.
3. Specify the Ethernet interface port number.
4. Click **OK**. The selected uplink is enforced on the Instant AP.

In the New WebUI

To enforce an uplink:

1. Go to **Configuration** > **System** > **Show advanced options.**
2. Expand **Uplink**.
3. Under **Management**, select the type of uplink from the **Enforce uplink** drop-down list. If **Ethernet uplink** is selected, the **Port** text box is displayed.
4. Specify the Ethernet interface port number.
5. Click **Save**. The selected uplink is enforced on the Instant AP.

In the CLI

To enforce an uplink:

```
(Instant AP)(config)# uplink
(Instant AP)(uplink)# enforce {cellular|ethernet | wifi | none}
```

Setting an Uplink Priority

You can set an uplink priority by using the WebUI or the CLI.

In the Old WebUI

Setting an uplink priority:

1. Go to **System** > **Show advanced options** > **Uplink**.
2. In the **Uplink Priority List** window, select the uplink, and click the **up** arrow or the **down** arrow icons to increase or decrease the priority. By default, the **Eth0** uplink is set as a high-priority uplink.
3. Click **OK**. The selected uplink is prioritized over other uplinks.

In the New WebUI

Setting an uplink priority:

1. Go to **Configuration** > **System** > **Show advanced options**.
2. Expand **Uplink**.
3. In the **Uplink Priority List** window, select the uplink, and click the **up** arrow or the **down** arrow icons to increase or decrease the priority. By default, the **eth0** uplink is set as a high-priority uplink.
4. Click **Save**. The selected uplink is prioritized over other uplinks.

In the CLI

Setting an uplink priority:

```
(Instant AP)(config)# uplink
```

```
(Instant AP)(uplink)# uplink-priority {cellular <priority> | ethernet <priority> |
[port <Interface-number> <priority>] | wifi <priority>}
```

Setting an Ethernet uplink priority :

```
(Instant AP)(uplink)# uplink-priority ethernet port 0 1
```

Enabling Uplink Preemption

The following configuration conditions apply to uplink preemption:

- Preemption can be enabled only when no uplink is enforced.
- When preemption is disabled and the current uplink goes down, the Instant AP tries to find an available uplink based on the uplink priority configuration.
- When preemption is enabled and if the current uplink is active, the Instant AP periodically tries to use a higher-priority uplink, and switches to a higher-priority uplink even if the current uplink is active.

You can enable uplink preemption by using WebUI or the CLI.

In the Old WebUI

To enable uplink preemption:

1. Go to **System** > **Show advanced options** > **Uplink**.
2. Under **Management**, ensure that **Enforce uplink** is set to **None**.
3. Select **Enabled** from the **Pre-emption** drop-down list.
4. Click **OK**.

In the New WebUI

To enable uplink preemption:

1. Go to **Configuration** > **System** > **Show advanced options**.
2. Expand **Uplink**.
3. Under **Management**, ensure that **Enforce uplink** is set to **None**.
4. Toggle the **Pre-emption** switch to enable.
5. Click **Save**.

In the CLI

To configure uplink preemption:

```
(Instant AP)(config)# uplink
(Instant AP)(uplink)# preemption
```

Configuring Wired Port Profile Settings for Uplink VLAN Port

The uplink port of an Instant AP is configured to allow traffic from all VLANs configured in the network by default. This may lead to flooding of broadcast and multicast data packets of all VLANs at the uplink port. However, the traffic on the uplink port can be controlled by configuring **uplink-enforce-wired-port-vlan-setting** command. Configuring this command will enforce the settings of the wired port profile defined in **enet<X>-port-profile** instead of the default uplink port settings. Thereby allowing you to modify the port mode, native vlan, and allowed vlan settings for the uplink port.

NOTE

The default wired port profile (**wired-SetMeUp**) cannot be used on an uplink port other than the default uplink port. If an Ethernet port other than the default uplink port is used as uplink, you must associate that Ethernet port with a new wired port profile with the desired configurations.

The **uplink-enforce-wired-port-vlan-setting** is only applicable in the following scenarios:

- Standalone Instant AP deployments.
- Mesh deployments with single mesh portal.

Limitation:

The **uplink-enforce-wired-port-vlan-setting** is not supported when:

- enet0-bridging is enabled.
- enet-vlan is configured.

NOTE

Disable the enet-vlan configuration of the access point for this command to take effect. When enabled, the **native-vlan** configuration in the wired port profile will be used for **enet-vlan**.

In the CLI

To configure uplink Uplink Wired Port VLAN setting:

```
(Instant AP)(config)# uplink-enforce-wired-port-vlan-setting
```

NOTE

The AP must be rebooted for the configuration to take effect.

Switching Uplinks Based on VPN and Internet Availability

The default priority for uplink switchover is Ethernet and then 3G/4G. The Instant AP can switch to the lower-priority uplink if the current uplink is down.

Switching Uplinks Based on VPN Status

Instant supports switching uplinks based on the VPN status when deploying multiple uplinks (Ethernet, 3G/4G, and Wi-Fi). When VPN is used with multiple backhaul options, the Instant AP switches to an uplink connection based on the VPN connection status, instead of only using the Ethernet or the physical backhaul link.

The following configuration conditions apply to uplink switching:

- If the current uplink is Ethernet and the VPN connection is down, the Instant AP tries to reconnect to VPN. The retry time depends on the fast failover configuration and the primary or backup VPN tunnel. If this fails, the Instant AP waits for the VPN failover timeout and selects a different uplink such as 3G/4G or Wi-Fi.
- If the current uplink is 3G or Wi-Fi, and Ethernet has a physical link, the Instant AP periodically suspends user traffic to try and connect to the VPN on the Ethernet. If the Instant AP succeeds, the Instant AP switches to Ethernet. If the Instant AP does not succeed, it restores the VPN connection to the current uplink.

Uplink switching based on VPN status is automatically enabled if VPN is configured on the Instant AP. However, you can specify the duration in the **VPN failover timeout** text box of the old WebUI or the new WebUI to wait for an uplink switch. By default, this duration is set to **180** seconds. The Instant AP monitors the VPN status and when the VPN connection is not available for 3 minutes, the uplink

switches to another available connection (if a low-priority uplink is detected and the uplink preference is set to none). When **VPN failover timeout** is set to **0** in the old WebUI or the new WebUI, the uplink does not switch over.

When uplink switching based on the Internet availability is enabled, the uplink switching based on VPN failover is automatically disabled.

Switching Uplinks Based on Internet Availability

You can configure Instant to switch uplinks based on Internet availability.

When the uplink switchover based on Internet availability is enabled, the Instant AP continuously sends Internet Control Management Protocol packets to some well-known Internet servers. If the request is timed out due to a bad uplink connection or uplink interface failure, and the public Internet is not reachable from the current uplink, the Instant AP switches to a different connection.

You can set preferences for uplink switching by using the WebUI and the CLI.

In the Old WebUI

To configure uplink switching:

1. Go to **System** > **Show advanced options** > **Uplink**.
2. Under **Management**, configure the following parameters:
   - **VPN failover timeout**—To configure uplink switching based on VPN status, specify the duration to wait for an uplink switch. The default duration is set to 180 seconds.
   - **Internet failover**—To configure uplink switching based on Internet availability, perform the following steps:
     a. Select **Enabled** from the **Internet failover** drop-down list.
     b. Specify the required values for the following parameters:
        - **Max allowed test packet loss**—The maximum number of ICMP test packets that are allowed to be lost to determine if the Instant AP must switch to a different uplink connection. You can specify a value within the range of 1–1000.
        - **Secs between test packets**—The frequency at which ICMP test packets are sent. You can specify a value within the range of 1–3600 seconds.
        - **Internet check timeout**—Internet check timeout is the duration for the test packet timeout. You can specify a value within the range of 0–3600 seconds and the default value is 10 seconds.
        - **Internet failover IP**—To configure the IP address to which the Instant AP must send Instant AP packets and verify if the Internet is reachable when the uplink is down. By default, the master Instant AP sends the ICMP packets to 8.8.8.8 IP address only if the out-of-service operation based on Internet availability (internet-down state) is configured on the SSID.
3. Click Ok

In the New WebUI

To configure uplink switching:

1. Go to **Configuration** > **System** > **Show advanced options**.
2. Expand **Uplink**.
3. Under **Management**, configure the following parameters:
   - **VPN failover timeout**—To configure uplink switching based on VPN status, specify the duration to wait for an uplink switch. The default duration is set to 180 seconds.

- **Internet failover**—To configure uplink switching based on Internet availability, enable the **Internet failover** toggle switch and perform the following steps:
  a. Specify the required values for the following parameters:
     - **Max allowed test packet loss**—The maximum number of ICMP test packets that are allowed to be lost to determine if the Instant AP must switch to a different uplink connection. You can specify a value within the range of 1–1000.
     - **Secs between test packets**—The frequency at which ICMP test packets are sent. You can specify a value within the range of 1–3600 seconds.
     - **Internet check timeout**—Internet check timeout is the duration for the test packet timeout. You can specify a value within the range of 0–3600 seconds and the default value is 10 seconds.
- **Internet failover IP**—To configure an IP address to which the Instant AP must send Instant AP packets and verify if the Internet is reachable when the uplink is down. By default, the master Instant AP sends the ICMP packets to 8.8.8.8 IP address only if the out-of-service operation based on Internet availability (internet-down state) is configured on the SSID.

4. Click **Save**.



When **Internet failover** is enabled, the Instant AP ignores the VPN status, although uplink switching based on VPN status is enabled.

In the CLI

To enable uplink switching based on VPN status:

```
(Instant AP)(config)# uplink
(Instant AP)(uplink)# failover-vpn-timeout <seconds>
```

To enable uplink switching based on Internet availability:

```
(Instant AP)(config)# uplink
(Instant AP)(uplink)# failover-internet
(Instant AP)(uplink)# failover-internet-ip <ip>
(Instant AP)(uplink)# failover-internet-pkt-lost-cnt <count>
(Instant AP)(uplink)# failover-internet-pkt-send-freq <frequency>
```

Viewing Uplink Status and Configuration

To view the uplink status:

```
(Instant AP)# show uplink status
Uplink preemption              :enable
Uplink preemption interval     :600
Uplink enforce                 :none
Ethernet uplink eth0         :DHCP
Uplink Table
------------
Type       State   Priority   In Use
----       -----   --------   ------
eth0       UP      2          Yes
Wifi-sta   INIT    1          No
3G/4G      INIT    3          No
Internet failover              :enable
Internet failover IP           :192.2.0.1
Max allowed test packet loss   :10
Secs between test packets      :30
VPN failover timeout (secs)    :180
```

```
Internet check timeout (secs) :10
ICMP pkt sent         :1
ICMP pkt lost         :1
Continuous pkt lost   :1
VPN down time         :0
AP1X type:NONE
Certification type:NONE
Validate server:NONE
```

To view the uplink configuration in the CLI:

```
(Instant AP)# show uplink config
Uplink preemption              :enable
Uplink preemption interval     :600
Uplink enforce                 :none
Ethernet uplink eth0         :DHCP
Internet failover              :disable
Max allowed test packet loss   :10
Secs between test packets      :30
VPN failover timeout (secs)    :180
Internet check timeout (secs) :10
Secs between test packets    :30
```

Chapter 29
Intrusion Detection

The IDS is a feature that monitors the network for the presence of unauthorized APs and clients. It also logs information about the unauthorized APs and clients, and generates reports based on the logged information.

The IDS feature in the Instant network enables you to detect rogue APs, interfering APs, and other devices that can potentially disrupt network operations.

This chapter describes the following procedures:

- Detecting and Classifying Rogue APs on page 469
- OS Fingerprinting on page 469
- Configuring WIP and Detection Levels on page 470
- Configuring IDS on page 474

Detecting and Classifying Rogue APs

A rogue AP is an unauthorized device plugged into the wired side of the network.

An interfering AP is a device seen in the RF environment but it is not connected to the wired network. While the interfering AP can potentially cause RF interference, it is not considered a direct security threat, because it is not connected to the wired network. However, an interfering AP may be reclassified as a rogue AP.

To detect the rogue APs, go to **More** > **IDS** in the Old WebUI or go to **Configuration** > **IDS** in the new WebUI. The built-in IDS scans for access points that are not controlled by the virtual controller. These are listed and classified as either Interfering or Rogue, depending on whether they are on a foreign network or your network.

OS Fingerprinting

The OS Fingerprinting feature gathers information about the client that is connected to the Instant network to find the operating system that the client is running on. The following is a list of advantages of this feature:

- Identifying rogue clients—Helps to identify clients that are running on forbidden operating systems.
- Identifying outdated operating systems—Helps to locate outdated and unexpected OS in the company network.
- Locating and patching vulnerable operating systems—Assists in locating and patching specific operating system versions on the network that have known vulnerabilities, thereby securing the company network.

OS Fingerprinting is enabled in the Instant network by default. The following operating systems are identified by Instant:

- Android
- AppleTV

- BlackBerry
- Chrome OS and later versions
- iPod
- Kindle
- Linux
- OS X
- Symbian
- Windows 95 and later versions
- Windows CE and later versions
- Windows
- Windows Mobile
- Windows Phone
- Windows ME and later versions
- Apple
- PlayStation
- Nintendo
- Ascom

Configuring WIP and Detection Levels

WIP offers a wide selection of intrusion detection and protection features to protect the network against wireless threats.

Like most other security-related features of the Instant network, the WIP can be configured on the Instant AP.

You can configure the following options:

- **Infrastructure Detection Policies**—Specifies the policy for detecting wireless attacks on access points.
- **Client Detection Policies**—Specifies the policy for detecting wireless attacks on clients.
- **Infrastructure Protection Policies**—Specifies the policy for protecting access points from wireless attacks.
- **Client Protection Policies**—Specifies the policy for protecting clients from wireless attacks.
- **Containment Methods**—Prevents unauthorized stations from connecting to your Instant network.

Each of these options contains several default levels that enable different sets of policies. An administrator can customize, enable, or disable these options accordingly.

The following procedure describes how to configure the detection levels using the WebUI.

Table 187: *Configuring Detection Levels*

New WebUI	Old WebUI
1. Navigate to the **Configuration** > **IDS** page. 2. Go to **Detection** > **Infrastructure** section, move the slider to a desired level and configure the following levels of detection:	1. Go to **More** > **IDS**. The **Wireless Intrusion Protection (WIP)** window is displayed. 2. In the **Detection** > **Infrastructure** section, move the slider to a desired level and configure the

New WebUI	Old WebUI
▪ High ▪ Medium ▪ Low ▪ Off 3. Under **Custom settings** configure the required policy settings described in the Infrastructure Detection Policies. 4. In the **Clients** section, move the slider to a desired level and configure the following levels of detection for clients: ▪ High ▪ Medium ▪ Low ▪ Off 5. Under **Custom settings** configure the required policy settings described in the Client Detection Policies. 6. Select **Protection**. 7. In the **Protection** > **Infrastructure** section, move the slider to a desired level and configure the following levels of protection for infrastructure: ▪ High ▪ Low ▪ Off 8. Under **Custom settings** configure the required policy settings described in the Infrastructure Protection Policies. 9. In the **Clients** section, move the slider to a desired level and configure the following levels of protection for clients: ▪ High ▪ Medium ▪ Low ▪ Off 10. Under **Custom settings** configure the required policy settings described in the Client Protection Policies. 11. Click **Save**.	following levels of detection for infrastructure: ▪ High ▪ Medium ▪ Low ▪ Off 3. Under **Custom settings** configure the required policy settings described in the Infrastructure Detection Policies. 4. In the **Clients** section, move the slider to a desired level and configure the following levels of detection for clients: ▪ High ▪ Medium ▪ Low ▪ Off 5. Under **Custom settings** configure the required policy settings described in the Client Detection Policies. 6. Click **Next**. 7. In the **Protection** > **Infrastructure** section, move the slider to a desired level and configure the following levels of protection for infrastructure: ▪ High ▪ Low ▪ Off 8. Under **Custom settings** configure the required policy settings described in the Infrastructure Protection Policies. 9. In the **Clients** section, move the slider to a desired level and configure the following levels of protection for clients: ▪ High ▪ Medium ▪ Low ▪ Off 10. Under **Custom settings** configure the required policy settings described in the Client Protection Policies. 11. Click **Finish**.

Table 188: *Infrastructure Detection Policies*

Detection Level	Detection Policy
High	■ Detect AP Impersonation ■ Detect ad hoc Networks ■ Detect Valid SSID Misuse ■ Detect Wireless Bridge ■ Detect 802.11 40 MHz intolerance settings ■ Detect Active 802.11n Greenfield Mode ■ Detect AP Flood Attack ■ Detect Client Flood Attack ■ Detect Bad WEP ■ Detect CTS Rate Anomaly ■ Detect RTS Rate Anomaly ■ Detect Invalid Address Combination ■ Detect Malformed Frame—HT IE ■ Detect Malformed Frame—Association Request ■ Detect Malformed Frame—Auth ■ Detect Overflow IE ■ Detect Overflow EAPOL Key ■ Detect Beacon Wrong Channel ■ Detect devices with invalid MAC OUI
Medium	■ Detect ad hoc networks using VALID SSID—Valid SSID list is autoconfigured based on the AP configuration ■ Detect Malformed Frame—Large Duration
Low	■ Detect AP Spoofing ■ Detect Windows Bridge ■ IDS Signature—Deauthentication Broadcast ■ IDS Signature—Deassociation Broadcast
Off	Rogue Classification

Table 189: *Client Detection Policies*

Detection Level	Detection Policy
High	■ Detect EAP Rate Anomaly ■ Detect Rate Anomaly ■ Detect Chop Chop Attack ■ Detect TKIP Replay Attack ■ IDS Signature—Air Jack

Detection Level	Detection Policy
	■ IDS Signature—ASLEAP
Medium	■ Detect Disconnect Station Attack ■ Detect Omerta Attack ■ Detect FATA-Jack Attack ■ Detect Block ACK DOS ■ Detect Hotspotter Attack ■ Detect unencrypted Valid Client ■ Detect Power Save DOS Attack
Low	■ Detect Valid Client Misassociation
Off	All detection policies are disabled.

Table 190: *Infrastructure Protection Policies*

Protection Level	Protection Policy
High	■ Protect from ad hoc Networks ■ Protect AP Impersonation
Low	■ Protect SSID—Valid SSID list should be auto-derived from Instant configuration ■ Rogue Containment
Off	All protection policies are disabled

Table 191: *Client Protection Policies*

Protection Level	Protection Policy
High	Protect Windows Bridge
Low	Protect Valid Station
Off	All protection policies are disabled

Containment Methods

You can enable wired and wireless containment to prevent unauthorized stations from connecting to your Instant network.

Instant supports the following types of containment mechanisms:

- Wired containment—When enabled, APs generate ARP packets on the wired network to contain wireless attacks.
  - wired-containment-ap-adj-mac—Enables a wired containment to Rogue APs whose wired interface MAC address is offset by one from its BSSID.

- wired-containment-susp-l3-rogue—Enables the users to identify and contain an AP with a preset MAC address that is different from the BSSID of the AP, if the MAC address that the AP provides is offset by one character from its wired MAC address.



Enable the **wired-containment-susp-l3-rogue** parameter only when a specific containment is required, to avoid a false alarm.

- Wireless containment—When enabled, the system attempts to disconnect all clients that are connected or attempting to connect to the identified Access Point.
  - None—Disables all the containment mechanisms.
  - Deauthenticate only—With deauthentication containment, the Access Point or client is contained by disrupting the client association on the wireless interface.
  - Tarpit containment—With Tarpit containment, the Access Point is contained by luring clients that are attempting to associate with it to a tarpit. The tarpit can be on the same channel or a different channel as the Access Point being contained.

Configuring IDS

The IDS policy for Instant APs can be created using the CLI.

The following CLI commands configure IDS:

```
(Instant AP)(config)# ids
(Instant AP)(IDS)# ap-max-unseen-timeout <seconds>
(Instant AP)(IDS)# infrastructure-detection-level <type>
(Instant AP)(IDS)# client-detection-level <type>
(Instant AP)(IDS)# infrastructure-protection-level <type>
(Instant AP)(IDS)# client-protection-level <type>
(Instant AP)(IDS)# wireless-containment <type>
(Instant AP)(IDS)# wired-containment
(Instant AP)(IDS)# wired-containment-ap-adj-mac
(Instant AP)(IDS)# wired-containment-susp-l3-rogue
(Instant AP)(IDS)# detect-ap-spoofing
(Instant AP)(IDS)# detect-windows-bridge
(Instant AP)(IDS)# signature-deauth-broadcast
(Instant AP)(IDS)# signature-deassociation-broadcast
(Instant AP)(IDS)# detect-adhoc-using-valid-ssid
(Instant AP)(IDS)# detect-malformed-large-duration
(Instant AP)(IDS)# detect-ap-impersonation
(Instant AP)(IDS)# detect-adhoc-network
(Instant AP)(IDS)# detect-valid-ssid-misuse
(Instant AP)(IDS)# detect-wireless-bridge
(Instant AP)(IDS)# detect-ht-40mhz-intolerance
(Instant AP)(IDS)# detect-ht-greenfield
(Instant AP)(IDS)# detect-ap-flood
(Instant AP)(IDS)# detect-client-flood
(Instant AP)(IDS)# detect-bad-wep
(Instant AP)(IDS)# detect-cts-rate-anomaly
(Instant AP)(IDS)# detect-rts-rate-anomaly
(Instant AP)(IDS)# detect-invalid-addresscombination
(Instant AP)(IDS)# detect-malformed-htie
(Instant AP)(IDS)# detect-malformed-assoc-req
(Instant AP)(IDS)# detect-malformed-frame-auth
(Instant AP)(IDS)# detect-overflow-ie
(Instant AP)(IDS)# detect-overflow-eapol-key
(Instant AP)(IDS)# detect-beacon-wrong-channel
(Instant AP)(IDS)# detect-invalid-mac-oui
(Instant AP)(IDS)# detect-valid-clientmisassociation
```

```
(Instant AP)(IDS)# detect-disconnect-sta
(Instant AP)(IDS)# detect-omerta-attack
(Instant AP)(IDS)# detect-fatajack
(Instant AP)(IDS)# detect-block-ack-attack
(Instant AP)(IDS)# detect-hotspotter-attack
(Instant AP)(IDS)# detect-unencrypted-valid
(Instant AP)(IDS)# detect-power-save-dos-attack
(Instant AP)(IDS)# detect-eap-rate-anomaly
(Instant AP)(IDS)# detect-rate-anomalies
(Instant AP)(IDS)# detect-chopchop-attack
(Instant AP)(IDS)# detect-tkip-replay-attack
(Instant AP)(IDS)# signature-airjack
(Instant AP)(IDS)# signature-asleap
(Instant AP)(IDS)# protect-ssid
(Instant AP)(IDS)# rogue-containment
(Instant AP)(IDS)# protect-adhoc-network
(Instant AP)(IDS)# protect-ap-impersonation
(Instant AP)(IDS)# protect-valid-sta
(Instant AP)(IDS)# protect-windows-bridge
(Instant AP)(IDS)# valid-ap-max-unseen-timeout <seconds>
```

For more information, refer *Aruba Instant 8.7.0.x Command-Line Interface Reference Guide*.

Configuring Ageout Time for Valid and Interfering APs

Instant APs monitor the RF environment to identify neighboring APs operating in the environment. This information is stored in the network database and referenced for IDS functions. To provide better control over the RF environment, the ageout time for valid and interfering AP entries in the network database can be configured through the CLI. When configured the entry of valid and interfering APs are removed from the network database if they are not seen in the RF environment after the ageout time is elapsed.

These settings are available under the **ids** command. The default ageout time for valid APs is 7200 seconds and interfering APs is 600 seconds.

Following is the command syntax to configure ageout time for valid APs:

```
(Instant AP)(config)# ids
(Instant AP)(IDS)# valid-ap-max-unseen-timeout <seconds>
```

Following is the command syntax to configure ageout time for interfering APs:

```
(Instant AP)(config)# ids
(Instant AP)(IDS)# ap-max-unseen-timeout <seconds>
```

Chapter 30
Mesh Instant AP Configuration

This chapter provides the following information:

- Mesh Network Overview on page 476
- Setting up Instant Mesh Network on page 478
- Configuring Wired Bridging on Ethernet 0 for Mesh Point on page 479
- Mesh Cluster Function on page 479
- Radio Selection for Mesh Links on page 481
- Fast Roaming with Mesh Access Points on page 481

Mesh Network Overview

The Instant secure enterprise mesh solution is an effective way to expand network coverage for outdoor and indoor enterprise environments without any wires. As traffic traverses across mesh Instant APs, the mesh network automatically reconfigures around broken or blocked paths. This self-healing feature provides increased reliability and redundancy and allows the network to continue operation even when an Instant AP stops functioning or if a connection fails.

Mesh Instant APs

Mesh network requires at least one valid uplink (wired or 3G) connection. Any provisioned Instant AP that has a valid uplink (wired or 3G) functions as a mesh portal, and the Instant AP without an Ethernet link functions as a mesh point. The mesh portal can also act as a virtual controller. Mesh portals and mesh points are also known as mesh nodes, a generic term used to describe Instant APs configured for mesh.

If two Instant APs have valid uplink connections, there is redundancy in the mesh network, and most mesh points try to mesh directly with one of the two portals. However, depending on the actual deployment and RF environment, some mesh points may mesh through other intermediate mesh points.

In an Instant mesh network, the maximum hop count is two nodes (point > point > portal) and the maximum number of mesh points per mesh portal is eight.

Mesh Instant APs detect the environment when they boot up, locate and associate with their nearest neighbor, to determine the best path to the mesh portal.

Instant mesh functionality is supported only on dual-radio Instant APs. On dual-radio Instant APs, the 2.4 GHz radio is always used for client traffic, while the 5 GHz radio is always used for both mesh-backhaul and client traffic.

The mesh network must be provisioned for the first time by plugging into the wired network. After that, the mesh service works on Instant APs like it does on any other regulatory domain.

Mesh Portals

A mesh portal is a gateway between the wireless mesh network and the enterprise wired LAN. The mesh roles are automatically assigned based on the Instant AP configuration. A mesh network could have multiple mesh portals to support redundant mesh paths (mesh links between neighboring mesh

points that establish the best path to the mesh portal) from the wireless mesh network to the wired LAN.

The mesh portal broadcasts a mesh services set identifier or mesh cluster name to advertise the mesh network service to other mesh points in that Instant network. This is not configurable and is transparent to the user. The mesh points authenticate to the mesh portal and establish a link that is secured using AES encryption.



The mesh portal reboots after 5 minutes when it loses its uplink connectivity to a wired network.

Mesh Points

The mesh point establishes an all-wireless path to the mesh portal. The mesh point provides traditional WLAN services such as client connectivity, IDS capabilities, user role association, and QoS for LAN-to-mesh communication to clients and performs mesh backhaul or network connectivity.



A mesh point also supports LAN bridging. You can connect any wired device to the downlink port of the mesh point. In the case of single Ethernet port platforms such as AP-505, you can convert the Eth0 uplink port to a downlink port by enabling **Eth0 Bridging**. For additional information, see Configuring Wired Bridging on Ethernet 0 for Mesh Point on page 479.

Automatic Mesh Role Assignment

Previously, when a mesh point discovered that the Ethernet 0 port link was up without Ethernet 0 bridge configured, the mesh point rebooted immediately. Aruba Instant supports enhanced role detection during Instant AP boot up and Instant AP running time.

When a mesh point discovers that the Ethernet 0 port link is up, it sends loop detection packets to check whether the Ethernet 0 link is available. If it is available, the mesh point reboots and becomes a mesh portal. Otherwise, the mesh point does not reboot.

Mesh Role Detection During System Boot Up

If an Instant AP boots up and discovers that the Ethernet link is down, it acts as a mesh point. If the Ethernet link is up, the Instant AP continues to detect if the network is reachable. In a static IP address scenario, the Instant AP pings the gateway. If the ping is successful, the Instant AP acts as a mesh portal. Otherwise, it acts as a mesh point. In case of DHCP, if the Instant AP obtains the IP address successfully, it acts as a mesh portal. Otherwise, it acts as a mesh point. In case of IPv6, Instant APs do not support the static IP address but only support DHCP for detection of network reachability.



If the Instant AP has a 3G/4G USB modem plugged, it always acts as a mesh portal.

If the Instant AP is set to Ethernet 0 bridging, it always acts as a mesh point.

Mesh Role Detection During System Running Time

- **Mesh Point Role Change**: When a mesh point detects whether its Ethernet link is up, it continues to use Loop Protection (based on the Loop Protection for Secure Jack Port feature), to check if the loop has been detected. If the loop is detected, the Instant AP reboots. Otherwise, the Instant AP does not reboot and the mesh role continues to act as a mesh point.

You can enable enhanced mesh role detection by using the CLI:

In the CLI

```
(Instant AP)(config)# enhanced-mesh-role-detect
```

Setting up Instant Mesh Network

Starting from Instant 6.4.0.2-4.1.0.0 release, mesh functionality is disabled by default, because of which over-the-air provisioning of mesh Instant APs is not supported.

To provision Instant APs as mesh Instant APs:

1. Connect the Instant APs to a wired switch.
2. Ensure that the virtual controller key is synchronized and the country code is configured.
3. Ensure that a valid SSID is configured on the Instant AP.



Mesh works best on IAP-315 and IAP-207 access points when an SSID is configured for the 5 GHz radio and selecting the 5 GHz channel using the dynamic channel method.

4. If the Instant AP has a factory default SSID (Instant SSID), delete the SSID.
5. If an ESSID is enabled on the virtual controller, disable it and reboot the Instant AP cluster.
6. Disconnect the Instant APs that you want to deploy as mesh points from the switch, and place the Instant APs at a remote location. The Instant APs come up without any wired uplink connection and function as mesh points. The Instant APs with valid uplink connections function as mesh portals.



Instant does not support the topology in which the Instant APs are connected to the downlink Ethernet port of a mesh point.

Mesh Network with Mixed Indoor and Outdoor APs

Indoor and outdoor APs participating in a mesh must be deployed with RF or regulatory settings, or assigned RF profiles, which allow overlapping channels to operate between the APs in the following scenarios:

- When setting up a mesh network between indoor and outdoor APs.
- When provisioning indoor APs as outdoor APs.
- When using AirMatch or ARM to support dynamic channel selection.

This allows both indoor and outdoor APs to always operate on the same channels. If you do not deploy the indoor and outdoor APs with regulatory settings or assigned RF profiles with overlapping channels, the indoor and outdoor channels for a given regulatory domain may not overlap. When the indoor and outdoor APs share a regulatory profile and are provisioned for the correct network environment, the dedicated indoor or outdoor mesh portals are deployed to support indoor or outdoor mesh points respectively.

The provisioned Indoor or Outdoor role of an AP is defined by the location of its antennas. Hence, when an indoor AP uses antennas installed in an outdoor area, the AP must be provisioned as Outdoor. For example, if the external outdoor antennas of an indoor AP are deployed to support outdoor APs as mesh points, and the indoor mesh portal is running on UNII-1 channel 36, then the outdoor mesh points may not be able to view the mesh portal to associate with. This occurs when the regulatory domain of that country has different allowed channels for indoor and outdoor APs, and the regulatory domain may disallow UNII-1 channels and UNII-3 channels for outdoor and indoor uses respectively. As a result, the mesh points cannot access UNII-1 APs. However, once the indoor AP with outdoor antennas is

provisioned as an outdoor AP, that AP can then run on a UNII-3 channel, allowing the mesh points to access the portal.

Configuring Wired Bridging on Ethernet 0 for Mesh Point

Instant supports wired bridging on the Ethernet 0 port of an Instant AP. If Instant AP is configured to function as a mesh point, you can configure wired bridging.



Enabling wired bridging on this port of anInstant AP makes the port available as a downlink wired bridge and allows client access through the port.

Eth0 bridging cannot be configured if Eth1 is configured as preferred uplink.

When using 3G uplink, the wired port will be used as downlink.

The following procedure describes how to configure support for wired bridging on the Ethernet 0 port of an Instant AP by using the WebUI.

Table 192: *Configuring Wired Bridging on Ethernet0*

New WebUI	Old WebUI
1. Go to **Configuration** > **Access Points** and select the Instant AP to modify and click **Edit**. 2. Expand **Uplink**. 3. Toggle the **Eth0 bridging** switch to enable. 4. Click **Save**. 5. Reboot the Instant AP.	1. On the **Access Points** tab, select the Instant AP to modify. 2. Click the **edit** link. 3. Click the **Uplink** tab. 4. Select **Enable** from the **Eth0 Bridging** drop-down list. 5. Click **OK**. 6. Reboot the Instant AP.

The following CLI command configures Ethernet bridging:

```
(Instant AP)# enet0-bridging
```



Make the necessary changes to the wired-profile when eth0 is used as the downlink port. For more information, see Configuring a Wired Profile on page 161.

Mesh Cluster Function

Instant 8.4.0.0 introduces the mesh cluster function for easy deployments of Instant APs. Users can configure an ID and a password, and can provision Instant APs to a specific mesh cluster.

In a cluster-based scenario, each network can support multiple mesh profiles. There is no limit to the number of profiles that can be configured. Mesh cluster function is a per-AP setting and must be configured by the user. When an Instant AP boots up, it attempts to find a mesh cluster configuration. If the Instant AP already has mesh cluster configured, it uses that configuration. Otherwise, it uses the default mesh configuration.

In the default profile, SSID, password, and cluster name are generated by the virtual controller key. Instant APs that belong to the same mesh network can establish mesh links with each other.

In a standalone scenario, Instant APs can establish a mesh link. However, the network role election does not take place. Users can set the same mesh cluster configuration to establish mesh links with other networks. The Instant AP operates as a mesh portal or a mesh point based on the uplink.



Mesh role detection remains the same for cluster-based and standalone Instant APs.

The following CLI command configures the key in a mesh cluster:

```
(Instant AP)# mesh-cluster-key <key>
```

The following CLI command configures the name in a mesh network:

```
(Instant AP)# mesh-cluster-name <name>
```

The following CLI command disables mesh functionality in a network:

```
(Instant AP)# mesh-disable
```

The following CLI command displays details of the mesh cluster:

```
(Instant AP)# show ap mesh cluster {active | configuration | stats <IP address> |
status | topology}
```

Configuring Multiple Mesh Clusters

Mesh clusters are grouped and defined by a mesh cluster profile, which provides the framework of the mesh network. The mesh cluster profile contains the MSSID, authentication methods, security credentials, and cluster priority required for mesh points to associate with their neighbors and join the cluster. Associated mesh points store this information in flash memory. Although most mesh deployments require only a single mesh cluster profile, you can configure and apply multiple mesh cluster profiles to an individual AP. If you have multiple cluster profiles, the mesh portal uses the profile with the highest priority to bring up the mesh network. Mesh points, in contrast, go through the list of mesh cluster profiles in order of priority to decide which profile to use to associate themselves with the network. The mesh cluster priority determines the order by which the mesh cluster profiles are used. This allows you, rather than the link metric algorithm, to explicitly segment the network by defining multiple cluster profiles.

Since the mesh cluster profile provides the framework of the mesh network, you must define and configure the mesh cluster profile before configuring an AP to operate as a mesh point. If you find it necessary to define more than one mesh cluster profile, you must assign priorities to each profile to allow the mesh points to identify the primary and backup mesh cluster profiles.

If the mesh cluster profile is unavailable, the mesh point can revert to the recovery profile to bring-up the mesh network until the cluster profile is available. You can also exclude one or more mesh cluster profiles from an individual access point, this prevents a mesh cluster profile defined at the AP group level from being applied to a specific AP.

Do not delete or modify mesh cluster profiles once you use them to provision mesh points. You can recover the mesh point if the original cluster profile is still available. It is recommended to create a new mesh cluster profile if needed. If you modify any mesh cluster setting, you must reprovision and manually reboot your AP for the changes to take effect.

If you configure multiple cluster profiles with different cluster priorities, you manually override the link metric algorithm because the priority takes precedence over the path cost. In this scenario, the mesh portal uses the profile with the highest priority to bring-up the mesh network. The mesh portal stores and advertises that one profile to neighboring mesh points to build the mesh network. This profile is known as the primary cluster profile. Mesh points, in contrast, go through the list of configured mesh cluster profiles in order of priority to find the profile being advertised by the mesh portal. Once the

primary profile has been identified, the other profiles are considered backup cluster profiles. Use this deployment if you want to enforce a particular mesh topology rather than allowing the link metric algorithm to determine the topology.

The following CLI command configures multiple mesh cluster profiles on an Instant AP:

```
(Instant AP)(config)# mesh-cluster <cluster_name_1> wpa2-psk <cluster_key_1> priority
<number_1>
(Instant AP)(config)# mesh-cluster <cluster_name_2> wpa2-psk <cluster_key_2> priority
<number_2>
(Instant AP)(config)# mesh-cluster <cluster_name_3> wpa2-psk <cluster_key_3> priority
<number_3>
(Instant AP)(config)# end
(Instant AP)# commit-apply
```

The following CLI commands are used to view the mesh cluster configuration on the Instant AP:

```
(Instant AP)# show running-config | include mesh-cluster
(Instant AP)# show running-config no-encrypt | include mesh-cluster
```

The following CLI commands display the mesh cluster with the highest priority:

```
(Instant AP)# show ap mesh cluster status
(Instant AP)# show ap mesh cluster configuration
```

Radio Selection for Mesh Links

The radio used for the mesh link can be configured in dual 5 GHz or split 5 GHz enabled access points. When dual 5 GHz radio or split 5 GHz radio is enabled on the access point, the operations on the 5 GHz band is split and carried out by two separate radios — lower 5 GHz radio and upper 5 GHz radio. The lower 5 GHz radio operates on channels 32 – 64 and the upper 5 GHz radio operates on channels 100-173. Configuring mesh links in different 5 GHz bands will reduce interference from neighboring mesh links and provide better control over the RF environment.



This feature is currently supported only in 340 Series and 550 Series access points.

The radio used for the mesh link is configured using the **mesh-split5g-range-band** command and can be configured only through the CLI. This configuration can only be applied on dual 5 GHz radio or split 5 GHz radio enabled APs. Apply the configuration and reboot the AP for the changes to take effect.

The following CLI command configures the radio for mesh link:

```
mesh-split5g-range-band { full | lower | upper | first }
```

The radio assignment and operating band information is listed in the following table:

Radio Mode	Radio	Operating Band
Dual 5 GHz (340 Series access points)	Radio 0	Lower 5 GHz band
	Radio 1	Upper 5 GHz band
Split 5 GHz (AP-555 access points)	Radio 0	Upper 5 GHz band
	Radio 2	Lower 5 GHz band

Fast Roaming with Mesh Access Points

Instant supports fast roaming for APs deployed in a wireless mesh network. The mesh points for which fast roaming is enabled are called mobility mesh points. Fast roaming on mesh APs is required mainly in fast moving environments such as buses or the subway. To support fast roaming, mobility mesh points perform a scan of other mesh points in the background first and then choose the best neighbor to connect from all the neighbors. The background scan implies when mesh is connected, the mesh point collects information about surrounding channels through background scanning. The mobility mesh point scan time between radio channels is altered to be faster than the mesh point scan in a regular mesh network. This feature is currently supported only on 300 Series, 310 Series, 320 Series, 330 Series, AP-365, and 370 Series access points.

The following CLI command enables fast roaming on a mesh point:

```
(Instant AP)# mesh-mobility [high|low|<number>
```

Chapter 31
Mobility and Client Management

This chapter provides the following information:

- Layer-3 Mobility Overview on page 483
- Configuring Layer-3 Mobility on page 484

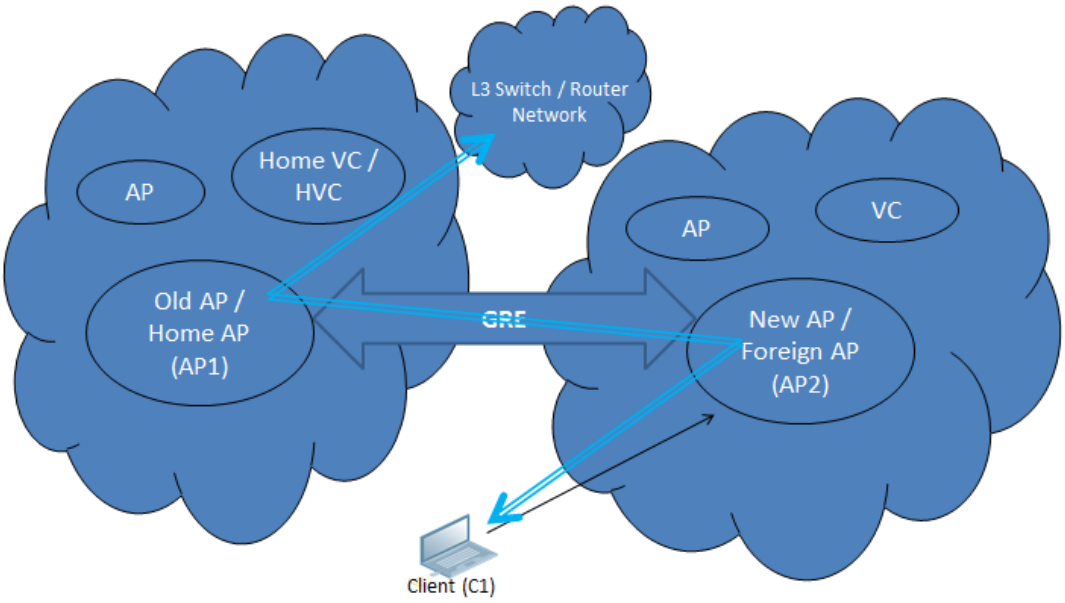
Layer-3 Mobility Overview

Instant APs form a single Instant network when they are in the same Layer-2 domain. As the number of clients increase, multiple subnets are required to avoid broadcast overhead. In such a scenario, a client must be allowed to roam away from the Instant network to which it first connected (home network) to another network supporting the same WLAN access parameters (foreign network) and continue its existing sessions.

Layer-3 mobility allows a client to roam without losing its IP address and sessions. If WLAN access parameters are the same across these networks, clients connected to Instant APs in a given Instant network can roam to Instant APs in a foreign Instant network and continue their existing sessions. Clients roaming across these networks are able to continue using their IP addresses after roaming. You can configure a list of virtual controller IP addresses across which Layer-3 mobility is supported.

The Aruba Instant Layer-3 mobility solution defines a Mobility Domain as a set of Instant networks, with the same WLAN access parameters, across which client roaming is supported. The Instant network to which the client first connects is called its home network. When the client roams to a foreign network, an Instant AP in the home network (home Instant AP) anchors all traffic to or from this client. The Instant AP to which the client is connected in the foreign network (foreign Instant AP) tunnels all client traffic to or from the home Instant AP through a GRE tunnel.

Figure 33 *Routing of traffic when the client is away from its home network*



When a client first connects to an Instant network, a message is sent to all configured virtual controller IP addresses to see if this is an Layer-3 roamed client. On receiving an acknowledgment from any of the configured virtual controller IP addresses, the client is identified as an Layer-3 roamed client. If the Instant AP has no GRE tunnel to this home network, a new tunnel is formed to an Instant AP (home Instant AP) from the client's home network.

Each foreign Instant AP has only one home Instant AP per Instant network to avoid duplication of broadcast traffic. Separate GRE tunnels are created for each foreign Instant AP-home Instant AP pair. If a peer Instant AP is a foreign Instant AP for one client and a home Instant AP for another, two separate GRE tunnels are used to handle Layer-3 roaming traffic between these Instant APs.

If client subnet discovery fails on association due to some reason, the foreign Instant AP identifies its subnet when it sends out the first Layer-3 packet. If the subnet is not a local subnet and belongs to another Instant network, the client is treated as an Layer-3 roamed client and all its traffic is forwarded to the home network through a GRE tunnel.

Configuring Layer-3 Mobility

To configure a mobility domain, you have to specify the list of all Instant networks that form the mobility domain. To allow clients to roam seamlessly among all the Instant APs, specify the virtual controller IP for each foreign subnet. You may include the local Instant or virtual controller IP address, so that the same configuration can be used across all Instant networks in the mobility domain.

It is recommended that you configure all client subnets in the mobility domain.

When the client subnets are configured, note the following scenarios:

- If a client is from a local subnet, it is identified as a local client. When a local client starts using the IP address, Layer-3 roaming is terminated.
- If the client is from a foreign subnet, it is identified as a foreign client. When a foreign client starts using the IP address, Layer-3 roaming is set up.

Home Agent Load Balancing

Home Agent Load Balancing is required in large networks where multiple tunnels might terminate on a single border or lobby Instant AP and overload it. When load balancing is enabled, the virtual controller assigns the home Instant AP for roamed clients by applying a *round robin* policy. With this policy, the load for the Instant APs acting as Home Agents for roamed clients is uniformly distributed across the Instant AP cluster.

Configuring a Mobility Domain for Instant

The following procedure describes how to configure Layer-3 mobility domain by using the WebUI.

Table 193: *Configuring Mobility Domain*

New WebUI	Old WebUI
1. Go to the **Configuration** > **System** page. 2. Click the **Show advanced options**. 3. Expand **L3 Mobility**. 4. Toggle the **Home agent load balancing** switch to enable. By default, home agent load balancing is disabled. 5. Click **+** in the **Virtual Controller IP Addresses** section, add the IP address of a virtual controller that is part of the mobility domain, and click **OK**. 6. Repeat Step 5, to add the IP addresses of all virtual controller that form the Layer-3 mobility domain. 7. Click **+** in the **Subnets** section and specify the following: 8. Enter the client subnet in the **IP address** text box. 9. Enter the mask in the **Subnet mask** text box. 10. Enter the VLAN ID of the home network in the **VLAN ID** text box. 11. Enter the home virtual controller IP address for this subnet in the **Virtual controller IP** text box. 12. Click **OK**. 13. Click **Save**.	1. Click the **System** link on the Instant main window. 2. Click the **Show advanced options** link. 3. Click the **L3 Mobility** tab. 4. Select **Enabled** from the **Home agent load balancing** drop-down list. By default, home agent load balancing is disabled. 5. Click **New** in the **Virtual Controller IP Addresses** section, add the IP address of a virtual controller that is part of the mobility domain, and click **OK**. 6. Repeat Steps 2 to 5, to add the IP addresses of all virtual controller that form the Layer-3 mobility domain. 7. Click **New** in the **Subnets** section and specify the following: 8. Enter the client subnet in the **IP address** text box. 9. Enter the mask in the **Subnet mask** text box. 10. Enter the VLAN ID of the home network in the **VLAN ID** text box. 11. Enter the home virtual controller IP address for this subnet in the **Virtual controller IP** text box. 12. Click **OK** in the **New Subnet** window. 13. Click **OK** in the **L3 Mobility** tab.

The following CLI commands configure a mobility domain:

```
(Instant AP)(config)# l3-mobility
(Instant AP)(L3-mobility)# home-agent-load-balancing
(Instant AP)(L3-mobility)# virtual-controller <IP-address>
(Instant AP)(L3-mobility)# subnet <IP-address> <subnet-mask> <VLAN-ID> <virtual-
controller-IP-address>
```

Chapter 32
Spectrum Monitor

This chapter provides the following information:

- Understanding Spectrum Data on page 486
- Configuring Spectrum Monitors and Hybrid Instant APs on page 493

Understanding Spectrum Data

Wireless networks operate in environments with electrical and RF devices that can interfere with network communications. Microwave ovens, cordless phones, and even adjacent Wi-Fi networks are all potential sources of continuous or intermittent interference. The spectrum monitor software modules on Instant APs can examine the RF environment in which the Wi-Fi network is operating, identify interference, and classify its sources. An analysis of the results can then be used to quickly isolate issues associated with packet transmission, channel quality, and traffic congestion caused by contention with other devices operating in the same band or channel.

Spectrum monitors are Instant AP radios that gather spectrum data but do not service clients. Each SM scans and analyzes the spectrum band used by the SM's radio (2.4 GHz or 5 GHz). An Instant AP radio in hybrid Instant AP mode continues to serve clients as an access point while it analyzes spectrum analysis data for the channel the radio uses to serve clients. You can record data for both types of spectrum monitor devices. However, the recorded spectrum is not reported to the virtual controller. A spectrum alert is sent to the virtual controller when a non-Wi-Fi interference device is detected.

The spectrum monitor is fully supported on all Instant APs or Remote APs with a few exceptions:

- Remote AP3 do not support Spectrum display in the WebUI.
- AP-207, AP-203H, and AP-203RP access points do not support Spectrum Monitor.

The spectrum data is collected by each Instant AP spectrum monitor and hybrid Instant AP. The spectrum data is not reported to the virtual controller. The **Spectrum** link is visible in the WebUI only if you have enabled the Spectrum Monitoring feature.

In the Old WebUI

You can view the following spectrum data:

- Device List
- Non-Wi-Fi Interferers
- Channel Metrics
- Channel Details
- Spectrum Alerts

Device List

The device list consists of a device summary table and channel information for active non-Wi-Fi devices currently seen by a spectrum monitor or hybrid Instant AP radio. To view the device list, click **Spectrum** in the dashboard.

Table 194 shows the device details that are displayed:

Table 194: *Device Summary and Channel Information*

Column	Description
Type	Device type. This parameter can be any of the following: ■ Audio FF (fixed frequency) ■ Bluetooth ■ Cordless base FH (frequency hopper) ■ Cordless phone FF (fixed frequency) ■ Cordless network FH (frequency hopper) ■ Generic FF (fixed frequency) ■ Generic FH (frequency hopper) ■ Generic interferer ■ Microwave ■ Microwave inverter ■ Video ■ Xbox **NOTE:** For additional details about non-Wi-Fi device types shown in this table, see Table 195.
ID	ID number assigned to the device by the spectrum monitor or hybrid Instant AP radio. Spectrum monitors and hybrid Instant APs assign a unique spectrum ID per device type.
Center Frequency (KHz)	Center frequency of the signal sent from the device.
Bandwidth (KHz)	Channel bandwidth used by the device.
Channels-affected	Radio channels affected by the wireless device.
Signal (dBm)	Strength of the signal sent from the device, represented in dBm.
Duty Cycle	Device duty cycle. This value represents the percent of time the device broadcasts a signal.
Add Time	Time at which the device was first detected.
Update Time	Time at which the device's status was updated.

Non-Wi-Fi Interferers

The following table describes each type of non-Wi-Fi interferer detected by the Spectrum Monitor feature:

Table 195: *Non-Wi-Fi Interferer Types*

Non Wi-Fi Interferer	Description
Bluetooth	Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a *Bluetooth* device. Bluetooth uses a frequency hopping protocol.
Fixed Frequency (Audio)	Some audio devices such as wireless speakers and microphones also use fixed frequency to continuously transmit audio. These devices are classified as *Fixed Frequency (Audio)*.
Fixed Frequency (Cordless Phones)	Some cordless phones use a fixed frequency to transmit data (much like the fixed frequency video devices). These devices are classified as *Fixed Frequency (Cordless Phones)*.
Fixed Frequency (Video)	Video transmitters that continuously transmit video on a single frequency are classified as *Fixed Frequency (Video)*. These devices typically have close to a 100% duty cycle. These types of devices may be used for video surveillance, TV or other video distribution, and similar applications.
Fixed Frequency (Other)	All other fixed frequency devices that do not fall into any of the above categories are classified as *Fixed Frequency (Other)*. Note that the RF signatures of the fixed frequency audio, video, and cordless phone devices are very similar and that some of these devices may be occasionally classified as *Fixed Frequency (Other)*.
Frequency Hopper (Cordless Base)	Frequency hopping cordless phone base units transmit periodic beacon-like frames at all times. When the handsets are not transmitting (that is, when there are no active phone calls), the cordless base is classified as *Frequency Hopper (Cordless Base)*.
Frequency Hopper (Cordless Network)	When there is an active phone call and one or more handsets are part of the phone conversation, the device is classified as *Frequency Hopper (Cordless Network)*. Cordless phones may operate in 2.4 GHz or 5 GHz bands. Some phones use both 2.4 GHz and 5 GHz bands (for example, 5 GHz for Base-to-handset and 2.4 GHz for Handset-to-base). These phones may be classified as unique Frequency Hopper devices on both bands.
Frequency Hopper (Xbox)	The Microsoft Xbox device uses a frequency hopping protocol in the 2.4 GHz band. These devices are classified as *Frequency Hopper (Xbox)*.
Frequency Hopper (Other)	When the classifier detects a frequency hopper that does not fall into any of the prior categories, it is classified as *Frequency Hopper (Other)*. Some examples include IEEE 802.11 FHSS devices, game consoles, and cordless or hands-free devices that do not use one of the known cordless phone protocols.
Microwave	Common residential microwave ovens with a single magnetron are classified as a *Microwave*. These types of microwave ovens may be used in cafeterias, break rooms, dormitories, and similar environments. Some industrial, healthcare, or manufacturing environments may also have other equipment that functions like a microwave and may also be classified as a Microwave device.

Table 195: *Non-Wi-Fi Interferer Types*

Non Wi-Fi Interferer	Description
Microwave (Inverter)	Some newer-model microwave ovens have the inverter technology to control the power output and these microwave ovens may have a duty cycle close to 100%. These microwave ovens are classified as *Microwave (Inverter)*. Dual-magnetron industrial microwave ovens with higher duty cycle may also be classified as *Microwave (Inverter)*. There may be other equipment that functions like inverter microwaves in some industrial, healthcare, or manufacturing environments. Those devices may also be classified as *Microwave (Inverter)*.
Generic Interferer	Any non-frequency hopping device that does not fall into any of the prior categories described in this table is classified as a *Generic Interferer*. For example, a Microwave-like device that does not operate in the known operating frequencies used by the Microwave ovens may be classified as a *Generic Interferer*. Similarly wide-band interfering devices may be classified as *Generic Interferers*.

Channel Details

When you move the mouse over a channel, the channel details or the summary of the 2.4 GHz and 5 GHz channels as detected by a spectrum monitor are displayed. You can view the aggregate data for each channel seen by the spectrum monitor radio, including the maximum Instant AP power, interference, and the SNIR. The SNIR is the ratio of signal strength to the combined levels of interference and noise on that channel. Spectrum monitors display spectrum data of all channels in the selected band, and hybrid Instant APs display data for the channel they are monitoring.

Channel Details Information shows the information that you can view in the Channel Details graph.

Table 196: *Channel Details Information*

Column	Description
Channel	An 802.11a or 802.11g radio channel.
Quality(%)	Current relative quality of the channel.
Utilization(%)	The percentage of the channel being used.
Wi-Fi (%)	The percentage of the channel currently being used by Wi-Fi devices.
Type	Device type.
Total nonwifi (%)	The percentage of the channel currently being used by non-Wi-Fi devices.
Known Instant APs	Number of valid Instant APs identified on the radio channel.
UnKnown Instant APs	Number of invalid or rogue Instant APs identified on the radio channel.
Channel Util (%)	Percentage of the channel currently in use.
Max Instant AP Signal (dBm)	Signal strength of the Instant AP that has the maximum signal strength on a channel.
Max Interference(dBm)	Signal strength of the non-Wi-Fi device that has the highest signal strength.

Table 196: *Channel Details Information*

Column	Description
SNIR (dB)	The ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

Channel Metrics

The channel metrics graph displays channel quality, availability, and utilization metrics as seen by a spectrum monitor or hybrid Instant AP. You can view the channel utilization data based on 2.4 GHz and 5 GHz radio channels. The percentage of each channel that is currently being used by Wi-Fi devices, and the percentage of each channel being used by non-Wi-Fi devices and 802.11 ACI. The graph shows the channel availability, the percentage of each channel that is available for use, and the current relative quality of selected channels in the 2.4 GHz or 5 GHz radio bands. To view the graphs, click **2.4 GHz** or **5 GHz** in the **Access Point > Spectrum** section of the dashboard. While spectrum monitors can display data for all channels in their selected band, hybrid Instant APs display data for a single monitored channel.

Channel Metrics shows the information displayed in the **Channel Metrics** graph.

Table 197: *Channel Metrics*

Column	Description
Channel	A 2.4 GHz or 5 GHz radio channel.
Quality(%)	Current relative quality of selected channels in the 2.4 GHz or 5 GHz radio bands, as determined by the percentage of packet retries, the current noise floor, and the duty cycle for non-Wi-Fi devices on that channel.
Availability(%)	The percentage of the channel currently available for use.
Utilization(%)	The percentage of the channel being used.
WiFi Util(%)	The percentage of the channel currently being used by Wi-Fi devices.
Interference Util(%)	The percentage of the channel currently being used by non-Wi-Fi interference plus Wi-Fi ACI.

Spectrum Alerts

When a new non-Wi-Fi device is found, an alert is reported to the virtual controller. The spectrum alert messages include the device ID, device type, IP address of the spectrum monitor or hybrid Instant AP, and the timestamp. The virtual controller reports the detailed device information to AMP.

In the New WebUI

Spectrum data is displayed in the following tabs:

- Overview
- 2.4 GHz
- 5 GHz

Overview

The following table describes each type of non-Wi-Fi interferer detected by the Spectrum Monitor feature:

Table 198: *Non-Wi-Fi Interferer Types*

Non Wi-Fi Interferer	Description
Type	Device type. This parameter can be any of the following: ■ Audio FF (fixed frequency) ■ Bluetooth ■ Cordless base FH (frequency hopper) ■ Cordless phone FF (fixed frequency) ■ Cordless network FH (frequency hopper) ■ Generic FF (fixed frequency) ■ Generic FH (frequency hopper) ■ Generic interferer ■ Microwave ■ Microwave inverter ■ Video ■ Xbox **NOTE:** For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferers .
ID	ID number assigned to the device by the spectrum monitor or hybrid Instant AP radio. Spectrum monitors and hybrid Instant APs assign a unique spectrum ID per device type.
Center Frequency (KHz)	Center frequency of the signal sent from the device.
Bandwidth (KHz)	Channel bandwidth used by the device.
Channels-Affected	Radio channels affected by the wireless device.
Signal (dBm)	Strength of the signal sent from the device, represented in dBm.
Duty Cycle	Device duty cycle. This value represents the percent of time the device broadcasts a signal.
Add Time	Time at which the device was first detected.
Update Time	Time at which the device's status was updated.

2.4 GHz

The following table describes the utilization and quality of a 2.4 GHz radio channel:

Table 199: *2.4 GHz Metrics*

Non Wi-Fi Interferer	Description
Quality(%)	Current relative quality of the channel.

Table 199: *2.4 GHz Metrics*

Non Wi-Fi Interferer	Description
Utilization(%)	The percentage of the channel being used.
WiFi (%)	The percentage of the channel currently being used by Wi-Fi devices.
Bluetooth (%)	Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a *Bluetooth* device. Bluetooth uses a frequency hopping protocol.
Microwave	Common residential microwave ovens with a single magnetron are classified as a *Microwave*. These types of microwave ovens may be used in cafeterias, break rooms, dormitories, and similar environments. Some industrial, healthcare, or manufacturing environments may also have other equipment that functions like a microwave and may also be classified as a Microwave device.
Microwave (Inverter)	Some newer-model microwave ovens have the inverter technology to control the power output and these microwave ovens may have a duty cycle close to 100%. These microwave ovens are classified as *Microwave (Inverter)*. Dual-magnetron industrial microwave ovens with higher duty cycle may also be classified as *Microwave (Inverter)*. There may be other equipments that function like inverter microwaves in some industrial, healthcare, or manufacturing environments. Those devices may also be classified as *Microwave (Inverter)*.
Total nonwifi (%)	The percentage of the channel currently being used by non-Wi-Fi devices.
KnownAPs	Number of valid Instant APs identified on the radio channel.
UnKnowAPs	Number of invalid or rogue Instant APs identified on the radio channel.
Noise Floor (dBm)	
MaxAP Signal (dBm)	Signal strength of the Instant AP that has the maximum signal strength on a channel.
MaxInterference(dBm)	Signal strength of the non-Wi-Fi device that has the highest signal strength.
SNIR (dB)	The ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

The **2.4 GHz** tab also shows a statistical view (in %) on radio channel availaility, Wi-Fi, interference, and quality.

5 GHz

The following table describes the utilization and quality of a 5 GHz radio channel:

Table 200: *5 GHz Metrics*

Non Wi-Fi Interferer	Description
Quality(%)	Current relative quality of the channel.

Table 200: *5 GHz Metrics*

Non Wi-Fi Interferer	Description
Utilization(%)	The percentage of the channel being used.
WiFi (%)	The percentage of the channel currently being used by Wi-Fi devices.
Bluetooth (%)	Any device that uses the Bluetooth protocol to communicate in the 5 GHz band is classified as a *Bluetooth* device. Bluetooth uses a frequency hopping protocol.
Microwave	Common residential microwave ovens with a single magnetron are classified as a *Microwave*. These types of microwave ovens may be used in cafeterias, break rooms, dormitories, and similar environments. Some industrial, healthcare, or manufacturing environments may also have other equipment that functions like a microwave and may also be classified as a Microwave device.
Microwave (Inverter)	Some newer-model microwave ovens have the inverter technology to control the power output and these microwave ovens may have a duty cycle close to 100%. These microwave ovens are classified as *Microwave (Inverter)*. Dual-magnetron industrial microwave ovens with higher duty cycle may also be classified as *Microwave (Inverter)*. There may be other equipments that function like inverter microwaves in some industrial, healthcare, or manufacturing environments. Those devices may also be classified as *Microwave (Inverter)*.
Total nonwifi (%)	The percentage of the channel currently being used by non-Wi-Fi devices.
KnownAPs	Number of valid Instant APs identified on the radio channel.
UnKnowAPs	Number of invalid or rogue Instant APs identified on the radio channel.
Noise Floor (dBm)	
MaxAP Signal (dBm)	Signal strength of the Instant AP that has the maximum signal strength on a channel.
MaxInterference(dBm)	Signal strength of the non-Wi-Fi device that has the highest signal strength.
SNIR (dB)	The ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

The **5 GHz** tab also shows a statistical view (in %) on radio channel availaility, Wi-Fi, interference, and quality.

Configuring Spectrum Monitors and Hybrid Instant APs

An Instant AP can be provisioned to function as a spectrum monitor or as a hybrid Instant AP. The radios on groups of Instant APs can be converted to dedicated spectrum monitors or hybrid Instant APs through the Instant AP group's 802.11a and 802.11g radio profiles.

Converting an Instant AP to a Hybrid Instant AP

You can convert all Instant APs in an Instant network into hybrid Instant APs by selecting the **Background Spectrum Monitoring** option in the 802.11a and 802.11g radio profiles of an Instant AP.

Instant APs in **Access** mode continue to provide normal access service to clients, while providing the additional function of monitoring RF interference. If any Instant AP in the Instant network does not support the Spectrum Monitoring feature, that Instant AP continues to function as a standard Instant AP, rather than a hybrid Instant AP. By default, the background spectrum monitoring option is disabled.

In the hybrid mode, spectrum monitoring is performed only on the home channel. In other words, if the Instant AP-channel width is 80 MHz, spectrum monitoring is performed for 80 MHz. If the channel width is 40, spectrum monitoring is performed for 40 MHz channel. In a dedicated Air Monitor mode, Instant APs perform spectrum monitoring on all channels.
You can convert Instant APs in an Instant network to hybrid mode by using the WebUI or the CLI.

In the Old WebUI

To convert an Instant AP to a hybrid Instant AP:

1. Click the **RF** link on the Instant main window.
2. Click **Show advanced options**.
3. Click the **Radio** tab.
4. To enable a spectrum monitor on the 802.11g radio band of the 2.4 GHz radio profile, select a radio profile in the **2.4 GHz band** section, click **Edit**, and set the **Background spectrum monitoring** parameter to **Enabled**. To create a new 2.4 GHz radio profile, click **New**.
5. To enable a spectrum monitor on the 802.11a radio band, in the 5 GHz radio profile, select a radio profile in the **5 GHz band** section, click **Edit**, and set the **Background spectrum monitoring** parameter to **Enabled**. To create a new 5 GHz radio profile, click **New**.
6. Click **OK**.
7. Click **OK** in the **Radio** tab.

In the New WebUI

To convert an Instant AP to a hybrid Instant AP:

1. Navigate to **Configuration** > **RF** page.
2. Click **Show advanced options**.
3. Expand **Radio**.
4. To enable a spectrum monitor on the 802.11g radio band of an existing 2.4 GHz radio profile, select a radio profile in the **2.4 GHz band** section, modify the profile as required, and enable the **Background spectrum monitoring** toggle switch. To create a new 2.4 GHz radio profile, click **+**.
5. To enable a spectrum monitor on the 802.11a radio band of an existing a 5 GHz radio profile, select a radio profile in the **5 GHz band** section, modify the profile as required, and enable the **Background spectrum monitoring** toggle switch. To create a new 5 GHz radio profile, click **+**.
6. Click **OK**.
7. Click **Save**.

In the CLI

To configure 2.4 GHz radio settings:

```
(Instant AP)(config)# rf dot11g-radio-profile
(Instant AP)(RF dot11g Radio Profile)# spectrum-monitor
```

To configure 5 GHz radio settings:

```
(Instant AP)(config)# rf dot11a-radio-profile
```

```
(Instant AP)(RF dot11a Radio Profile)# spectrum-monitor
```

Converting an Instant AP to a Spectrum Monitor

In spectrum mode, spectrum monitoring is performed on entire bands and the Instant AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring Instant APs or from non-Wi-Fi devices such as microwaves and cordless phones.

By default, spectrum monitoring is performed on a higher band of the 5 GHz radio.

You can configure an Instant AP to function as a stand-alone spectrum monitor by using the WebUI or the CLI.

In the Old WebUI

To convert an Instant AP to a spectrum monitor:

1. In the **Access Points** tab, select the Instant AP that you want to convert to a spectrum monitor.
2. Click the **edit** link.
3. Click the **Radio** tab.
4. From the **Mode** drop-down list, select **Spectrum Monitor**.
5. Click **OK**.
6. Reboot the Instant AP for the changes to take effect.

In the New WebUI

To convert an Instant AP to a spectrum monitor:

1. Go to **Configuration** > **Access Points** and select the Instant AP that you want to convert to a spectrum monitor and click **Edit**.
2. Click **Radio**.
3. Select your preferred band and from the **Mode** drop-down list, select **Spectrum Monitor**.
4. Click **Save**.
5. Reboot the Instant AP for the changes to take effect.

In the CLI

To convert an Instant AP to a spectrum monitor:

```
(Instant AP)# wifi0-mode {<access> | <monitor> | <spectrum-monitor>}
(Instant AP)# wifi1-mode {<access> | <monitor> | <spectrum-monitor>}
```

To enable spectrum monitoring for any other band for the 5 GHz radio:

```
(Instant AP)(config)# rf dot11a-radio-profile
(Instant AP)(RF dot11a Radio Profile)# spectrum-band <type>
```

To view the radio configuration:

```
(Instant AP)# show radio config
2.4 GHz:
Legacy Mode:disable
Beacon Interval:100
802.11d/802.11h:disable
Interference Immunity Level:2
Channel Switch Announcement Count:0
Channel Reuse Type:disable
Channel Reuse Threshold:0
```

```
Background Spectrum Monitor:disable
```

```
5.0 GHz:
Legacy Mode:disable
Beacon Interval:100
802.11d/802.11h:disable
Interference Immunity Level:2
Channel Switch Announcement Count:0
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable
Standalone Spectrum Band:5ghz-upper
```

This section provides information on the following procedures:

- Generating Default Certificates
- Backing up and Restoring Instant AP Configuration Data on page 498
- Converting an Instant AP to a Remote AP and Campus AP on page 499
- Resetting a Remote AP or Campus AP to an Instant AP on page 503
- Rebooting the Instant AP on page 503
- DRT Upgrade

Generating Default Certificates

Instant APs generate default self-signed certificates for captive portal, server authentication, and WebUI management access during initial boot of the AP. These certificates are used as the default certificate for captive portal, WebUI authentication, 802.1X termination, and SSO. Though these certificates serve authentication functions, Aruba *strongly* recommends that you replace these default certificates with a custom certificate issued for your site or domain by a trusted CA. If the validity of default self-signed certificates are expired or about to expire, new ones can be generated by factory resetting the AP.

To generate new default certificates and replace existing ones, use the following procedure:

1. Use the **write erase all** command to delete existing default certificates.
```
(Instant AP) #write erase all
Are you sure you want to erase the configuration? (y/n): y
Erase configuration all.
```



Executing the **write erase all** command factory resets the AP and deletes all data and configurations of the Instant AP.

2. Execute the **reload** command to reboot the AP
```
(Instant AP) #reload
Do you really want to reset the system(y/n): y
Reloading
```

When the Instant AP reboots, the new default certificates are generated and saved to flash. The new default certificates have a validity of 10 years and the issued on time of these certificates is based on the following scenarios:

- If the NTP server is reachable, the issued on time is the current time.
- If the NTP server is not reachable but Central is reachable, the issued on time is Central's time.
- If both NTP and Central are not reachable, the issued on time is the installation time of the current Instant version.



If default certificates are generated for APs in a cluster with 802.1X enabled, the clients will be prompted to accept the self-signed certificate of the AP. Clients can only roam successfully if they trust the certificate of the APs.

Backing up and Restoring Instant AP Configuration Data

You can back up the Instant AP configuration data and restore the configuration when required.

Viewing Current Configuration

The following procedure describes how to view the current configuration on the Instant AP:

- In the old WebUI or the new WebUI, navigate to **Maintenance** > **Configuration** > **Current Configuration**.
- In the CLI, enter the following command at the command prompt:

```
(Instant AP)# show running-config
```

Backing up Configuration Data

The following procedure describes how to back up configuration data using the WebUI

Table 201: *Backing up Configuration Data*

New WebUI	Old WebUI
1. Navigate to the **Maintenance** > **Configuration** page. 2. Click **Backup Configuration**. 3. Click **Continue** to confirm the backup. The *instant.cfg* containing the Instant AP configuration data will be saved in your local file system.	1. Navigate to the **Maintenance** > **Configuration** page. 2. Click **Backup Configuration**. 3. Click **Continue** to confirm the backup. The *instant.cfg* containing the Instant AP configuration data will be saved in your local file system.

The following CLI command shows the configuration that is backed up by the Instant AP:

```
(Instant AP)# show backup-config
```

Restoring Configuration Data

Table 202: *Restoring Configuration Data*

New WebUI	Old WebUI
1. Navigate to the **Maintenance** > **Configuration** page. 2. Click **Restore Configuration**. 3. Click **Browse** to browse your local system and select the configuration file. 4. Click **Restore Now**. 5. Click **Restore Configuration** to confirm restoration. The configuration is restored and the Instant AP reboots to load the new configuration.	1. Navigate to the **Maintenance** > **Configuration** page. 2. Click **Restore Configuration**. 3. Click **Browse** to browse your local system and select the configuration file. 4. Click **Restore Now**. 5. Click **Restore Configuration** to confirm restoration. The configuration is restored and the Instant AP reboots to load the new configuration.

The following CLI command restores the Instant AP configuration:

```
(Instant AP)(config)# copy config tftp://x.x.x.x/confgi.cfg
```

Converting an Instant AP to a Remote AP and Campus AP

This section provides the following information:

- Regulatory Domain Restrictions for Instant AP to RAP or CAP Conversion on page 499
- Converting an Instant AP to a Remote AP on page 499
- Converting an Instant AP to a Campus AP on page 501
- Converting an Instant AP to Stand-Alone Mode on page 503
- Converting an Instant AP using CLI on page 503

Regulatory Domain Restrictions for Instant AP to RAP or CAP Conversion

You can provision an Instant AP as a Campus AP or a Remote AP in a controller-based network. Before converting an Instant AP, ensure that there is a regulatory domain match between the Instant AP and the controller.

The following table describes the regulatory domain restrictions that apply for the Instant AP-to-Campus AP conversion:

Table 203: *Instant AP-to-ArubaOS Conversion*

Instant AP Variant	Instant AP Regulatory Domain	Controller Regulatory Domain			Instant release
		US	Unrestricted	IL	
▪ IAP-207 ▪ IAP-304/IAP-305	US	Y	X	X	Instant 6.5.1.0 or later
	RW	X	Y	Y	
	JP	X	Y	X	
▪ IAP-314/IAP-315 ▪ IAP-334/IAP-335	US	Y	X	X	Instant 6.5.0.0 or later
	RW	X	Y	Y	
	JP	X	Y	X	
▪ IAP-324/IAP-325	US	Y	X	X	Instant 6.4.4.0 or later
	RW	X	Y	Y	
	JP	X	Y	X	
All other Instant APs	US	Y	X	X	Versions prior to Instant 6.3.0.x, Instant 6.3.x.x, Instant 6.4.0.0, and Instant 6.4.x.x
	Unrestricted	X	Y	X	
	IL	X	X	Y	
	JP	X	Y	X	

Converting an Instant AP to a Remote AP

For converting an Instant AP to a Remote AP, the virtual controller sends the Remote AP convert command to all the other Instant APs. The virtual controller, along with the slave Instant APs, sets a VPN tunnel to the remote controller, and downloads the firmware through FTP. The virtual controller uses IPsec to communicate to the Mobility Controller over the Internet.

- If the Instant AP obtains AirWave information through DHCP (Option 43 and Option 60), it establishes an HTTPS connection to the AirWave server, downloads the configuration, and operates in the Instant AP mode.
- If the Instant AP does not get AirWave information through DHCP provisioning, it tries provisioning through the Activate server in the cloud by sending a serial number MAC address. If an entry for the Instant AP is present in Activate and is provisioned as an Instant AP > Remote AP, Activate responds with mobility controller IP address, Instant AP group, and Instant AP type. The Instant AP then contacts the controller, establishes certificate-based secure communication, and obtains configuration and image from the controller. The Instant AP reboots and comes up as a Remote AP. The Instant AP then establishes an IPsec connection with the controller and begins operating in the Remote AP mode.
- If an Instant AP entry is present in Activate and a provisioning rule is configured to return the IP address or host name of the AirWave server, the Instant AP downloads configuration from AirWave and operates in the Instant AP mode.
- If there is no response from Activate, the access point comes up with default configuration and operates in the Instant AP mode.



A mesh point cannot be converted to Remote AP, because mesh access points do not support VPN connection.

An Instant AP can be converted to a Campus AP and Remote AP only if the controller is running ArubaOS 6.1.4.0 or later versions:

The following table describes the supported Instant AP platforms and minimal Instant version required for the Campus AP or Remote AP conversion.

Table 204: *Instant AP Platforms and Minimum Instant Versions for Instant AP-to-Remote AP Conversion*

Instant AP Platform	ArubaOS Release	Instant Release
▪ AP-303P ▪ 510 Series ▪ AP-387	ArubaOS 8.4.0.0 or later versions	Instant 8.4.0.0 or later versions
▪ AP-344/AP-345 ▪ AP-374/ AP-375/AP-377 ▪ 318 Series ▪ 303 Series	ArubaOS 8.3.0.0 or later versions	Instant 8.3.0.0 or later versions
▪ AP-203H	ArubaOS 6.5.3.0 or later versions	Instant 6.5.3.0 or later versions
▪ AP-203R/AP-203RP ▪ AP-303H ▪ AP-365/AP-367	ArubaOS 6.5.2.0 or later versions	Instant 6.5.2.0 or later versions

Instant AP Platform	ArubaOS Release	Instant Release
▪ IAP-304/IAP-305 ▪ IAP-207	ArubaOS 6.5.1.0 or later versions	Instant 4.3.1.0 or later versions
▪ IAP-314/IAP-315 ▪ IAP-334/IAP-335	ArubaOS 6.5.0.0 or later versions	Instant 4.3.0.0 or later versions
▪ IAP-324/IAP-325	ArubaOS 6.4.4.0 or later versions	Instant 4.2.2.0 or later versions

The following procedure describes how to convert an Instant AP to a Remote AP by using the WebUI.

Table 205: *Converting Remote AP to Instant AP*

New WebUI	Old WebUI
1. Go to the **Maintenance** > **Convert** page. 2. Select **Remote APs managed by a Mobility Controller** from the **Convert one or more Access Points to** drop-down list. 3. Enter the host name or the IP address of the controller in the **Hostname or IP Address of Mobility Controller** text box. Contact your local network administrator to obtain the IP address. 4. Ensure that the Mobility Controller IP address is reachable by the Instant APs. 5. Click **Convert** to complete the conversion. 6. Click **OK** to confirm the conversion. The Instant AP reboots and begins operating in the Remote AP mode. After conversion, the Instant AP is managed by the Mobility Controller.	1. Click **Maintenance** in the Instant main window. 2. Click the **Convert** tab. 3. Select **Remote APs managed by a Mobility Controller** from the **Convert one or more Access Points to** drop-down list. 4. Enter the host name or the IP address of the controller in the **Hostname or IP Address of Mobility Controller** text box. Contact your local network administrator to obtain the IP address. 5. Ensure that the Mobility Controller IP address is reachable by the Instant APs. 6. Click **Convert Now** in the **Maintenance** tab. 7. Click **Convert Now** in the **Confirm Access Point Conversion** window. The Instant AP reboots and begins operating in the Remote AP mode. After conversion, the Instant AP is managed by the Mobility Controller. 8. Click **Close**.

NOTE:

- For Instant APs to function as Remote APs, configure the Instant AP in the Remote AP whitelist and enable the FTP service on the controller.
- If the VPN setup fails and an error message is displayed, click **OK**, copy the error logs, and share them with your local administrator.

Converting an Instant AP to a Campus AP

The following procedure describes how to convert an Instant AP to a Campus AP by using the WebUI.

Table 206: *Converting an Instant AP to a Campus AP*

New WebUI	Old WebUI
1. Go to the **Maintenance** > **Convert** page. 2. Select **Campus APs managed by a Mobility**	1. Click **Maintenance** in the Instant main window. 2. Click the **Convert** tab.

New WebUI	Old WebUI
Controller from the **Convert one or more Access Points to** drop-down list. 3. Enter the host name, FQDN, or the IP address of the controller in the **Hostname or IP Address of Mobility Controller** text box. Contact your local administrator to obtain these details. 4. Click **Convert** to complete the conversion. 5. Click **OK** to confirm the conversion. The Instant AP reboots and begins operating in the Campus AP mode. After conversion, the Instant AP is managed by the Mobility Controller.	3. Select **Campus APs managed by a Mobility Controller** from the **Convert one or more Access Points to** drop-down list. 4. Enter the host name, FQDN, or the IP address of the controller in the **Hostname or IP Address of Mobility Controller** text box. Contact your local administrator to obtain these details. 5. Click **Convert Now** in the **Maintenance** tab. 6. Click **Convert Now** in the **Confirm Access Point Conversion** window. The Instant AP reboots and begins operating in the Campus AP mode. After conversion, the Instant AP is managed by the Mobility Controller. 7. Click **Close**.

Instant AP to Campus AP conversion using Activate

Instant Access Points can be converted into Campus Access Points using Activate. An Instant AP periodically checks for provisioning updates with the Activate server and the Activate server responds with a provisioning rule, if configured. To convert an Instant AP to a Campus AP, the provisioning rule from Activate contains the AP mode and the Controller IP address to download the image. Upon receiving the Provisioning rule , the Instant AP downloads the image from the controller at the Controller IP address. The Instant AP then erases all configurations, reboots with the new image and converts itself into a Campus AP. The Instant AP now operates as a Campus AP and searches for a controller to connect with.

The converted Campus APs can be enabled with Zero Touch Provisioning for easy installation or can be bound to a controller. This is done by configuring the **IAP to CAP provisioning rule** in the Activate Server. For information on configuring provisioning rules in Activate, refer to the *Aruba Activate User Guide*.

Campus AP with ZTP enabled

In this mode, the Instant AP receives the provisioning rule from Activate and downloads the image from the controller at the Controller IP address. It then reboots as a Campus AP with ZTP enabled and searches for a controller to connect with using ZTP. Campus APs enabled with ZTP can be provisioned to any network with a Controller without any manual configuration changes. To enable ZTP on Campus APs, uncheck the **Persist Controller IP** checkbox when configuring a **IAP to CAP Provisioning rule** in Activate.

Campus AP bound to a Controller

In this mode, the Instant AP receives the provisioning rule from Activate , downloads the image from the controller at the Controller IP address, saves the IP address and is bound to that controller. The Instant AP then reboots as a Campus AP and is bound with the Controller. Campus APs bound to a controller do not perform standard controller discovery and cannot be provisioned in another network without manual configuration changes. To bind the Campus AP to the Controller, select the **Persist Controller IP** checkbox when configuring a **IAP to CAP Provisioning rule** in Activate.

The following CLI command shows logs related to provision update with Activate:

```
(Instant AP)# show log provision
```

Converting an Instant AP to Stand-Alone Mode

This feature allows you to deploy an Instant AP as an autonomous Instant AP, which is a separate entity from the existing virtual controller cluster in the Layer 2 domain.

When an Instant AP is converted to function in stand-alone mode, it cannot join a cluster of Instant APs even if the Instant AP is in the same VLAN. If the Instant AP is in the cluster mode, it can form a cluster with other virtual controller Instant APs in the same VLAN.

The following procedure describes how to deploy an Instant AP as a stand-alone or autonomous Instant AP using the WebUI.

Table 207: *Converting an Instant AP to Stand-Alone Mode*

New WebUI	Old WebUI
1. Go to the **Maintenance** > **Convert** page. 2. Select **Standalone AP** from the **Convert one or more Access Points to** drop-down list. 3. Select the Access Point from the **Access Point to Convert** drop-down list. 4. Click **Convert** to complete the conversion. The Instant AP now operates in the stand-alone mode. 5. Click **Close**.	1. Click **Maintenance** in the Instant main window. 2. Click the **Convert** tab. 3. Select **Standalone AP** from the **Convert one or more Access Points to** drop-down list. 4. Select the Access Point from the **Access Point to Convert** drop-down list. 5. Click **Convert Now** to complete the conversion. The Instant AP now operates in the stand-alone mode. 6. Click **Close**.

Converting an Instant AP using CLI

The following CLI command converts an Instant AP to a Remote AP or Campus AP:

```
(Instant AP)# convert-aos-ap <mode> <controller-IP-address>
```

The following CLI command converts an Instant AP to a stand-alone Instant AP or to provision an Instant AP in the cluster mode:

```
(Instant AP)# swarm-mode <mode>
```

Resetting a Remote AP or Campus AP to an Instant AP

The reset knob located on the rear of an Instant AP can be used to reset the Instant AP to factory default settings.

To reset an Instant AP, perform the following steps:

1. Turn off the Instant AP.
2. Press and hold the reset knob using a small and narrow object such as a paperclip.
3. Turn on the Instant AP without releasing the reset knob. The power LED flashes within 5 seconds indicating that the reset is completed.
4. Release the reset knob. The Instant AP reboots with the factory default settings.

Rebooting the Instant AP

If you encounter any problem with the Instant APs, you can reboot all Instant APs or a selected Instant AP in a network using the WebUI.

Table 208: *Configuring RTLS Support*

New WebUI	Old WebUI
1. Go to the **Maintenance** > **Reboot** page. 2. In the **Select the access point you wish to reboot** drop-down list, select the Instant AP that you want to reboot and click **Reboot**. To reboot all the Instant APs in the network, click **Reboot All** from the drop-down list and click **Reboot**. 3. Click **OK** to continue. The **Access Points are rebooting** message is displayed indicating that the reboot is in progress. 4. Click **OK**.	1. Click **Maintenance** in the Instant main window. 2. Click the **Reboot** tab. 3. In the Instant AP list, select the Instant AP that you want to reboot and click **Reboot selected Access Point**. To reboot all the Instant APs in the network, click **Reboot All.** 4. The **Confirm Reboot for AP** message is displayed. Click **Reboot Now** to proceed. The **Reboot in Progress** message is displayed indicating that the reboot is in progress. The **Reboot Successful** message is displayed after the process is complete. If the system fails to boot, the **Unable to contact Access Points after reboot was initiated** message is displayed. 5. Click **OK**.

DRT Upgrade

The DRT upgrade feature installs and upgrades the DRT file for an Instant AP. When new certifications are available for Instant APs, the subsequent releases will automatically receive support for these certs. Only the newer version of the DRT file is used for an upgrade.



Instant supports DRT upgrade from AirWave, over HTTPs and WebSocket. Instant APs can report the DRT upgrade status to AirWave and AirWave can also display the DRT upgrade status to users.

The DRT file is installed under the following scenarios:

Instant AP Boot Up

The DRT information is stored at two locations, one in the image file, and another in the flash memory. Every time an Instant AP boots up, it compares the DRT version at both the locations and uses the newer version of DRT in the flash.

Install DRT File In a Cluster

When all the Instant APs in a cluster finish downloading the DRT table, the master Instant AP communicates to the slave Instant APs to upgrade the DRT file. After the slave Instant APs upgrade the DRT file, the master Instant AP proceeds with DRT upgrade. There is a timeout mechanism set during the download and upgrade process. When a slave Instant AP has finished DRT downloading from the master Instant AP, but has not received an upgrade command within 5 minutes, the slave Instant AP will attempt to upgrade the DRT file without waiting. Similarly, if the slave Instant AP has not finished downloading within 5 minutes, the master Instant AP will not wait for these slaves. It will continue with the rest of the upgrade process.

The DRT version can be upgraded by using the WebUI.

Table 209: *Upgrading DRT version*

New WebUI	Old WebUI
1. Navigate to the **Maintenance** > **Regulatory** page. 2. To manually upgrade an Instant AP's DRT version, select the DRT file or update a URL in the **Manual** section. 3. If you are using a DRT file, select the **DRT file** radio button, click **Browse**, and then click **Upgrade Now**. 4. If you are using a DRT URL, select the **DRT URL** radio button and enter the link in the URL text box. 5. Click **Upgrade Now**.	1. Navigate to the **Maintenance** > **DRT** page. 2. To upgrade by using a DRT file, select the **DRT file** radio button and click **Browse** to upload the file. 3. To upgrade the DRT by using a web URL, select the **DRT URL** radio button and enter the link in the **URL** text box. 4. Click **Upgrade Now**.
NOTE: If a new version of DRT is displayed in the **Automatic** section, upgrade it by clicking **Upgrade Now**.	

The following CLI command upgrades an Instant AP cluster with the new DRT version:

```
upgrade-drt <url>
```

The following CLI command resets the DRT version on an Instant AP:

```
reset drt
```

The following CLI command shows the status of DRT version on an Instant AP:

```
show drt state
```



Instant supports DRT upgrade from AirWave, over HTTPs and WebSocket. Instant APs can report the DRT upgrade status to AirWave and AirWave can also display the DRT upgrade status to users.

This chapter describes the following topics:

- Configuring SNMP on page 506
- Configuring Syslog Servers on page 509
- Configuring TFTP Dump Server on page 511
- Running Debug Commands on page 511
- Uplink Bandwidth Monitoring on page 515
- WAN Link Health Monitoring on page 516

Configuring SNMP

This section provides the following information:

- SNMP Parameters for Instant AP on page 506
- Configuring SNMP on page 507
- Configuring SNMP Traps on page 508

SNMP Parameters for Instant AP

Instant supports SNMPv1, SNMPv2, and SNMPv3 for reporting purposes only. An Instant AP cannot use SNMP to set values in an Aruba system.

You can configure the following parameters for an Instant AP:

Table 210: *SNMP Parameters for Instant AP*

Parameter	Description
Community Strings for SNMPV1 and SNMPV2	An SNMP community string is a text string that acts as a password, and is used to authenticate messages sent between the virtual controller and the SNMP agent.
If you are using SNMPv3 to obtain values from the Instant AP, you can configure the following parameters:	
Name	A string representing the name of the user.
Authentication Protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol used. This can take one of the two values: ■ MD5—HMAC-MD5-96 Digest Authentication Protocol ■ SHA—HMAC-SHA-96 Digest Authentication Protocol

Table 210: *SNMP Parameters for Instant AP*

Parameter	Description
Authentication protocol password	If messages sent on behalf of this user can be authenticated, a (private) authentication key is used with the authentication protocol. This is a string password for MD5 or SHA based on the conditions mentioned above.
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol that is used. This takes the value of CBC-DES symmetric encryption.
Privacy protocol password	If messages sent on behalf of this user can be encrypted or decrypted with DES, the (private) privacy key with the privacy protocol is used.

Configuring SNMP

The following procedure describes how to configure SNMPv1, SNMPv2, and SNMPv3 community strings by using the WebUI.

Creating Community Strings for SNMPv1 and SNMPv2

The following procedure describes how to create community strings for SNMPv1 and SNMPv2:

Table 211: *Configuring Community Strings for SNMPv1 and SNMPv2*

New WebUI	Old WebUI
1. Go to **Configuration** > **System**. 2. Click the **Show advanced options** link. 3. Expand **Monitoring**. 4. Click **+** under the **Community Strings for SNMPV1 and SNMPV2** box. 5. Enter the string in the **Edit Community String** text box and click **OK**. 6. To delete a community string, select the string and delete. 7. Click **Save**.	1. Click the **System** link on the Instant main window. 2. Click the **Show advanced options** link. 3. Go to the **Monitoring** tab. 4. Click **New** under the **Community Strings for SNMPv1 and SNMPv2** box. 5. Enter the string in the **New Community String** text box and click **OK**. 6. To delete a community string, select the string, and click **Delete**. 7. Click **OK** in the **Monitoring** tab.

Creating Community Strings for SNMPv3

The following procedure describes how to create community strings for SNMPv3:

Table 212: *Configuring Community Strings for SNMPv3*

New WebUI	Old WebUI
1. Go to **Configuration** > **System**. 2. Click the **Show advanced options** link. 3. Expand **Monitoring**. 4. Click **+** under the **Users for SNMPV3** box. 5. Enter the name of the user in the **Name** text box. 6. Select the type of authentication protocol from the **Authentication Protocol** drop-down list.	1. Click the **System** link on the Instant main window. 2. Click the **Show advanced options** link. 3. Go to the **Monitoring** tab. 4. Click **New** under the **Users for SNMPV3** box. The **New SNMPv3 User** window is displayed. 5. Enter the name of the user in the **Name** text box. 6. Select the type of authentication protocol from the

New WebUI	Old WebUI
7. Enter the authentication password in the **Password** text box and retype the password in the **Retype** text box. 8. Select the type of privacy protocol from the **Privacy Protocol** drop-down list. 9. Enter the privacy protocol password in the **Password** text box and retype the password in the **Retype** text box. 10. Click **OK**. 11. To edit the details for a particular user, select the user and edit. 12. To delete a particular user, select the user and delete. 13. Click **Save**.	**Auth protocol** drop-down list. 7. Enter the authentication password in the **Password** text box and retype the password in the **Retype** text box. 8. Select the type of privacy protocol from the **Privacy protocol** drop-down list. 9. Enter the privacy protocol password in the **Password** text box and retype the password in the **Retype** text box. 10. Click **OK**. 11. To edit the details for a particular user, select the user and click **Edit**. 12. To delete a particular user, select the user and click **Delete**. 13. Click **OK** in the **Monitoring** tab.

The following CLI commands configure an SNMP engine ID and host:

```
(Instant AP)(config)# snmp-server engine-id <engine-ID>
(Instant AP)(config)# host <ipaddr> version {1 <name> udp-port <port>}|{2c|3 <name>
[inform] [udp-port <port>]}
```

The following CLI command configures SNMPv1 and SNMPv2 community strings:

```
(Instant AP)(config)# snmp-server community <password>
```

The following CLI command configures SNMPv3 community strings:

```
(Instant AP)(config)# snmp-server user <name> <auth-protocol> <password> <privacy-
protocol> <password>
```

The following CLI command shows SNMP configuration:

```
(Instant AP)# show snmp-configuration
Engine ID:D8C7C8C44298
Community Strings
-----------------
Name
----
SNMPv3 Users
------------
Name  Authentication Type  Encryption Type
----  -------------------  ---------------
SNMP Trap Hosts
---------------
IP Address  Version  Name  Port  Inform
----------  -------  ----  ----  ------
```

Configuring SNMP Traps

Instant supports the configuration of external trap receivers. Only the Instant AP acting as the virtual controller generates traps. The traps for Instant AP cluster are generated with virtual controller IP as the source IP, if virtual controller IP is configured. The OID of the traps is 1.3.6.1.4.1.14823.2.3.3.1.200.2.X.

The following procedure describes how to configure SNMP traps by using the WebUI.

Table 213: *Configuring SNMP Traps*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **System**.	1. Navigate to **System** > **Show advanced options** >

New WebUI	Old WebUI
2. Click **Show advanced options**. 3. Expand **Monitoring**. 4. Go to the **SNMP** section. 5. Under **SNMP Trap Receivers**, click **+** and update the following information in the window that is displayed: ▪ **IP address**—Enter the **IP Address** of the new SNMP Trap receiver. ▪ **Version**—Select the SNMP version— **v1, v2c, v3** from the drop-down list. The version specifies the format of traps generated by the access point. ▪ **Community/Username**—Specify the community string for SNMPv1 and SNMPv2c traps and a username for SNMPv3 traps. ▪ **Port**—Enter the port to which the traps are sent. The default value is 162. ▪ **Inform**—When enabled, traps are sent as SNMP INFORM messages. It is applicable to SNMPv3 only. The default value is **Yes**. 6. Click **OK**. The trap receiver information will be displayed in the **SNMP Trap Receivers** window. 7. Click **Save**.	**Monitoring**. 2. Under **SNMP Traps**, click **New**. The **New SNMP Trap Receiver** window is displayed. 3. Enter the following information: ▪ **IP Address**—Enter the **IP Address** of the new SNMP Trap receiver. ▪ **Version**—Select the SNMP version— **v1, v2c, v3** from the drop-down list. The version specifies the format of traps generated by the access point. ▪ **Community/Username**—Specify the community string for SNMPv1 and SNMPv2c traps and a username for SNMPv3 traps. ▪ **Port**—Enter the port to which the traps are sent. The default value is 162. ▪ **Inform**—When enabled, traps are sent as SNMP INFORM messages. It is applicable to SNMPv3 only. The default value is **Yes**. 4. Click **OK**. The trap receiver information will be displayed in the **SNMP Trap Receivers** window. 5. Click **OK** in the **Monitoring** tab.

The following CLI command configures SNMP traps:

```
(Instant AP)(config)# snmp-server host <IP-address> {version 1 | version 2 | version 3}
<name> udp-port <port> inform
```



Instant APs support SNMP MIBs along with Instant MIBs. For information about MIBs and SNMP traps, refer to the *ArubaInstant MIB Reference Guide*.

Configuring Syslog Servers

The following procedure describes how to specify a syslog server for sending syslog messages to the external servers by using the WebUI.

Table 214: *Configuring Syslog Servers*

New WebUI	Old WebUI
1. Go to **Configuration** > **System**. 2. Click **Show advanced options**. 3. Expand **Monitoring**. 4. In the **Syslog server** text box which is in the **Servers** section, enter the IP address of the syslog servers to which you want to send system logs. Up to of 3 syslog servers can be configured for the AP,	1. In the Instant main window, click the **System** link. 2. Click **Show advanced options** to display the advanced options. 3. Click the **Monitoring** tab. 4. In the **Syslog server** text box in the **Servers** section, enter the IP address of the syslog servers to which you want to send system logs. Up to 3

New WebUI	Old WebUI
each one separated by a comma in the following format: syslog server 1, syslog server 2, syslog server 3. **NOTE:** The syslog source address is sent individually by the Instant APs in the cluster and never the virtual controller IP. Even the master Instant AP sends the syslog source address from its actual IP address. 5. In the **Syslog Facility Levels** section, select the required values to configure syslog facility levels. Syslog Facility is an information field associated with a syslog message. It is an application or operating system component that generates a log message. The following seven facilities are supported by Syslog: ■ **System**—Log about configuration and system status. ■ **Ap-Debug**—Detailed log about the Instant AP device. ■ **User**—Important logs about client. ■ **Network**—Log about change of network; for example, when a new Instant AP is added to a network. ■ **User-Debug**—Detailed logs about client debugging. ■ **Security**—Log about network security; for example, when a client connects using wrong password. ■ **Wireless**—Log about radio. 6. The logging levels in the Syslog Dialog box are described in the Logging Levels table below. 7. Click **Save**.	syslog servers can be configured for the AP, each one separated by a comma in the following format: syslog server 1, syslog server 2, syslog server 3. **NOTE:** The syslog source address is sent individually by the Instant APs in the cluster and never the virtual controller IP. Even the master Instant AP sends the syslog source address from its actual IP address. 5. Select the required values to configure syslog facility levels. Syslog Facility is an information field associated with a syslog message. It is an application or operating system component that generates a log message. The following seven facilities are supported by Syslog: ■ **Ap-Debug**—Detailed log about the Instant AP device. ■ **Network**—Log about change of network; for example, when a new Instant AP is added to a network. ■ **Security**—Log about network security; for example, when a client connects using wrong password. ■ **System**—Log about configuration and system status. ■ **User**—Important logs about client. ■ **User-Debug**—Detailed logs about client debugging. ■ **Wireless**—Log about radio. 6. The logging levels in the Syslog Dialog box are described in the Logging Levels table below. 7. Click **OK**.

The following table describes the logging levels in the **Syslog** drop-down list, in order of severity from the most severe to the least severe.

Table 215: *Logging Levels*

Logging Level	Description
Emergency	Panic conditions that occur when the system becomes unusable.
Alert	Any condition requiring immediate attention and correction.
Critical	Any critical conditions such as a hard drive error.
Errors	Error conditions.
Warning	Warning messages.

Logging Level	Description
Notice	Significant events of a noncritical and normal nature. The default value for all Syslog facilities.
Information	Messages of general interest to system users.
Debug	Messages containing information useful for debugging.

The following CLI commands configure a syslog server:

```
(Instant AP)(config)# syslog-server <syslog server 1> <syslog server 2> <syslog server 3>
```

The following CLI commands configure syslog facility levels:

```
(Instant AP)(config)# syslog-level <logging-level>[ap-debug |network |security |system
|user | user-debug | wireless]
```

The following CLI commands show syslog logging levels:

```
(Instant AP)# show syslog-level
Logging Level
-------------
Facility    Level
--------    -----
ap-debug    warn
network     warn
security    warn
system      warn
user        warn
user-debug  warn
wireless    error
```

Configuring TFTP Dump Server

The following procedure describes how to configure a TFTP server for storing core dump files by using the WebUI.

Table 216: *Configuring TFTP Dump Server*

New WebUI	Old WebUI
1. Go to **Configuration** > **System**. 2. Click **Show advanced options**. 3. Expand **Monitoring**. 4. In the **Servers** section, enter the IP address of the TFTP server in the **TFTP Dump Server** text box. 5. Click **Save**.	1. In the Instant main window, click the **System** link. 2. Click **Show advanced options** to display the advanced options. 3. Click the **Monitoring** tab. 4. Enter the IP address of the TFTP server in the **TFTP Dump Server** text box. 5. Click **OK**.

The following CLI command configures a TFTP server:

```
(Instant AP)(config)# tftp-dump-server <IP-address>
```

Running Debug Commands

The following procedure describes how to run the debugging commands using the WebUI.

Table 217: *Running Debug Commands*

New WebUI	Old WebUI
1. Select **Support** from the left pane of the Instant main window. 2. Select the required option from the **Command** drop-down list. 3. Select **All Access Points** or **Instant Access Point (VC)** from the **Target** drop-down list. 4. Click **Run** and then click **Save**. The output of all the selected commands is displayed in the same page. Additionally, the output of all the selected commands is displayed in the **Console** page.	1. Navigate to **More** > **Support** on the Instant main window. 2. Select the required option from the **Command** drop-down list. 3. Select **All Access Points** or **Instant Access Point (VC)** from the **Target** drop-down list. 4. Click **Run** and then click **Save**. The output of all the selected commands is displayed in a single page.
NOTE: The **Support** window allows you to run commands for each access point and virtual controller in a cluster.	

For a complete list of commands supported in a particular release train, execute the **show support-commands** command at the Instant AP CLI. The output of this command displays the list of support commands that you can run through the WebUI and the corresponding CLI commands. For more information on these commands, refer to the respective command page in the *Aruba Instant CLI Reference Guide*.

```
(Instant AP) # show support-commands
Support Commands
----------------
Description                                Command Name
-----------                                ------------
AP Tech Support Dump                       show tech-support
AP Tech Support Dump Supplemental          show tech-support supplemental
AP Provisioning Status                     show activate status
AP 3G/4G Status                            show cellular status
AP 802.1X Statistics                       show ap debug dot1x-statistics
AP Access Rule Table                       show access-rule-all
AP Inbound Firewall Rules                  show inbound-firewall-rules
AP Active                                  show aps
AP AirGroup Cache                          show airgroup cache entries
AP AirGroup CPPM Entries                   show airgroup cppm entries
AP AirGroup CPPM Servers                   show airgroup cppm server
AP AirGroup Debug Statistics               show airgroup debug statistics
AP AirGroup Servers                        show airgroup servers verbose
AP AirGroup User                           show airgroup users verbose
AP ALE Configuration                       show ale config
AP ALE Status                              show ale status
AP Allowed Channels                        show ap allowed-channels
AP Allowed MAX-EIRP                        show ap allowed-max-EIRP
AP All Supported Timezones                 show clock timezone all
AP ARM Bandwidth Management                show ap arm bandwidth-management
AP ARM Channels                            show arm-channels
AP ARM Configuration                       show arm config
AP ARM History                             show ap arm history
AP ARM Neighbors                           show ap arm neighbors
AP ARM RF Summary                          show ap arm rf-summary
AP ARM Scan Times                          show ap arm scan-times
AP ARP Table                               show arp
AP Association Table                       show ap association
AP Authentication Frames                   show ap debug auth-trace-buf
AP Auth-Survivability Cache                show auth-survivability cached-info
AP Auth-Survivability Debug Log            show auth-survivability debug-log
```

AP BSSID Table	show ap bss-table
AP Captive Portal Domains	show captive-portal-domains
AP Captive Portal Auto White List	show captive-portal auto-white-list
AP Client Match Status	show ap debug client-match
AP Client Match History	show ap client-match-history
AP Client Match Action	show ap client-match-actions
AP Client Match Live	show ap client-match-live
AP Client Match Triggers	show ap client-match-triggers
AP Client Table	show ap debug client-table
AP Client View	show ap client-view
AP Country Codes	show country-codes
AP CPU Details	show cpu details
AP CPU Utilization	show cpu
AP Crash Info	show ap debug crash-info
AP Current Time	show clock
AP Current Timezone	show clock timezone
AP Datapath ACL Table Allocation	show datapath acl-allocation
AP Datapath ACL Tables	show datapath acl-all
AP Datapath Bridge Table	show datapath bridge
AP Datapath DMO session	show datapath dmo-session
AP Datapath DMO station	show datapath dmo-station
AP Datapath Dns Id Map	show datapath dns-id-map
AP Datapath Multicast Table	show datapath mcast
AP Datapath Nat Pool	show datapath nat-pool
AP Datapath Route Table	show datapath route
AP Datapath Session Table	show datapath session
AP Datapath DPI Session Table	show datapath session dpi
AP Datapath DPI Session Table Verbose	show datapath session dpi verbose
AP Datapath Statistics	show datapath statistics
AP Datapath User Table	show datapath user
AP Datapath VLAN Table	show datapath vlan
AP DPI Debug statistics	show dpi debug statistics
AP Daylight Saving Time	show clock summer-time
AP Derivation Rules	show derivation-rules
AP Driver Configuration	show ap debug driver-config
AP Election Statistics	show election statistics
AP External Captive Portal Status	show external-captive-portal
AP Environment Variable	show ap-env
AP ESSID Table	show network
AP Flash Configuration	show ap flash-config
AP IGMP Group Table	show ip igmp
AP Interface Counters	show interface counters
AP Interface Status	show port status
AP Internal DHCP Status	show dhcp-allocation
AP IP Interface	show ip interface brief
AP IP Route Table	show ip route
AP L3 Mobility Datapath	show l3-mobility datapath
AP L3 Mobility Events log	show log l3-mobility
AP L3 Mobility Status	show l3-mobility status
AP LACP Status	show lacp status
AP Log All	show log debug
AP Log AP-Debug	show log ap-debug
AP Log Conversion	show log convert
AP Log Driver	show log driver
AP Log Kernel	show log kernel
AP Log Network	show log network
AP Log PPPd	show log pppd
AP Log Rapper	show log rapper
AP Log Rapper Counter	show log rapper-counter
AP Log Rapper Brief	show log rapper-brief
AP Log Sapd	show log sapd

AP Log Security	show log security
AP Log System	show log system
AP Log Tunnel Status Management	show log apifmgr
AP Log Upgrade	show log upgrade
AP Log User-Debug	show log user-debug
AP Log User	show log user
AP Log VPN Tunnel	show log vpn-tunnel
AP Log Wireless	show log wireless
AP Management Frames	show ap debug mgmt-frames
AP Memory Allocation State Dumps	show malloc-state-dumps
AP Memory Utilization	show memory
AP Mesh Counters	show ap mesh counters
AP Mesh Link	show ap mesh link
AP Mesh Neighbors	show ap mesh neighbours
AP Monitor Active Laser Beams	show ap monitor active-laser-beams
AP Monitor AP Table	show ap monitor ap-list
AP Monitor ARP Cache	show ap monitor ARP Cache
AP Monitor Client Table	show ap monitor sta-list
AP Monitor Containment Information	show ap monitor containment-info
AP Monitor Potential AP Table	show ap monitor pot-ap-list
AP Monitor Potential Client Table	show ap monitor pot-sta-list
AP Monitor Router	show ap monitor routers
AP Monitor Scan Information	show ap monitor scan-info
AP Monitor Status	show ap monitor status
AP Persistent Clients	show ap debug persistent-clients
AP PMK Cache	show ap pmkcache
AP PPPoE uplink debug	show pppoe debug-logs
AP PPPoE uplink status	show pppoe status
AP Processes	show process
AP Radio 0 Client Probe Report	show ap client-probe-report 0
AP Radio 0 Stats	show ap debug radio-stats 0
AP Radio 0 info	show ap debug radio-info 0
AP Radio 1 Client Probe Report	show ap client-probe-report 1
AP Radio 1 Stats	show ap debug radio-stats 1
AP Radio 1 info	show ap debug radio-info 1
AP RADIUS Statistics	show ap debug radius-statistics
AP Termination RADIUS Statistics	show ap debug radius-statistics termination
AP Shaping Table	show ap debug shaping-table
AP Sockets	show socket
AP STM Configuration	show ap debug stm-config
AP Swarm State	show swarm state
AP System Status	show ap debug system-status
AP System Summary	show summary support
AP Uplink Status	show uplink status
AP User Table	show clients
AP Valid Channels	show valid-channels
AP Version	show version
AP Virtual Beacon Report	show ap virtual-beacon-report
AP VPN Config	show vpn config
AP VPN Status	show vpn status
AP IAP-VPN Retry Counters	show vpn tunnels
AP Wired Port Settings	show wired-port-settings
AP Wired User Table	show clients wired
AP Checksum	show ap checksum
AP Spectrum AP table	show ap spectrum ap-list
AP Spectrum channel table	show ap spectrum channel-details
AP Spectrum channel metrics	show ap spectrum channel-metrics
AP Spectrum channel summary	show ap spectrum channel-summary
AP Spectrum client table	show ap spectrum client-list
AP Spectrum device duty cycle	show ap spectrum device-duty-cycle
AP Spectrum non-wifi device history	show ap spectrum device-history

AP Spectrum non-wifi device table	show ap spectrum device-list
AP Spectrum non-wifi device log	show ap spectrum device-log
AP Spectrum number of device	show ap spectrum device-summary
AP Spectrum interference-power table	show ap spectrum interference-power
AP Spectrum status	show ap spectrum status
VC 802.1x Certificate	show 1xcert
VC All Certificates	show cert all
VC radsec Certificates	show radseccert
VC Captive Portal domains	show captive-portal-domains
VC About	show about
VC Active Configuration	show running-config
VC AirGroup Service	show airgroupservice
VC AirGroup Status	show airgroup status
VC Allowed AP Table	show allowed-aps
VC AMP Status	show ap debug airwave
VC AMP Current State Data	show ap debug airwave-state
VC AMP Current Stats Data	show ap debug airwave-stats
VC AMP Data Sent	show ap debug airwave-data-sent
VC AMP Events Pending	show ap debug airwave-events-pending
VC AMP Last Configuration Received	show ap debug airwave-config-received
VC AMP Single Sign-on Key	show ap debug airwave-signon-key
VC AMP Configuration Restore Status	show ap debug airwave-restore-status
VC Central Current State Data	show ap debug cloud-state
VC Central Current Stats Data	show ap debug cloud-stats
VC Central Data Sent	show ap debug cloud-data-sent
VC Central Events Pending	show ap debug cloud-events-pending
VC Central Last Configuration Received	show ap debug cloud-config-received
VC Central Single Sign-on Key	show ap debug cloud-signon-key
VC Central Configuration Restore Status	show ap debug cloud-restore-status
VC Application Services	show app-services
VC Cloud Server Status	show ap debug cloud-server
VC DHCP Option 43 Received	show dhcpc-opts
VC Global Alerts	show alert global
VC Global Statistics	show stats global
VC IDS AP List	show ids aps
VC IDS Client List	show ids clients
VC Internal DHCP Server Configuration	show ip dhcp database
VC Local User Database	show users
VC Provisioning Log	show log provision
VC Radius Attributes	show radius-attributes
VC Radius Servers	show radius-servers support
AP Radius Status	show radius status
VC Saved Configuration	show configuration
VC Scanning Stats	show aps scanning
VC Show SBR Table	show datapath sbr
VC SNMP Configuration	show snmp-configuration
VC Uplink 3G/4G Configuration	show cellular config
VC Uplink Management Configuration	show uplink config
VC WISPr Configuration	show wispr config
VC XML API Server Information	show xml-api-server
VC rfc3576-radius statistics	show ap debug rfc3576-radius-statistics



Use the **support** commands under the supervision of Aruba technical support.

Uplink Bandwidth Monitoring

An Instant AP uses Iperf3 as a TCP or UDP client to run a speed test and measure the bandwidth on an uplink. The results from the speed test are collated by the Instant AP and published to ALE. Speed tests can be run only on master Instant APs. They cannot be run on slave Instant APs.

Apart from ALE, Instant APs can collate and send speed test information to Central by using Iperf3.

You may choose to configure and execute a speed test profile during boot time and additionally at specific time intervals using the configuration mode or execute the speed test at any preferred time using the privileged EXEC mode in the CLI.

The following CLI commands configure and automatically run speed tests at specific time intervals:

```
(Instant AP)(config)# speed-test
(Instant AP)(speed-test)# include-reverse
(Instant AP)(speed-test)# server-ip <server>
(Instant AP)(speed-test)# server-port <port>
(Instant AP)(speed-test)# on-boot
(Instant AP)(speed-test)# omit
(Instant AP)(speed-test)# protocol <tcp/udp>
(Instant AP)(speed-test)# parallel
(Instant AP)(speed-test)# time-interval <interval>
(Instant AP)(speed-test)# bandwidth <bandwidth>
(Instant AP)(speed-test)# sec-to-measure <secs>
(Instant AP)(speed-test)# window
```

The following CLI command configures and executes a speed test at any preferred time:

```
(Instant AP)(config)# speed-test 10.17.144.8  tcp include-reverse sec-to-measure 10
server-port 5201 parallel 10 omit 1 window 512
```

The following CLI command shows the speed test results:

```
(Instant AP)# show speed-test data
```

The following CLI command shows the uplink bandwidth counter:

```
(Instant AP)# show ale stats
ALE Stats
---------
Type Value
---- -----
VC package 0
RSSI package 0
APPRF package 0
URLv package 0
STATE package 0
STAT package 0
UPLINK BW package 0
Total 0
```

WAN Link Health Monitoring

Starting from Instant 8.3.0.0, Instant APs support the WAN Link Health Monitoring feature for the Service Assurance application. The Service Assurance application helps run various tests to determine the network performance and reachability of hosts that are configured by the customer.

WAN Link Health Monitoring supports Aruba Central WAN Health Monitoring feature. It helps Aruba Central customers get periodic statistics on reachability, connectivity, and Instant AP performance.



WAN Link Health Monitoring supports only IPv4 addresses. It does not support IPv6 addresses in this release.

From Central, customers can send request (using the **Clarity > Health Checks** page or API interface) to run the following performance and reachability test suites:

- Reachability
  - Ping/ICMP test for reachability
    - Supports up to five host names/IP addresses.
    - Response information for the Ping test containing the number of transmitted and received packets, and response time are sent.
- Connectivity
  - TCP Connect test for connectivity to hosts
  - Supports maximum of five host name/IP address and port combinations. Only IPv4 addresses are supported.
- Performance
  - Iperf (UDP/TCP) test for WAN speed/performance
    - Supports maximum of five host IPs as input.
    - Response contains the important parameters parsed from iperf3 response.
  - wget (webpage load) tests for Instant AP performance
    - Supports up to five valid URLs.
    - Download rate and download bytes are sent back in response along with the

      The execution time for each test can be up to 36 seconds. Central customers can configure any of these tests that can be run on demand or at scheduled intervals for any branch or site.



Instant APs support a maximum of four test suites with five hosts each. On-demand policies are prioritized against periodic policies.

On-Demand Policies

An on-demand policy is executed once when a request is received. It is not stored on the AP. For example, when a network admin finds a problem and wants to troubleshoot it, the admin user can send an on-demand policy to run some tests and check the results to troubleshoot the problem.

- Each Instant AP can handle one on-demand policy at a time. If there is an on-demand policy in progress and another on-demand policy request is received by anInstant AP, Central receives a NACK response.
- If an Instant AP is executing a periodic policy and an on-demand policy request is received, then the on-demand policy is executed after executing the periodic policy.

Periodic Policies

Periodic policies are run periodically based on a schedule and periodicity. Up to 4 periodic policies can be added for an Instant AP. The schedule is defined at policy level and periodicity is defined test suite level. They can be used to monitor a given branch or site for various parameters, and get the required statistics.

Points to Note:

- Central customers must have an API Gateway or Clarity Health Check license.
- The user from the customer's branch or site must have admin access to Instant AP and Central.
- This feature is supported only on Instant APs.
- IPv6 address is not supported.

- Central customers can set thresholds so that the application can trigger notifications when set thresholds are reached.
- Central customers can monitor the network performance data.
- The policy entries are cleared when Central connection goes DOWN.
- If a device restarts or Central connection goes DOWN and then restores, then Central takes care to resend the policies to the same device or a different device.
- When a policy request is received and no test is running at that time, all the tests in the request are run sequentially. The order in which tests are executed (if configured) is reachability, connectivity, and then performance tests.
- When a test is already running and a new policy request is seen, NACK response is sent to Aruba Central and the policy is rejected.

Aruba Central sends the customer-configured tests and the associated data to Instant AP devices as protocol buffer messages. The Instant APs parse the protocol buffer messages and converts them into a policy. Instant APs then run these tests sequentially, collate the test results, and send them as protocol buffer messages to Central.

Verification of WAN Link Health Monitoring Status

The following CLI command shows the WAN Link Health Monitoring status:

```
(Instant AP) #show lhm status
```

The following command shows the Health Checks sent from Central to Instant AP:

```
(Instant AP) #show lhm policy
```

Troubleshooting WAN Link Health Monitoring

The following command shows trace logs of WAN Link Health Monitoring process:

```
(Instant AP) #trace component LHM sub-component ALL
(Instant AP) #trace level DEBUG LHM
(Instant AP) #show trace log lhm <no_of_lines>
```



These commands are for troubleshooting purpose only and must be disabled after that.

Chapter 35
Hotspot Profiles

This chapter contains the following topics:

- Understanding Hotspot Profiles on page 519
- Configuring Hotspot Profiles on page 521
- Sample Configuration on page 538



In the current release, Instant supports the hotspot profile configuration only through the CLI.

Understanding Hotspot Profiles

Hotspot 2.0 R1 is a WFA specification based on the 802.11u protocol, which allows wireless clients to discover hotspots using management frames (such as beacon, association request, and association response), connect to networks, and roam between networks without additional authentication.

Hotspot 2.0 provides the following services:

- Network discovery and selection—Allows the clients to discover suitable and available networks by advertising the access network type, roaming consortium, and venue information through the management frames. For network discovery and selection, GAS and ANQP are used.
- QOS Mapping—Provides a mapping between the network-layer QoS packet marking and over- the-air QoS frame marking based on user priority.

Starting from Aruba Instant 8.3.0.0, the Hotspot 2.0 R2 is introduced. This feature is supported on all Instant APs except the 5xx series access points. This release supports the following new features:

- Online Sign-Up—Mobile devices use Online Sign-Up (OSU) for registration and credential provisioning to obtain secure network access using the service provider's OSU server.
- WNM Subscription Remediation—Subscription remediation is a process that Home Service Providers use to correct, update, and resolve subscription issues. WNM(11v) is used for Subscription Remediation.
- When a hotspot is configured in a network:
- The clients search for available hotspots using the beacon management frame.
- When a hotspot is found, the client sends queries to obtain information about the type of network authentication and IP address, and IP address availability using the GAS action frames.
- Based on the response of the advertisement server (response to the GAS Action Frames), the relevant hotspot is selected and the client attempts to associate with it.
- Based on the authentication mode used for mobility clients, the client authenticates to access the network.

GAS

GAS is a request-response protocol, that provides L2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps to determine an 802.11 infrastructure before associating clients and allows clients to send queries to multiple 802.11 networks in parallel.

An Instant AP can include its SP Organization Identifier indicating the identity of the SP in beacons and probe responses to clients. When a client recognizes an Instant AP's OI, it attempts to associate to that Instant AP using the security credentials corresponding to that SP. If the client does not recognize the AP's OI, the client sends a GAS query to the Instant AP to request more information about the network before associating. A client transmits a GAS Query using a GAS Initial Request frame and the Instant AP provides the query response or information on how to receive the query response in a GAS Initial Response frame. To transmit a GAS query for any advertisement protocol, the advertisement protocol ID must include the advertisement protocol information element with details of the advertisement protocol and its corresponding advertisement control.

ANQP

ANQP provides a range of information, such as IP address type and availability, roaming partners accessible through a hotspot, and the EAP method supported for authentication, for a query and response protocol. The ANQP Information Elements provide additional data that can be sent from an Instant AP to the client to identify the Instant AP's network and service provider. If a client requests this information through a GAS query, the hotspot Instant AP sends the ANQP capability list in the GAS Initial Response frame indicating support for the following IEs:

- Venue Name
- Domain Name
- Network Authentication Type
- Roaming Consortium List
- Network Access Identifier Realm
- 3GPP Cellular Network Data
- IP Address Availability

H2QP

The H2QP profiles provide a range of information on Hotspot 2.0 elements such as hotspot protocol and port, operating-class, operator names, WAN status, OSU provider list, and uplink and downlink metrics.

Information Elements and Management Frames

The Hotspot 2.0 configuration supports the following IEs:

- Interworking IE—Provides information about the Interworking service capabilities such as the Internet availability in a specific service provider network.
- Advertisement Protocol IE—Provides information about the advertisement protocol that a client can use for communication with the advertisement servers in a network.
- Roaming Consortium IE—Provides information about the service provider network for roaming clients, which can be used to authenticate with the Instant AP.

The IEs are included in the following Management Frames when 802.11u is enabled:

- Beacon Frame
- Probe Request Frame

- Probe Response frame
- Association Request
- Re-Association request

Network Access Identifier Realm List

A Network Access Identifier Realm profile identifies and describes a NAI realm to which the clients can connect. The NAI realm settings on an Instant AP act as an advertisement profile to determine the NAI realm elements that must be included as part of a GAS Response frame.

Configuring Hotspot Profiles

To configure a hotspot profile, perform the following steps:

1. Create the required ANQP and H2QP advertisement profiles.
2. Create a hotspot profile.
3. Associate the required ANQP and H2QP advertisement profiles created in step 1 to the hotspot profile created in step 2.
4. Create an SSID Profile with enterprise security and WPA2 encryption settings and then associate the SSID with the hotspot profile created in step 2.

Creating Advertisement Profiles for Hotspot Configuration

A hotspot profile contains one or several advertisement profiles. The following advertisement profiles can be configured through the Instant CLI:

- ANQP advertisement profiles
  - NAI Realm profile
  - Venue Name Profile
  - Network Authentication Profile
  - Roaming Consortium Profile
  - 3GPP Profile
  - IP Address availability Profile
  - Domain Name Profile
- H2QP advertisement profiles
  - Operator Friendly Name Profile
  - Connection Capability Profile
  - Operating-Class Profile
  - WAN-Metrics Profile
  - OSU Provider Profile

Configuring an NAI Realm Profile

The following CLI commands configure a Network Access Identifier Realm profile to define the NAI realm information, which can be sent as an ANQP IE in a GAS query response.

The following CLI commands configure a NAI profile:

```
(Instant AP)(config)# hotspot anqp-nai-realm-profile <name>
(Instant AP)(nai-realm <name>)# nai-realm-name <name>
(Instant AP)(nai-realm <name>)# nai-realm-encoding {<utf8>|<rfc4282>}
```

```
(Instant AP)(nai-realm <name>)# nai-realm-eap-method <eap-method>
(Instant AP)(nai-realm <name>)# nai-realm-auth-id-1 <authentication-ID>
(Instant AP)(nai-realm <name>)# nai-realm-auth-id-2 <authentication-ID>
(Instant AP)(nai-realm <name>)# nai-realm-auth-value-1 <authentication-value>
(Instant AP)(nai-realm <name>)# nai-realm-auth-value-2 <authentication-value>
(Instant AP)(nai-realm <name>)# nai-home-realm
(Instant AP)(nai-realm <name>)# enable
```

You can specify any of the following EAP methods for the **nai-realm-eap-method <eap-method>** command:

- **identity**—To use EAP Identity type. The associated numeric value is 1.
- **notification**—To allow the hotspot realm to use EAP Notification messages for authentication. The associated numeric value is 2.
- **one-time-password**—To use Authentication with a single-use password. The associated numeric value is 5.
- **generic-token-card**—To use EAP-GTC. The associated numeric value is 6.
- **eap-tls**—To use EAP-TLS. The associated numeric value is 13.
- **eap-sim**—To use EAP for GSM SIM. The associated numeric value is 18.
- **eap-ttls**—To use EAP-TTLS. The associated numeric value is 21.
- **peap**—To use PEAP. The associated numeric value is 25.
- **crypto-card**—To use crypto card authentication. The associated numeric value is 28.
- **peapmschapv2**—To use PEAP with MSCHAPv2. The associated numeric value is 29.
- **eap-aka**—To use EAP for UMTS Authentication and Key Agreement. The associated numeric value is 50.

The following table lists the possible authentication IDs and their respective values:

Table 218: *NAI Realm Profile Configuration Parameters*

Authentication ID	Authentication Value
reserved ■ Uses the reserved authentication method. ■ The associated numeric value is **0**.	—
expanded-eap ■ Uses the expanded EAP authentication method. ■ The associated numeric value is **1**.	Use expanded-eap as the authentication value.
non-eap-inner-auth ■ Uses non-EAP inner authentication type. ■ The associated numeric value is **2**.	The following authentication values apply: ■ **reserved**—The associated numeric value is **0**. ■ **pap**—The associated numeric value is **1**. ■ **chap**—The associated numeric value is **2**. ■ **mschap**—The associated numeric value is **3**. ■ **mschapv2**—The associated numeric value is **4**.
eap-inner-auth	The following authentication values apply:

Table 218: *NAI Realm Profile Configuration Parameters*

Authentication ID	Authentication Value
■ Uses EAP inner authentication type.The associated numeric value is **3**.	■ **reserved**—The associated numeric value is **0**. ■ **pap**—The associated numeric value is **1**. ■ **chap**—The associated numeric value is **2**. ■ **mschap**—The associated numeric value is **3**. ■ **mschapv2**—The associated numeric value is **4**.
exp-inner-eap ■ Uses the expanded inner EAP authentication method. ■ The associated numeric value is **4**.	Use the exp-inner-eap authentication value.
credential ■ Uses credential authentication. ■ The associated numeric value is **5**.	The following authentication values apply: ■ **sim**—The associated numeric value is **1**. ■ **usim**—The associated numeric value is **2**. ■ **nfc-secure**—The associated numeric value is **3**. ■ **hw-token**—The associated numeric value is **4**. ■ **softoken**—The associated numeric value is **5**. ■ **certificate**—The associated numeric value is **6**. ■ **uname-password**—The associated numeric value is **7**. ■ **none**—The associated numeric value is **8**. ■ **reserved**—The associated numeric value is **9**. ■ **vendor-specific**—The associated numeric value is **10**.

Configuring a Venue Name Profile

The following CLI commands configure a venue name profile to send the venue information as an ANQP IE in a GAS query response.

The following CLI commands configure a venue name profile:

```
(Instant AP)(config)# hotspot anqp-venue-name-profile <name>
(Instant AP)(venue-name <name>)# venue-name <name>
(Instant AP)(venue-name <name>)# venue-group <group-name>
(Instant AP)(venue-name <name>)# venue-type <type>
(Instant AP)(venue-name <name>)# venue-lang-code <language>
(Instant AP)(venue-name <name>)# enable
```

You can specify any of the following venue groups and the corresponding venue types:

Table 219: *Venue Types*

Venue Group	Associated Venue Type Value
unspecified The associated numeric value is **0**.	—
assembly The associated numeric value is **1**.	■ unspecified—The associated numeric value is **0**. ■ arena—The associated numeric value is **1**.

Table 219: *Venue Types*

Venue Group	Associated Venue Type Value
	▪ stadium—The associated numeric value is **2**. ▪ passenger-terminal—The associated numeric value is **3**. ▪ amphitheater—The associated numeric value is **4**. ▪ amusement-park—The associated numeric value is **5**. ▪ place-of-worship—The associated numeric value is **6**. ▪ convention-center—The associated numeric value is **7**. ▪ library—The associated numeric value is **8**. ▪ museum—The associated numeric value is **9**. ▪ restaurant—The associated numeric value is **10**. ▪ theater—The associated numeric value is **11**. ▪ bar—The associated numeric value is **12**. ▪ coffee-shop—The associated numeric value is **13**. ▪ zoo-or-aquarium—The associated numeric value is **14**. ▪ emergency-cord-center—The associated numeric value is **15**.
business The associated numeric value is **2**.	▪ unspecified—The associated numeric value is **0**. ▪ doctor—The associated numeric value is **1**. ▪ bank—The associated numeric value is **2**. ▪ fire-station—The associated numeric value is **3**. ▪ police-station—The associated numeric value is **4**. ▪ post-office—The associated numeric value is **6**. ▪ professional-office—The associated numeric value is **7**. ▪ research-and-dev-facility—The associated numeric value is **8**. ▪ attorney-office—The associated numeric value is **9**.
educational The associated numeric value is **3**.	▪ unspecified—The associated numeric value is **0**. ▪ school-primary—The associated numeric value is **1**. ▪ school-secondary—The associated numeric value is **2**. ▪ univ-or-college—The associated numeric value is **3**.
factory-and-industrial The associated numeric value is **4**.	▪ unspecified—The associated numeric value is **0**. ▪ factory—The associated numeric value is **1**.
institutional The associated numeric value is **5**.	▪ unspecified—The associated numeric value is **0**. ▪ hospital—The associated numeric value is **1**. ▪ long-term-care—The associated numeric value is **2**. ▪ alc-drug-rehab—The associated numeric value is **3**. ▪ group-home—The associated numeric value is **4**. ▪ prison-or-jail—The associated numeric value is **5**.

Table 219: *Venue Types*

Venue Group	Associated Venue Type Value
mercantile The associated numeric value is **6**.	▪ unspecified—The associated numeric value is **0**. ▪ retail-store—The associated numeric value is **1**. ▪ grocery-market—The associated numeric value is **2**. ▪ auto-service-station—The associated numeric value is **3**. ▪ shopping-mall—The associated numeric value is **4**. ▪ gas-station—The associated numeric value is **5**
residential The associated numeric value is **7**.	▪ unspecified—The associated numeric value is **0**. ▪ private-residence—The associated numeric value is **1**. ▪ hotel—The associated numeric value is **2**. ▪ dormitory—The associated numeric value is **3**. ▪ boarding-house—The associated numeric value is **4**.
storage The associated numeric value is **8**.	unspecified—The associated numeric value is **0**.
utility-misc The associated numeric value is **9**.	unspecified—The associated numeric value is **0**.
vehicular The associated numeric value is **10**.	▪ unspecified—The associated numeric value is **0**. ▪ automobile-or-truck—The associated numeric value is **1**. ▪ airplane—The associated numeric value is **2**. ▪ bus—The associated numeric value is **3**. ▪ ferry—The associated numeric value is **4**. ▪ ship—The associated numeric value is **5**. ▪ train—The associated numeric value is **6**. ▪ motor-bike—The associated numeric value is **7**.
outdoor The associated numeric value is **11**.	▪ unspecified—The associated numeric value is **0** ▪ muni-mesh-network—The associated numeric value is **1**. ▪ city-park—The associated numeric value is **2**. ▪ rest-area—The associated numeric value is **3**. ▪ traffic-control—The associated numeric value is **4**. ▪ bus-stop—The associated numeric value is **5**. ▪ kiosk—The associated numeric value is **6**.

Configuring a Network Authentication Profile

The following CLI commands configure a network authentication profile to define the authentication type used by the hotspot network.

The following CLI commands configure a network authentication profile:

```
(Instant AP)(config)# hotspot anqp-nwk-auth-profile <name>
(Instant AP)(network-auth <name>)# nwk-auth-type <type>
(Instant AP)(network-auth <name>)# url <URL>
```

```
(Instant AP)(network-auth <name>)# enable
```

You can specify any of the following network authentication type for the **nwk-auth-type <type>** command:

- **accept-term-and-cond**—When configured, the network requires the user to accept terms and conditions. This option requires you to specify a redirection URL string as an IP address, FQDN or URL.
- **online-enrollment**—When configured, the network supports the online enrollment.
- **http-redirect**—When configured, additional information on the network is provided through HTTP or HTTPS redirection.
- **dns-redirect**—When configured, additional information on the network is provided through DNS redirection. This option requires you to specify a redirection URL string as an IP address, FQDN, or URL.

Configuring a Roaming Consortium Profile

The following CLI commands configure a roaming consortium profile to send the roaming consortium information as an ANQP IE in a GAS query response.

The following CLI commands configure a roaming consortium profile:

```
(Instant AP)(config)# hotspot anqp-roam-cons-profile <name>
(Instant AP)(roaming-consortium <name>)# roam-cons-oi <roam-cons-oi>
(Instant AP)(roaming-consortium <name>)# roam-cons-oi-len <roam-cons-oi-len>
(Instant AP)(roaming-consortium <name>)# enable
```

Specify a hexadecimal string of 3–5 octets for **roam-cons-oi <roam-cons-oi>**.

Based on the organization identifier specified, you can specify the following parameters for the length of organization identifier in **roam-cons-oi-len <roam-cons-oi-len>**.

- For 0: 0 Octets in the organization identifier (Null)
- For 3: OI length is 24-bits (3 Octets)
- For 5: OI length is 36-bits (5 Octets)

Configuring a 3GPP Profile

The following CLI commands configure a 3GPP profile to define information for the 3G Cellular Network for hotspots.

The following CLI commands configure a 3GPP profile:

```
(Instant AP)(config)# hotspot anqp-3gpp-profile <name>
(Instant AP)(3gpp <name>)# 3gpp-plmn1 <plmn-ID>
(Instant AP)(3gpp <name>)# enable
```

The PLMN ID is a combination of the mobile country code and network code. You can specify up to 6 PLMN IDs for a 3GPP profile.

Configuring an IP Address Availability Profile

The following CLI commands configure an available IP address types to send information on IP address availability as an ANQP IE in a GAS query response.

To configure an IP address availability profile:

```
(Instant AP)(config)# hotspot anqp-ip-addr-avail-profile <name>
(Instant AP)(IP-addr-avail <name>)# ipv4-addr-avail
(Instant AP)(IP-addr-avail <name>)# ipv6-addr-avail
(Instant AP)(IP-addr-avail <name>)# enable
```

Configuring a Domain Profile

You can configure a domain profile to send the domain names as an ANQP IE in a GAS query response.

The following CLI commands configure a domain name profile, execute the following commands:

```
(Instant AP)(config)# hotspot anqp-domain-name-profile <name>
(Instant AP)(domain-name <name>)# domain-name <domain-name>
(Instant AP)(domain-name <name>)# enable
```

Configuring an Operator-Friendly Profile

The following CLI commands configure an operator-friendly name profile to define the identify the operator.

The following CLI commands configure an H2QP operator-friendly name profile:

```
(Instant AP)(config)# hotspot h2qp-oper-name-profile <name>
(Instant AP)(operator-friendly-name <name>)# op-fr-name <op-fr-name>
(Instant AP)(operator-friendly-name <name>)# op-lang-code <op-lang-code>
(Instant AP)(operator-friendly-name <name>)# enable
```

Configuring a Connection Capability Profile

The following CLI commands configure a connection capability profile to define information such as the hotspot IP protocols and associated port numbers that are available for communication.

The following CLI commands configure an H2QP connection capability profile:

```
(Instant AP)(config) # hotspot h2qp-conn-cap-profile <name>
(Instant AP)(connection-capabilities <name>)# esp-port
(Instant AP)(connection-capabilities <name>)# icmp
(Instant AP)(connection-capabilities <name>)# tcp-ftp
(Instant AP)(connection-capabilities <name>)# tcp-http
(Instant AP)(connection-capabilities <name>)# tcp-pptp-vpn
(Instant AP)(connection-capabilities <name>)# tcp-ssh
(Instant AP)(connection-capabilities <name>)# tcp-tls-vpn
(Instant AP)(connection-capabilities <name>)# tcp-voip
(Instant AP)(connection-capabilities <name>)# udp-ike2
(Instant AP)(connection-capabilities <name>)# udp-ipsec-vpn
(Instant AP)(connection-capabilities <name>)# udp-voip
(Instant AP)(connection-capabilities <name>)# enable
```

Configuring an Operating-Class Profile

The following CLI commands configure an operating-class profile to list the channels on which the hotspot is capable of operating. To configure an H2QP operating-class profile:

```
(Instant AP)(config) # hotspot h2qp-oper-class-profile <name>
(Instant AP)(operator-class <name>)# op-class <class-ID>
(Instant AP)(operator-class <name>)# enable
```

Configuring a WAN Metrics Profile

The following CLI commands configure a WAN metrics profile to define information about access network characteristics such as link status and metrics.

The following CLI commands configure a WAN metrics profile:

```
(Instant AP)(config)# hotspot h2qp-wan-metrics-profile <name>
(Instant AP)(WAN-metrics <name>)# at-capacity
(Instant AP)(WAN-metrics <name>)# downlink-load <load>
(Instant AP)(WAN-metrics <name>)# downlink-speed <speed>
(Instant AP)(WAN-metrics <name>)# load-duration <duration>
(Instant AP)(WAN-metrics <name>)# symm-link
```

```
(Instant AP)(WAN-metrics <name>)# uplink-load <load>
(Instant AP)(WAN-metrics <name>)# uplink-speed <speed>
(Instant AP)(WAN-metrics <name>)# wan-metrics-link-status <status>
```

You can specify the following WAN downlink and uplink parameters:

- **Downlink load**—Indicates the percentage of the WAN downlink currently utilized. The default value of 0 indicates that the downlink speed is unknown or unspecified.
- **Downlink speed**—Indicates the WAN downlink speed in Kbps.
- **Uplink load**—Indicates the percentage of the WAN uplink currently utilized. The default value of 0 indicates that the downlink speed is unknown or unspecified.
- **Uplink speed**—Indicates the WAN uplink speed in Kbps.
- **Load duration**—Indicates the duration in seconds during which the downlink utilization is measured.
- **Symmetric links**—Indicates if the uplink and downlink have the same speed.
- **WAN Link Status**—Indicates if the WAN is down (link-down), up (link-up), or in test state (link-under-test).

Configuring an OSU Provider Profile

You can create an OSU provider profile and attach them to a hotspot profile to enable wireless devices to use OSU. The OSU providers list element provides information for one or more entities offering OSU service. For each OSU provider, information such as friendly name (in one or more human languages), NAI(used to authenticate to the OSU ESS if configured for OSEN), icon(s), and URI of the OSU Server are provided.

The following CLI command downloads the icon file to the Instant AP:

```
(Instant AP)# hs2-osu-icon-download <idx> <ftp/tftp/http URL syntax>
```



The maximum size supported for the icon file is 32 KB.

The icon file is downloaded from the specified location using the specified protocol and stored in the file system with the specified index as reference.

The following CLI command deletes an icon file from Instant AP:

```
(Instant AP)# hs2-osu-icon-delete <idx>
```

Table 220: *HS2 OSU Icon Download Parameters*

Parameter	Description
<idx>	Indicates the index of the file which can take values from 1 to 16.
<url>	The protocol that is used to download the icon file. The protocol can be FTP, TFTP, or HTTP.

The following commands create and configure various parameters of the OSU provider profile:

```
(Instant AP) (config) # hotspot h2qp-osu-provider-profile <name>
(Instant AP) (osu-provider <name>) # frnd-name-count <count>
(Instant AP) (osu-provider <name>) # frnd-name1-lang-code <lang code>
(Instant AP) (osu-provider <name>) # frnd-name1 <OSU Friendly name>
(Instant AP) (osu-provider <name>) # frnd-name1-hex <OSU Friendly name>
(Instant AP) (osu-provider <name>) # frnd-name2-lang-code <lang code>
(Instant AP) (osu-provider <name>) # frnd-name2 <OSU Friendly name>
(Instant AP) (osu-provider <name>) # frnd-name2-hex <OSU Friendly name>
(Instant AP) (osu-provider <name>) # iconfile-count <count>
(Instant AP) (osu-provider <name>) # icon1-width <width>
(Instant AP) (osu-provider <name>) # icon1-height <height>
(Instant AP) (osu-provider <name>) # icon1-lang-code <lang code>
(Instant AP) (osu-provider <name>) # icon1-type <file type>
(Instant AP) (osu-provider <name>) # icon1-file <idx> <File Name>
(Instant AP) (osu-provider <name>) # icon2-width <width>
(Instant AP) (osu-provider <name>) # icon2-height <height>
(Instant AP) (osu-provider <name>) # icon2-lang-code <lang code>
(Instant AP) (osu-provider <name>) # icon2-type <file type>
(Instant AP) (osu-provider <name>) # icon2-file <idx> <File Name>
(Instant AP) (osu-provider <name>) # srvcdesc-count <count>
(Instant AP) (osu-provider <name>) # srvc-desc1-lang-code <lang code>
(Instant AP) (osu-provider <name>) # srvc-desc1 <description>
(Instant AP) (osu-provider <name>) # srvc-desc1-hex <description>
(Instant AP) (osu-provider <name>) # srvc-desc2-lang-code <lang code>
(Instant AP) (osu-provider <name>) # srvc-desc2 <description>
(Instant AP) (osu-provider <name>) # srvc-desc2-hex <description>
(Instant AP) (osu-provider <name>) # osu-server-uri <OSU server URI>
(Instant AP) (osu-provider <name>) # osu-method <OSU method>
```

Table 221: *HS2 OSU Provider Parameters*

Parameter	Description	Range
enable	Enables the OSU provider profile. This is enabled by default.	—
frnd-name-count	Number of OSU friendly names to be configured.	1-2
frnd-name1	The first OSU friendly name if you selected the language code as English. A string value of maximum 64 characters.	—
frnd-name1-hex	The first OSU friendly name in hexadecimal format for language codes other than English.	—
frnd-name1-lang-code	The language code used for configuring the first OSU friendly name.	—
frnd-name2	The second OSU friendly name if the language code chosen is English. A string value of maximum 64 characters.	—
frnd-name2-hex	The second OSU friendly name in hexadecimal format for language codes other than English.	—
frnd-name2-lang-code	The language code used for configuring the second OSU friendly name.	—
icon1-file	The index and name of the first icon image file. **NOTE:** The index value and the filename value must match the file downloaded to Instant AP. For more information on downloading the icon file, refer to Downloading Icon Files to Instant AP on page	—

Table 221: *HS2 OSU Provider Parameters*

Parameter	Description	Range
	528.	
icon1-height	Height of the first icon image file.	1-256
icon1-lang-code	Indicates the language used in the first icon image.	—
icon1-type	Type of the image file used as first icon.	—
icon1-width	Width of the first icon image file.	1-256
icon2-file	The index and name of the second icon image file. **NOTE:** The index value and the filename value must match the file downloaded to Instant AP. For more information on downloading the icon file, refer to Downloading Icon Files to Instant AP on page 528.	—
icon2-height	Height of the second icon image file.	—
icon2-lang-code	Indicates the language used in the second icon image.	—
icon2-type	Type of the image file used as second icon.	—
icon2-width	Width of the second icon image file.	—
iconfile-count	Number of icon files to be used for the OSU provider.	1-2
no	Deletes the command.	—
osu-method	Indicates the method used by OSU to provision the HS2 client.	■ OMA-DM ■ SOAP-XML
osu-server-uri	The URI of the OSU Server that is used for OSU with the service provider configured in the **frnd-name1** parameter.	—
srvc-desc1	The first service description if you selected the language code as English.	—
srvc-desc1-hex	The first service description in hexadecimal format for language codes other than English.	—
srvc-desc1-lang-code	The language code used for the first description.	—
srvc-desc2	The second service description if you selected the language code as English.	—
srvc-desc2-hex	The second service description in hexadecimal format for language codes other than English.	—

Table 221: *HS2 OSU Provider Parameters*

Parameter	Description	Range
srvc-desc2-lang-code	The second service description if you selected the language code as English.	—
srvcdesc-count	Number of descriptions to be provided for the OSU provider.	—

Creating a Hotspot Profile

The following CLI commands create a hotspot profile:

```
(Instant AP)(config)# hotspot hs-profile <name>
(Instant AP)(Hotspot2.0 <name>)# asra
(Instant AP)(Hotspot2.0 <name>)# access-network-type <type>
(Instant AP)(Hotspot2.0 <name>)# addtl-roam-cons-ois <roam-consortium-OIs>
(Instant AP)(Hotspot2.0 <name>)# comeback-mode
(Instant AP)(Hotspot2.0 <name>)# gas-comeback <delay-interval>
(Instant AP)(Hotspot2.0 <name>)# group-frame-block
(Instant AP)(Hotspot2.0 <name>)# hessid <hotspot-essid>
(Instant AP)(Hotspot2.0 <name>)# internet
(Instant AP)(Hotspot2.0 <name>)# osu-nai <osu-nai>
(Instant AP)(Hotspot2.0 <name>)# osu-ssid <ssid>
(Instant AP)(Hotspot2.0 <name>)# p2p-cross-connect
(Instant AP)(Hotspot2.0 <name>)# p2p-dev-mgmt
(Instant AP)(Hotspot2.0 <name>)# pame-bi
(Instant AP)(Hotspot2.0 <name>)# qos-map-excp
(Instant AP)(Hotspot2.0 <name>)# qos-map-range
(Instant AP)(Hotspot2.0 <name>)# query-response-length-limit <integer>
(Instant AP)(Hotspot2.0 <name>)# roam-cons-len-1 <integer>
(Instant AP)(Hotspot2.0 <name>)# roam-cons-len-2 <integer>
(Instant AP)(Hotspot2.0 <name>)# roam-cons-len-3 <integer>
(Instant AP)(Hotspot2.0 <name>)# roam-cons-oi-1 <integer>
(Instant AP)(Hotspot2.0 <name>)# roam-cons-oi-2 <integer>
(Instant AP)(Hotspot2.0 <name>)# roam-cons-oi-3 <integer>
(Instant AP)(Hotspot2.0 <name>)# venue-group <group>
(Instant AP)(Hotspot2.0 <name>)# venue-type <type>
(Instant AP)(Hotspot2.0 <name>)# enable
```

OSU ESS can either be open or encrypted. When OSU ESS is using open encryption, create an SSID profile with the same name as provided in the hotspot profile and set the operation mode to open. When OSU ESS is encypted, create a hotspot profile with only **osen** enabled and attach it to an SSID that broadcasts OSEN capable network. In this case, choose the operation mode to WPA2-AES.

The following CLI commands configure Online Sign-Up SSID in Encryption mode (OSEN), create a separate hotspot profile to enable OSEN and attach it to the SSID that broadcasts OSEN capable network:

```
(Instant AP)(config)# hotspot hs-profile <name>
(Instant AP)(Hotspot2.0 <name>)# osen
```



Ensure that all parameters except OSEN are disabled in the separate hotspot profile created for OSEN.

The hotspot profile configuration parameters are described in the following table:

Table 222: *Hotspot Profile Configuration Parameters*

Parameter	Description	Range	Default
access-network-type <type>	Configures any of the following access network (802.11u network type) type: ▪ **private**—This network is accessible for authorized users only. For example, home networks or enterprise networks that require user authentication. The corresponding integer value for this network type is 0. ▪ **private-with-guest**—This network is accessible to guest users based on guest authentication methods. For example, enterprise networks that allow guest users with captive portal authentication. The corresponding integer value for this network type is 1. ▪ **chargeable-public**— This network provides access to the Internet based on payment. For example, a subscription-based Internet access in a coffee shop or a hotel offering chargeable in-room Internet access service. The corresponding integer value for this network type is 2. ▪ **free-public**—This network is accessible to all without any charges applied. For example, a hotspot in airport or other public places that provide Internet access with no additional cost. The corresponding integer value for this network type is 3. ▪ **personal-device**—This network is accessible for personal devices. For example, a laptop or camera configured with a printer for the purpose of printing. The corresponding integer value for this network type is 4. ▪ **emergency-services**—This network is limited to accessing emergency services only. The corresponding integer value for	private, private-with-guest,chargeable-public, free-public, personal-device, emergency-services, test, wildcard	chargeable-public

Table 222: *Hotspot Profile Configuration Parameters*

Parameter	Description	Range	Default
	this network type is 5. ■ **test**—This network is used for test purposes only. The corresponding integer value for this network type is 14. ■ **wildcard**—This network indicates a wildcard network. The corresponding integer value for this network type is 15.		
addtl-roam-cons-ois <addtl-roam-cons-ois>	Configures the number of additional roaming consortium OIs advertised by the Instant AP. This feature supports up to three additional OIs, which are defined using the roam-cons-oi-1, roam-cons-oi-2 and roam-cons-oi-3 parameters.	—	—
advertisement-profile	Associates an advertisement profile with the hotspot profile. You can associate any of the following advertisement profiles: ■ anqp-3gpp-profile ■ anqp-domain-name-profile ■ anqp-ip-addr--profile ■ anqp-nai-realm-profile ■ anqp-nwk-auth-profile ■ anqp-roam-cons-profile ■ anqp-venue-name-profile ■ h2qp-conn-cap-profile ■ h2qp-oper-class-profile ■ h2qp-osu-provider-profile ■ h2qp-oper-name-profile ■ h2qp-wan-metrics-profile	—	—
<profile-name>	Allows you to associate a specific advertisement profile to the hotspot profile.	—	—
asra	Indicates if any additional steps are required for network access.	—	—

Table 222: *Hotspot Profile Configuration Parameters*

Parameter	Description	Range	Default
comeback-mode	By default, ANQP information is obtained from a GAS Request and Response. If you enable the comeback-mode option, advertisement information is obtained using a GAS Request and Response. as well as a Comeback-Request and Comeback-Response. This option is disabled by default.	—	—
enable	Enables the hotspot profile.	—	—
gas-comeback-delay <delay>	Configures a GAS comeback delay interval after which the client can attempt to retrieve the query response using a Comeback Request Action frame.	100—2000 milliseconds	100
group-frame-block	Configures the DGAF Disabled Mode. This feature ensures that the Instant AP does not forward downstream group-addressed frames. It is disabled by default, allowing the Instant AP to forward downstream group-addressed frames.	—	—
hessid	Configures a homogenous ESS identifier.	MAC address in colon-separated hexadecimal format	_
internet	Allows the Instant AP to send an Information Element indicating that the network allows the Internet access. By default, a hotspot profile does not advertise network internet access.	—	—
no	Removes any existing configuration.	—	—
osen	Uses the OSEN information element to advertise and select an OSEN capable network. **NOTE:** You must create a separate hotspot profile only with OSEN enabled and attach it to the Online Sign-UP (OSU) SSID profile. Ensure that all the other parameters of the OSEN hotspot profile are disabled.	—	Disabled

Table 222: *Hotspot Profile Configuration Parameters*

Parameter	Description	Range	Default
osu-nai	Indicates the Network Access Identifier(NAI) that is used for OSU with the service provider configured in the OSU provider profile. When the OSU NAI is configured, the OSU ESS employs a link-layer encryption. For open OSU ESS, this parameter is not applicable.	—	—
osu-ssid	Configures the SSID that the wireless devices use for OSU with all the OSU providers.	—	—
p2p-cross-connect	Advertises support for P2P Cross Connections.	—	Disabled
p2p-dev-mgmt	Advertises support for P2P device management.	—	Disabled
pame-bi	Enables the PAME-BI bit, which is used by anInstant AP to indicate whether the Instant AP indicates that the Advertisement Server can return a query response that is independent of the BSSID used for the GAS Frame exchange.	—	—
qos-map-excp	Includes the DSCP exceptions in the QoS map set. You can configure a maximum of 21 sets of DSCP exception fields. It must be entered in Hexadecimal format. It is in the format, <value>-<up> separated by ',' where <value> can be 0-3F or FF, and user priority <up> can be 0-7).	—	—
qos-map-range	Configures the DSCP range value between 0 and 63 inclusive, or 255. It must be entered in Hexadecimal format. You must configure 8 sets each corresponding to a user priority. The format is <low>-<high> separated by a ',' where low and high are 0-3F and FF. For Example: 08-0F,00-07,FF-FF,10-1F,20-27,FF-FF,28-2F,30-3F	—	—
query-response-length-limit <len>	Configures the maximum length of the GAS query response. GAS enables advertisement services that allow the clients to query multiple 802.11 networks at once, while also allowing the client to learn more about a network's 802.11 infrastructure before associating.	1-6	1

Table 222: *Hotspot Profile Configuration Parameters*

Parameter	Description	Range	Default
	If a client transmits a GAS Query using a GAS Initial Request frame, the responding Instant AP will provide the query response (or information on how to receive the query response) in a GAS Initial Response frame.		
release-number	Indicates the release number of Hotspot.	1-2	1
roam-cons-len-1	Configures the length of the OI. The value of the **roam-cons-len-1**parameter is based upon the number of octets of the **roam-cons-oi-1** field.	**0**: Zero Octets in the OI (Null), **3**: OI length is 24-bit (3 Octets), **5**: OI length is 36-bit (5 Octets)	—
roam-cons-len-2	Length of the OI. The value of the **roam-cons-len-2**parameter is based upon the number of octets of the **roam-cons-oi-2** field.	**0**: Zero Octets in the OI (Null), **3**: OI length is 24-bit (3 Octets), **5**: OI length is 36-bit (5 Octets)	—
roam-cons-len-3	Length of the OI. The value of the **roam-cons-len-3**parameter is based upon the number of octets of the **roam-cons-oi-3** field.	**0**: Zero Octets in the OI (Null), **3**: OI length is 24-bit (3 Octets), **5**: OI length is 36-bit (5 Octets)	—
roam-cons-oi-1 **roam-cons-oi-2** **roam-cons-oi-3**	Configures the roaming consortium OI to assign to one of the service provider's top three roaming partners. This additional OI will only be sent to a client if the **addtl-roam-cons-<oisaddtl-roam-cons-ois>** parameter is set to 1 or higher. **NOTE:** The service provider's own roaming consortium OI is configured using the **hotspot anqp-roam-cons-profile** command.	—	—
venue-group <venue-group>	Configures one of the following venue groups to be advertised in the IEs from Instant APs associated with this hotspot profile. ▪ assembly ▪ business ▪ educational ▪ factory-and-industrial ▪ institutional	assembly, business, educational, factory-and-industrial, institutional, mercantile, outdoor, residential, storage, unspecified, utility-and-misc, vehicular	business

Table 222: *Hotspot Profile Configuration Parameters*

Parameter	Description	Range	Default
	▪ mercantile ▪ outdoor ▪ residential ▪ storage ▪ unspecified ▪ utility-and-misc ▪ vehicular **NOTE:** This parameter only defines the venue group advertised in the IEs from hotspot Instant APs. To define the venue group to be included in ANQP responses, use **anqp-venue-name-profile <profile-name>** command.		
venue-type <venue-type>	Specifies the venue type to be advertised in the IEs from Instant APs associated with this hotspot profile. The complete list of supported venue types is described in Creating a Hotspot Profile on page 531 This parameter only defines the venue type advertised in the IEs from hotspot Instant APs. To define the venue type to be included in ANQP responses, use the **hotspot anqp-venue-name-profile <profile-name>** command.	—	—

Associating an Advertisement Profile to a Hotspot Profile

The following CLI commands associate a hotspot profile with an advertisement profile:

```
(Instant AP)(config)# hotspot hs-profile <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-protocol <protocol>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile anqp-3gpp <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile anqp-domain-name <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile anqp-ip-addr-avail <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile anqp-nai-realm <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile anqp-nwk-auth <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile anqp-roam-cons <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile anqp-venue-name <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile h2qp-conn-cap <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile h2qp-oper-class <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile h2qp-oper-name <name>
(Instant AP)(Hotspot2.0 <name>)# advertisement-profile h2qp-osu-provider <name>
```

The configuration parameters for associating an advertisement profile with a hotspot profile are described in the following table:

Table 223: *Advertisement Profile Association Parameters*

Parameter	Description
advertisement-profile	Specify the advertisement profile to associate with this hotspot profile. For information on advertisement profiles, see Downloading Icon Files to Instant AP on page 528.
advertisement-protocol	Specify the advertisement protocol type; for example, specify the ANQP as **anqp**.

Creating a WLAN SSID and Associating Hotspot Profile

The following CLI commands create a WLAN SSID with Enterprise Security and WPA2 Encryption Settings:

```
(Instant AP)(config)# wlan ssid-profile <name>
(Instant AP)(SSID Profile <name>)# essid <ESSID-name>
(Instant AP)(SSID Profile <name>)# type {<Employee> | <Voice>| <Guest>}
(Instant AP)(SSID Profile <name>)# vlan <vlan-ID>
(Instant AP)(SSID Profile <name>)# set-vlan <attribute>{equals|not-equals|starts-
with|ends-with|contains} <operator> <VLAN-ID>| value-of}
(Instant AP)(SSID Profile <name>)# opmode {wpa2-aes|wpa-tkip,wpa2-aes}
(Instant AP)(SSID Profile <name>)# blacklist
(Instant AP)(SSID Profile <name>)# mac-authentication
(Instant AP)(SSID Profile <name>)# l2-auth-failthrough
(Instant AP)(SSID Profile <name>)# termination
(Instant AP)(SSID Profile <name>)# external-server
(Instant AP)(SSID Profile <name>)# auth-server <server-name>
(Instant AP)(SSID Profile <name>)# server-load-balancing
(Instant AP)(SSID Profile <name>)# radius-accounting
(Instant AP)(SSID Profile <name>)# radius-accounting-mode {user-authentication| user-
association}
(Instant AP)(SSID Profile <name>)# radius-interim-accounting-interval <minutes>
(Instant AP)(SSID Profile <name>)# radius-reauth-interval <minutes>
(Instant AP)(SSID Profile <name>)# set-role-by-ssid
```

Sample Configuration

Step 1: Creating ANQP and H2QP Advertisement Profiles

```
(Instant AP)# configure terminal
(Instant AP)(config)#  hotspot anqp-nai-realm-profile nr1
(Instant AP)(nai-realm "nr1")# nai-realm-name name1
(Instant AP)(nai-realm "nr1")# nai-realm-encoding utf8
(Instant AP)(nai-realm "nr1")# nai-realm-eap-method eap-sim
(Instant AP)(nai-realm "nr1")# nai-realm-auth-id-1 non-eap-inner-auth
(Instant AP)(nai-realm "nr1")# nai-realm-auth-value-1 mschapv2
(Instant AP)(nai-realm "nr1")# nai-home-realm
(Instant AP)(nai-realm "nr1")# exit

(Instant AP)(config)# hotspot anqp-venue-name-profile vn1
(Instant AP)(venue-name "vn1")# venue-group business
(Instant AP)(venue-name "vn1")# venue-type research-and-dev-facility
(Instant AP)(venue-name "vn1")# venue-lang-code eng
(Instant AP)(venue-name "vn1")# venue-name VenueName
(Instant AP)(venue-name "vn1")# exit

(Instant AP)(config)# hotspot anqp-nwk-auth-profile na1
(Instant AP)(network-auth "na1")# nwk-auth-type accept-term-and-cond
(Instant AP)(network-auth "na1")# url www.nwkauth.com
(Instant AP)(network-auth "na1")# exit
```

```
(Instant AP)(config)# hotspot anqp-roam-cons-profile rc1
(Instant AP)(roaming-consortium "rc1")# roam-cons-oi-len 3
(Instant AP)(roaming-consortium "rc1")# roam-cons-oi 888888
(Instant AP)(roaming-consortium "rc1")# exit

(Instant AP)(config)# hotspot anqp-3gpp-profile 3g
(Instant AP)(3gpp "3g")# 3gpp-plmn1 40486
(Instant AP)(3gpp "3g")# exit

(Instant AP)(config)# hotspot anqp-ip-addr-avail-profile ip1
(Instant AP)(IP-addr-avail "ip1")# no ipv4-addr-avail
(Instant AP)(IP-addr-avail "ip1")# ipv6-addr-avail
(Instant AP)(IP-addr-avail "ip1")# exit

(Instant AP)(config)# hotspot anqp-domain-name-profile dn1
(Instant AP)(domain-name "dn1")# domain-name DomainName
(Instant AP)(domain-name "dn1")# exit

(Instant AP)(config)# hotspot h2qp-oper-name-profile on1
(Instant AP)(operator-friendly-name"on1")# op-lang-code eng
(Instant AP)(operator-friendly-name"on1")# op-fr-name OperatorFriendlyName
(Instant AP)(operator-friendly-name"on1")# exit

(Instant AP)(config) # hotspot h2qp-conn-cap-profile cc1
(Instant AP)(connection-capabilities "cc1")# esp-port
(Instant AP)(connection-capabilities "cc1")# icmp
(Instant AP)(connection-capabilities "cc1")# tcp-ftp
(Instant AP)(connection-capabilities "cc1")# tcp-http
(Instant AP)(connection-capabilities "cc1")# tcp-pptp-vpn
(Instant AP)(connection-capabilities "cc1")# tcp-ssh
(Instant AP)(connection-capabilities "cc1")# tcp-tls-vpn
(Instant AP)(connection-capabilities "cc1")# tcp-voip
(Instant AP)(connection-capabilities "cc1")# udp-ike2
(Instant AP)(connection-capabilities "cc1")# udp-ipsec-vpn
(Instant AP)(connection-capabilities "cc1")# udp-voip
(Instant AP)(connection-capabilities "cc1")# enable
(Instant AP)(connection-capabilities "cc1")# exit

(Instant AP)(config) # hotspot h2qp-oper-class-profile oc1
(Instant AP)(operator-class "oc1")# op-class <class-ID>
(Instant AP)(operator-class "oc1")# enable
(Instant AP)(operator-class "oc1")# exit

(Instant AP) (config) # hotspot h2qp-osu-provider-profile osu1
(Instant AP) (osu-provider "osu1") # frnd-name-count 2
(Instant AP) (osu-provider "osu1") # frnd-name1-lang-code "eng"
(Instant AP) (osu-provider "osu1") # frnd-name1 "SP Red Test Only"
(Instant AP) (osu-provider "osu1") # frnd-name1-hex
(Instant AP) (osu-provider "osu1") # frnd-name2-lang-code "kor"
(Instant AP) (osu-provider "osu1") # frnd-name2 ""
(Instant AP) (osu-provider "osu1") # frnd-name2-hex
535020ebb9a8eab09520ed858cec8aa4ed8ab820eca084ec9aa9
(Instant AP) (osu-provider "osu1") # iconfile-count 2
(Instant AP) (osu-provider "osu1") # icon1-width 128
(Instant AP) (osu-provider "osu1") # icon1-height 61
(Instant AP) (osu-provider "osu1") # icon1-lang-code zxx
(Instant AP) (osu-provider "osu1") # icon1-type image/png
(Instant AP) (osu-provider "osu1") # icon1-file 1 "icon_red_zxx.png"
(Instant AP) (osu-provider "osu1") # icon2-width 160
(Instant AP) (osu-provider "osu1") # icon2-height 76
(Instant AP) (osu-provider "osu1") # icon2-lang-code eng
(Instant AP) (osu-provider "osu1") # icon2-type image/png
(Instant AP) (osu-provider "osu1") # icon2-file 2 "icon_red_eng.png"
```

```
(Instant AP) (osu-provider "osu1") # srvcdesc-count 2
(Instant AP) (osu-provider "osu1") # srvc-desc1-lang-code eng
(Instant AP) (osu-provider "osu1") # srvc-desc1 "Free service for test purpose"
(Instant AP) (osu-provider "osu1") # srvc-desc1-hex
(Instant AP) (osu-provider "osu1") # srvc-desc2-lang-code kor
(Instant AP) (osu-provider "osu1") # srvc-desc2 ""
(Instant AP) (osu-provider "osu1") # srvc-desc2-hex
ed858cec8aa4ed8ab820ebaaa9eca081ec9cbceba19c20ebacb4eba38c20ec849cebb984ec8aa4
(Instant AP) (osu-provider "osu1") # osu-server-uri https://osu-server.r2-testbed-
aru.wi-fi.org:443/guest/HotSpot2OnlineSignUp.php
(Instant AP) (osu-provider "osu1") # osu-method SOAP-XML
(Instant AP)(WAN-metrics "osu1")# exit

(Instant AP)(config)# hotspot h2qp-wan-metrics-profile wm1
(Instant AP)(WAN-metrics "wm1")# at-capacity
(Instant AP)(WAN-metrics "wm1")# downlink-load <load>
(Instant AP)(WAN-metrics "wm1")# downlink-speed <speed>
(Instant AP)(WAN-metrics "wm1")# load-duration <duration>
(Instant AP)(WAN-metrics "wm1")# symm-link
(Instant AP)(WAN-metrics "wm1")# uplink-load <load>
(Instant AP)(WAN-metrics "wm1")# uplink-speed <speed>
(Instant AP)(WAN-metrics "wm1")# wan-metrics-link-status <status>
(Instant AP)(WAN-metrics "wm1")# exit
```

Step 2: Creating a hotspot profile

```
(Instant AP)# configure terminal
(Instant AP)(config)# hotspot hs-profile hs1
(Instant AP)(Hotspot2.0 "hs1")# enable
(Instant AP)(Hotspot2.0 "hs1")# comeback-mode
(Instant AP)(Hotspot2.0 "hs1")# gas-comeback-delay 100
(Instant AP)(Hotspot2.0 "hs1")# no asra
(Instant AP)(Hotspot2.0 "hs1")# no internet
(Instant AP)(Hotspot2.0 "hs1")# osu-ssid OSU-SSID
(Instant AP)(Hotspot2.0 "hs1")# qos-map-excp 35-2,16-6
(Instant AP)(Hotspot2.0 "hs1")# qos-map-range 08-0F,00-07,FF-FF,10-1F,20-27,FF-FF,28-
2F,30-3F
(Instant AP)(Hotspot2.0 "hs1")# query-response-length-limit 2
(Instant AP)(Hotspot2.0 "hs1")# access-network-type chargeable-public
(Instant AP)(Hotspot2.0 "hs1")# roam-cons-len-1 3
(Instant AP)(Hotspot2.0 "hs1")# roam-cons-oi-1 123456
(Instant AP)(Hotspot2.0 "hs1")# roam-cons-len-2 3
(Instant AP)(Hotspot2.0 "hs1")# roam-cons-oi-2 223355
(Instant AP)(Hotspot2.0 "hs1")# addtl-roam-cons-ois 0
(Instant AP)(Hotspot2.0 "hs1")# venue-group business
(Instant AP)(Hotspot2.0 "hs1")# venue-type research-and-dev-facility
(Instant AP)(Hotspot2.0 "hs1")# pame-bi
(Instant AP)(Hotspot2.0 "hs1")# group-frame-block
(Instant AP)(Hotspot2.0 "hs1")# p2p-dev-mgmt
(Instant AP)(Hotspot2.0 "hs1")# p2p-cross-connect
```

Step 3 (Optional): Creating a hotspot profile for OSEN

```
(Instant AP) (config) # hotspot hs-profile hs2
(Instant AP) (Hotspot2.0 "hs2") # osen
(Instant AP) (Hotspot2.0 "hs2") # no enable
```

Step 4: Associating advertisement profiles with the hotspot profile

```
(Instant AP)# configure terminal
(Instant AP)(config)# hotspot hs-profile hs1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-nai-realm-profile nr1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-venue-name-profile vn1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-nwk-auth-profile na1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-roam-cons-profile rc1
```

```
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-3gpp-profile 3g1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-ip-addr-avail-profile ip1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-domain-name-profile dn1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile h2qp-oper-name-profile on1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile h2qp-wan-metrics-profile wm1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile h2qp-conn-cap-profile cc1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile h2qp-oper-class-profile oc1
(Instant AP)(Hotspot2.0 "hs1")# advertisement-profile h2qp-osu-provider-profile osu1
```

Step 5: Associating the hotspot profile with production WLAN SSID:

```
(Instant AP)# configure terminal
(Instant AP)# wlan ssid-profile ssidProfile1
(Instant AP)(SSID Profile "ssidProfile1")# essid hsProf
(Instant AP)(SSID Profile "ssidProfile1")# type employee
(Instant AP)(SSID Profile "ssidProfile1")# vlan 200
(Instant AP)(SSID Profile "ssidProfile1")# opmode wpa2-aes
(Instant AP)(SSID Profile "ssidProfile1")# auth-server RADIUS1
(Instant AP)(SSID Profile "ssidProfile1")# hotspot-profile hs1
```

Step 6 (Only if Step 3 is configured): Associating OSEN hotspot profile with an SSID that broadcasts OSEN capable network:

```
(Instant AP)# configure terminal
(Instant AP)# wlan ssid-profile OSU-SSID
(Instant AP)(SSID Profile "OSU-SSID")# hotspot-profile hs2
```



OSU ESS can either be open or encrypted. When OSU ESS is using open encryption, create an SSID profile with the same name as provided in the hotspot profile and set the operation mode to open. When OSU ESS is encypted, create a hotspot profile with only **osen** enabled and attach it to an SSID that broadcasts OSEN capable network. In this case, choose the operation mode to WPA2-AES.

Chapter 36
Mobility Access Switch Integration

This chapter provides the following information:

- Mobility Access Switch Overview on page 542
- Configuring Instant APs for Mobility Access Switch Integration on page 543

Mobility Access Switch Overview

The Aruba Mobility Access Switch enables a secure, role-based network access for wired users and devices, independent of their location or application. Installed in wiring closets, the Mobility Access Switch delivers up to 384 wire-speed Gigabit Ethernet switch ports and operates as a wired access point when deployed with an Aruba Mobility Controller.

As a wired access point, users and their devices are authenticated and assigned a unique role by the Mobility Controller. These roles are applied irrespective of whether the user is a Wi-Fi client, or is connected to a port on the Mobility Access Switch. The use of Mobility Access Switch allows an enterprise workforce to have a consistent and secure access to network resources based on the type of users, client devices, and connection method used.

Instant supports S3500 and S2500 Mobility Access Switch models.

For more information on Mobility Access Switches, refer to *ArubaOS User Guide*.

Mobility Access Switch Integration with an Instant AP

You can integrate an Instant AP with a Mobility Access Switch by connecting it directly to the switch port. The following integration features can be applied while integrating Mobility Access Switch with an Instant AP:

- **Rogue AP containment**—When a rogue Instant AP is detected by an Instant AP, it sends the MAC Address of the rogue Instant AP to the Mobility Access Switch. The Mobility Access Switch blacklists the MAC address of the rogue Instant AP and turns off the PoE on the port.
- **PoE prioritization**—When an Instant AP is connected directly into the switch port, the switch increases the PoE priority of the port. This is done only if the PoE priority is set by default in the Mobility Access Switch.



The PoE Prioritization and Rogue AP Containment features are available for Instant 7.2 release on Aruba Mobility Access Switches.

- **GVRP Integration**—Configuring GVRP enables the switch to dynamically register or unregister VLAN information received from a GVRP applicant such as an Instant AP. GVRP also enables the switch to propagate the registered VLAN information to the neighboring switches in the network.



The associated static VLANs used in wired and wireless profiles are propagated to the upstream Mobility Access Switch using GVRP messages.

For information on steps to integrate Mobility Access Switch with an Instant AP, see Configuring Instant APs for Mobility Access Switch Integration on page 543.

Configuring Instant APs for Mobility Access Switch Integration

When an Instant AP is integrated with a Mobility Access Switch, the LLDP is enabled. Using this protocol, the Instant APs instruct the switch to turn off the ports where rogue Instant APs are connected, perform actions such as increasing the PoE priority, and configure the VLANs on the ports to which the Instant APs are connected.

The following procedure describes how to enable Mobility Access Switch integration either by using the WebUI.

Table 224: *Configuring Instant AP for Mobility Access Switch Integration*

New WebUI	Old WebUI
1. Navigate to **Configuration** > **System** > **General**. 2. Enable the **MAS integration** toggle switch. 3. Click **Save**.	1. Navigate to **System** > **General**. 2. Select **Enabled** from the **MAS integration** drop-down list. 3. Click **OK**.

The following CLI command enables the Mobility Access Switch integration:

```
(Instant AP)(config)# mas-integration
```

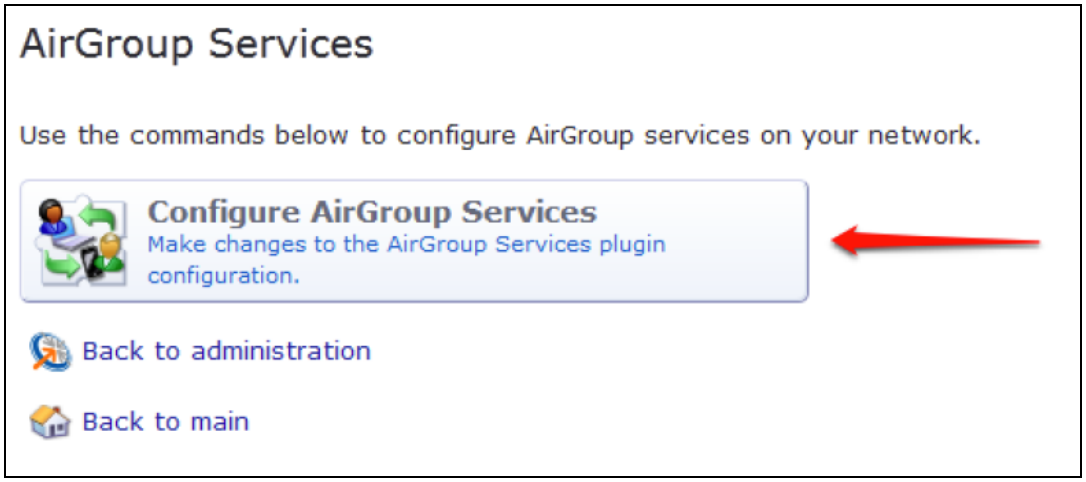
This chapter consists of the following topics:

- Configuring ClearPass Guest on page 544
- Verifying ClearPass Guest Setup on page 548
- Troubleshooting on page 548

Configuring ClearPass Guest

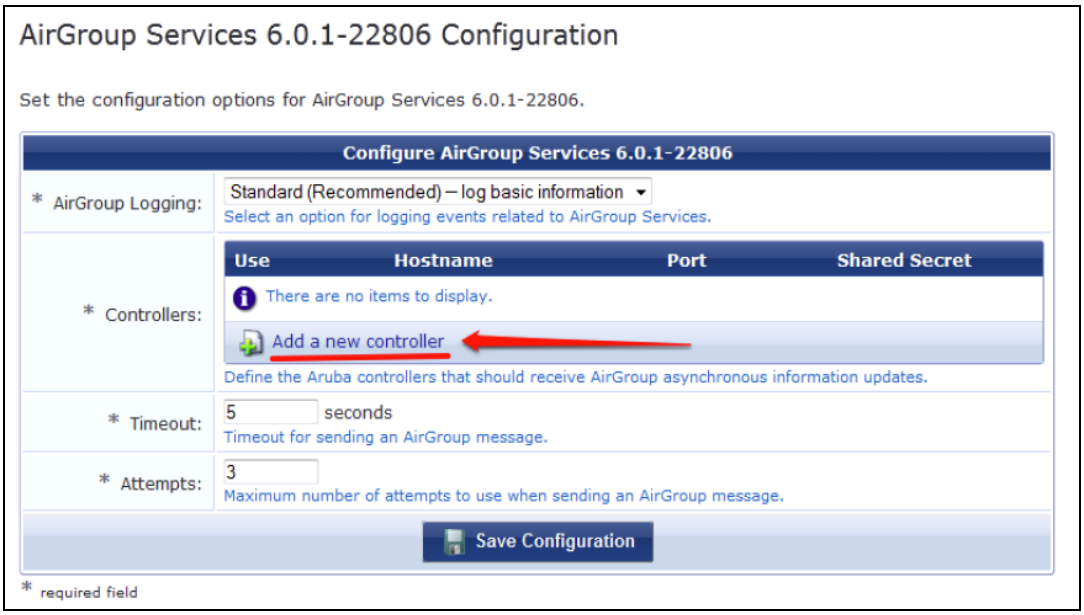
1. From the ClearPass Guest WebUI, navigate to **Administration > AirGroup Services**.
2. Click **Configure AirGroup Services**.

Figure 34 *Configure AirGroup Services*



3. Click **Add a new controller**.

Figure 35 *Add a New Controller for AirGroup Services*

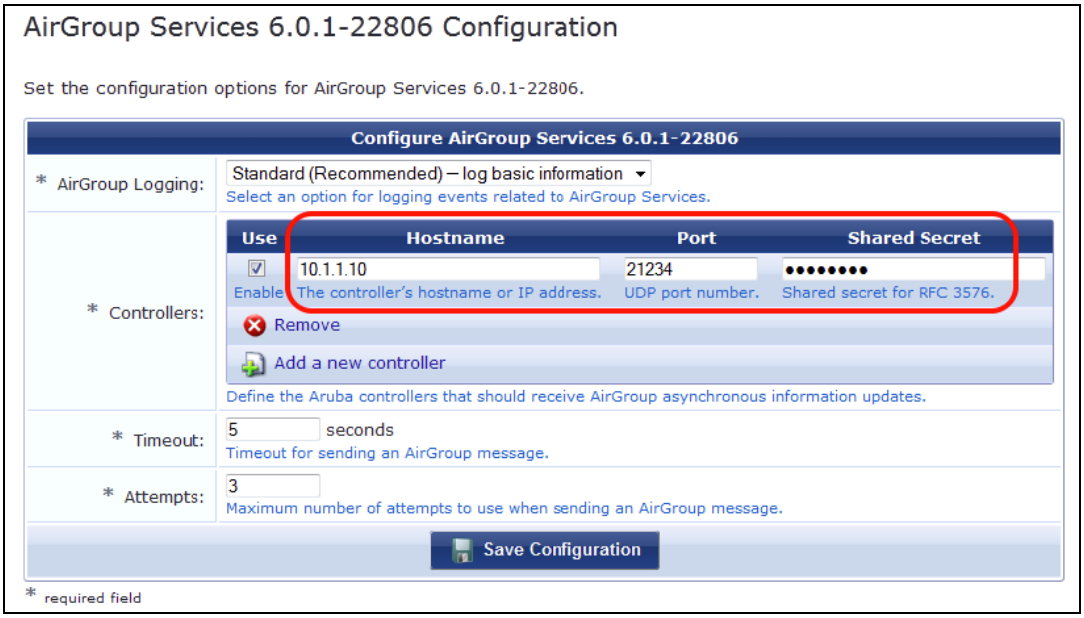


4. Update the parameters with appropriate values.

NOTE

Ensure that the port configured matches the CoA port (RFC 3576) set on the Instant AP configuration.

Figure 36 *Configure AirGroup Services: Controller Settings*



5. Click **Save Configuration**.

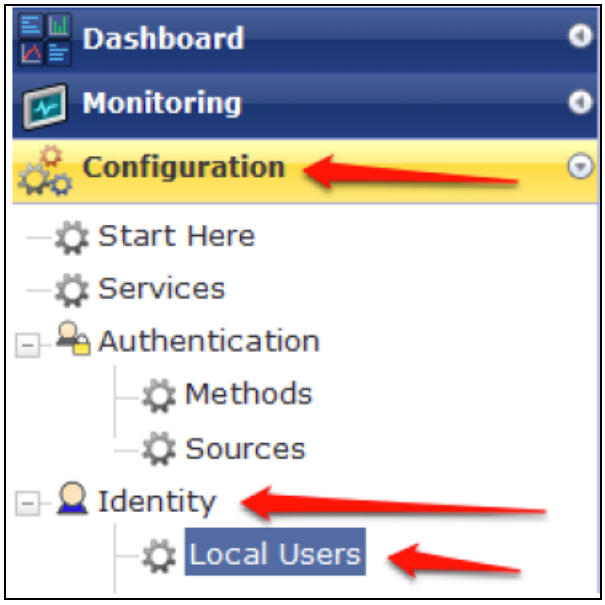
In order to demonstrate AirGroup, either an AirGroup Administrator or an AirGroup Operator account must be created.

Creating AirGroup Administrator and Operator Account

To create a AirGroup administrator and AirGroup operator account using the ClearPass Policy Manager UI:

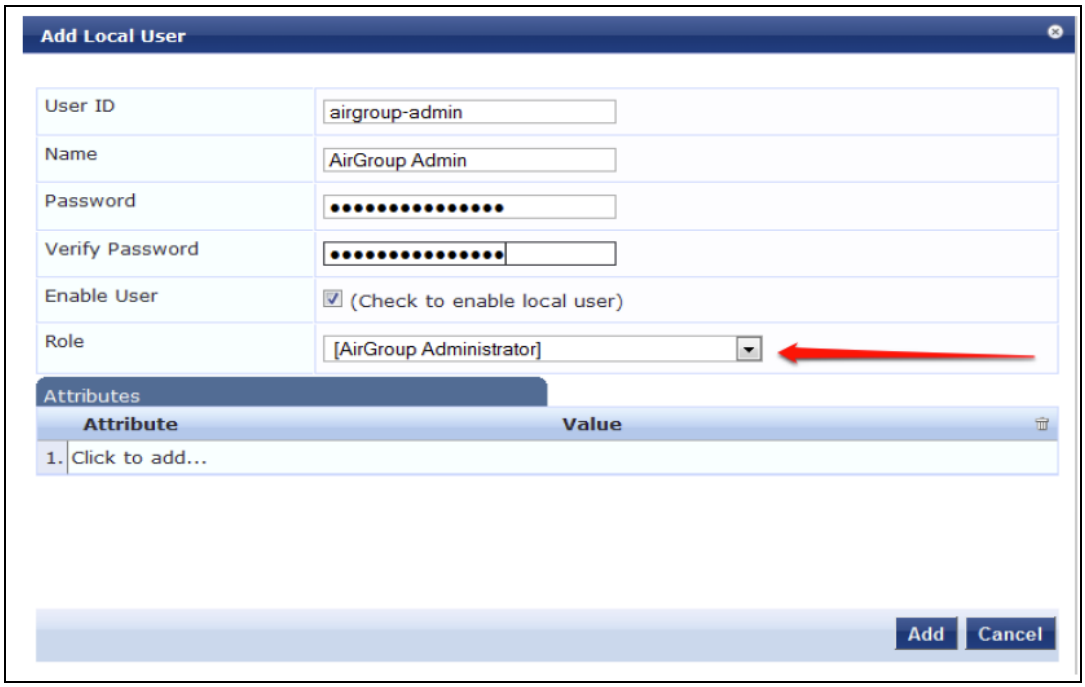
1. Navigate to the ClearPass Policy Manager WebUI, and navigate to **Configuration > Identity > Local Users**.

   Figure 37 *Configuration > Identity > Local Users Selection*



2. Click **Add User**.
3. Create an **AirGroup Administrator** by entering the required values.

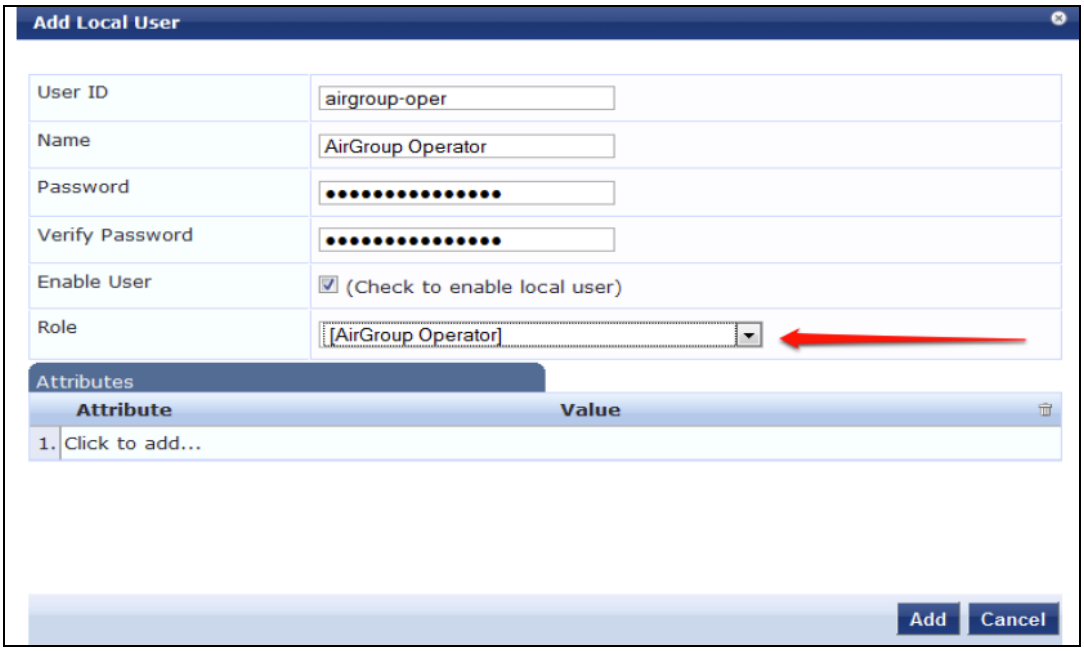
   Figure 38 *Create an AirGroup Administrator*



4. Click **Add**.

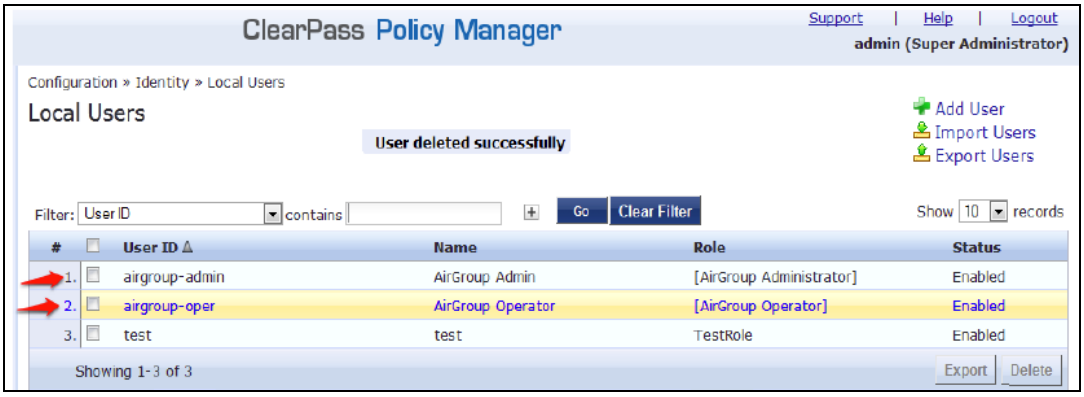
5. Now click **Add User** to create an **AirGroup Operator**.

Figure 39 *Create an AirGroup Operator*



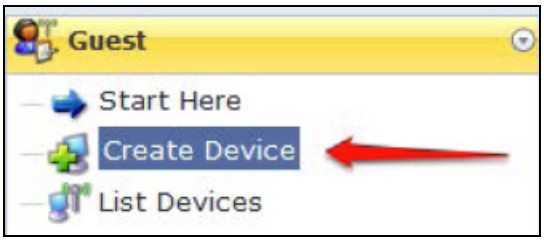
6. Click **Add** to save the user with an **AirGroup Operator** role. The **AirGroup Administrator** and **AirGroup Operator IDs** will be displayed in the **Local Users** UI screen.

Figure 40 *Local Users UI Screen*



7. Navigate to the ClearPass Guest UI and click **Logout**. The **ClearPass Guest Login** page is displayed. Use the AirGroup admin credentials to log in.
8. After logging in, click **Create Device**.

Figure 41 *Create a Device*



The **Register Shared Device** page is displayed.

Figure 42 *ClearPass Guest- Register Shared Device*



For this test, add your AppleTV device name and MAC address but leave all other boxes empty.

9. Click **Register Shared Device**.

Verifying ClearPass Guest Setup

1. Disconnect your AppleTV and OSX Mountain Lion or iOS 6 devices if they were previously connected to the wireless network. Remove their entries from the controller's user table using these commands:
   - Find the MAC address—**show user table**
   - Delete the address from the table—**aaa user delete mac 00:aa:22:bb:33:cc**
2. Reconnect both devices. To limit access to the AppleTV, access the ClearPass Guest UI using either the AirGroup admin or the AirGroup operator credentials. Next, navigate to **List Devices > Test Apple TV > Edit**. Add a username that is not used to log in to the Apple devices in the **Shared With** box.
3. Disconnect and remove the OSX Mountain Lion or iOS 6 device from the controller's user table. Reconnect the device by not using the username that you added to the **Shared With** box. The AppleTV should not be available to this device.
4. Disconnect the OSX Mountain Lion or iOS 6 device and delete it from the controller's user table. Reconnect using the username that was added to the **Shared With** box. The OSX Mountain Lion or iOS 6 device should once again have access to the AppleTV.

Troubleshooting

Table 225: *Troubleshooting*

Problem	Solution
Limiting devices has no effect.	Ensure IPv6 is disabled.
Apple Macintosh running Mountain Lion can use AirPlay but iOS devices cannot.	Ensure IPv6 is disabled.

Appendix A
Glossary of Terms

The following table provides a brief description of the terminology used in this guide.

3DES

Triple Data Encryption Standard. 3DES is a symmetric-key block cipher that applies the DES cipher algorithm three times to each data block.

3G

Third Generation of Wireless Mobile Telecommunications Technology. See W-CDMA.

3GPP

Third Generation Partnership Project. 3GPP is a collaborative project aimed at developing globally acceptable specifications for third generation mobile systems.

4G

Fourth Generation of Wireless Mobile Telecommunications Technology. See LTE.

802.11

802.11 is an evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and Carrier Sense Multiple Access with collision avoidance (CSMA/CA) for path sharing.

802.11 bSec

802.11 bSec is an alternative to 802.11i. The difference between bSec and standard 802.11i is that bSec implements Suite B algorithms wherever possible. Notably, Advanced Encryption Standard-Counter with CBC-MAC is replaced by Advanced Encryption Standard - Galois/Counter Mode, and the Key Derivation Function (KDF) of 802.11i is upgraded to support SHA-256 and SHA-384.

802.11a

802.11a provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5 GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.

802.11ac

802.11ac is a wireless networking standard in the 802.11 family that provides high-throughput WLANs on the 5 GHz band.

802.11b

802.11b is a WLAN standard often called Wi-Fi and is backward compatible with 802.11. Instead of the Phase-Shift Keying (PSK) modulation method used in 802.11 standards, 802.11b uses Complementary Code Keying (CCK) that allows higher data speeds and makes it less susceptible to multipath-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.

802.11d

802.11d is a wireless network communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate. Configuration can be fine-tuned at the Media Access Control (MAC) layer level to comply with the rules of the country or district in which the network is to be used. Rules are subject to variation and include allowed frequencies, allowed power levels, and allowed signal bandwidth. 802.11d facilitates global roaming.

802.11e

802.11e is an enhancement to the 802.11a and 802.11b specifications that enhances the 802.11 Media Access Control layer with a coordinated Time Division Multiple Access (TDMA) construct. It adds error-correcting mechanisms for delay-sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability between business, home, and public environments such as airports and hotels, and offers all subscribers high-speed Internet access with full-motion video, high-fidelity audio, and VoIP.

802.11g

802.11g offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b standard. 802.11g employs Orthogonal Frequency Division Multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speed of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.

802.11h

802.11h is intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with military Radar systems and medical devices. Dynamic Frequency Selection (DFS) detects the presence of other devices on a channel and automatically switches the network to another channel if and when such signals are detected. Transmit Power Control (TPC) reduces the radio frequency (RF) output power of each network transmitter to a level that minimizes the risk of interference.

802.11i

802.11i provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards. It requires new encryption key protocols, known as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

802.11j

802.11j is a proposed addition to the 802.11 family of standards that incorporates Japanese regulatory extensions to 802.11a; the main intent is to add channels in the radio frequency (RF) band of 4.9 GHz to 5.0 GHz.

802.11k

802.11k is an IEEE standard that enables APs and client devices to discover the best available radio resources for seamless BSS transition in a WLAN.

802.11m

802.11m is an Initiative to perform editorial maintenance, corrections, improvements, clarifications, and interpretations relevant to documentation for 802.11 family specifications.

802.11n

802.11n is a wireless networking standard to improve network throughput over the two previous standards, 802.11a and 802.11g. With 802.11n, there will be a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz.

802.11r

802.11r is an IEEE standard for enabling seamless BSS transitions in a WLAN. 802.11r standard is also referred to as Fast BSS transition.

802.11u

802.11u is an amendment to the IEEE 802.11 WLAN standards for connection to external networks using common wireless devices such as smartphones and tablet PCs. The 802.11u protocol provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users to roam between partner networks without additional authentication. An 802.11u-capable device supports the Passpoint technology from the Wi-Fi Alliance Hotspot 2.0 R2 Specification that simplifies and automates access to public Wi-Fi.

802.11v

802.11v is an IEEE standard that allows client devices to exchange information about the network topology and RF environment. This information is used for assigning best available radio resources for the client devices to provide seamless connectivity.

802.1Q

802.1Q is an IEEE standard that enables the use of VLANs on an Ethernet network. 802.1Q supports VLAN tagging.

802.1X

802.1X is an IEEE standard for port-based network access control designed to enhance 802.11 WLAN security. 802.1X provides an authentication framework that allows a user to be authenticated by a central authority.

802.3af

802.3af is an IEEE standard for Power over Ethernet (PoE) version that supplies up to 15.4W of DC power. See PoE.

802.3at

802.3at is an IEEE standard for PoE version that supplies up to 25.5W of DC power. See PoE+.

A-MPDU

Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.

A-MSDU

Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.

AAA

Authentication, Authorization, and Accounting. AAA is a security framework to authenticate users, authorize the type of access based on user credentials, and record authentication events and information about the network access and network resource consumption.

ABR

Area Border Router. ABR is used for establishing connection between the backbone networks and the Open Shortest Path First (OSPF) areas. ABR is located near the border of one or more OSPF areas.

AC

Access Category. As per the IEEE 802.11e standards, AC refers to various levels of traffic prioritization in Enhanced Distributed Channel Access (EDCA) operation mode. The WLAN applications prioritize traffic based on the Background, Best Effort, Video, and Voice access categories. AC can also refer to Alternating Current, a form of electric energy that flows when the appliances are plugged to a wall socket.

ACC

Advanced Cellular Coexistence. The ACC feature in APs enable WLANs to perform at peak efficiency by minimizing interference from 3G/4G/LTE networks, distributed antenna systems, and commercial small cell/femtocell equipment.

Access-Accept

Response from the RADIUS server indicating successful authentication and containing authorization information.

Access-Reject

Response from RADIUS server indicating that a user is not authorized.

Access-Request

RADIUS packet sent to a RADIUS server requesting authorization.

Accounting-Request

RADIUS packet type sent to a RADIUS server containing accounting summary information.

Accounting-Response

RADIUS packet sent by the RADIUS server to acknowledge receipt of an Accounting-Request.

ACE

Access Control Entry. ACE is an element in an ACL that includes access control information.

ACI

Adjacent Channel Interference. ACI refers to interference or interruptions detected on a broadcasting channel, caused by too much power on an adjacent channel in the spectrum.

ACL

Access Control List. ACL is a common way of restricting certain types of traffic on a physical port.

Active Directory

Microsoft Active Directory. The directory server that stores information about a variety of things, such as organizations, sites, systems, users, shares, and other network objects or components. It also provides authentication and authorization mechanisms, and a framework within which related services can be deployed.

ActiveSync

Mobile data synchronization app developed by Microsoft that allows a mobile device to be synchronized with either a desktop or a server running compatible software products.

ad hoc network

An ad hoc network is a network composed of individual devices communicating with each other directly. Many ad hoc networks are Local Area Networks (LANs) where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point.

ADO

Active X Data Objects is a part of Microsoft Data Access Components (MDACs) that enables client applications to access data sources through an (Object Linking and Embedding Database) OLE DB provider. ADO supports key features for building client-server and Web-based applications.

ADP

Aruba Discovery Protocol. ADP is an Aruba proprietary Layer 2 protocol. It is used by the APs to obtain the IP address of the TFTP server from which it downloads the AP boot image.

AES

Advanced Encryption Standard. AES is an encryption standard used for encrypting and protecting electronic data. The AES encrypts and decrypts data in blocks of 128 bits (16 bytes), and can use keys of 128 bits, 192 bits, and 256 bits.

AIFSN

Arbitrary Inter-frame Space Number. AIFSN is set by the AP in beacon frames and probe responses. AIFS is a method of prioritizing a particular category of traffic over the other, for example prioritizing voice or video messages over email.

AirGroup

The application that allows the end users to register their personal mobile devices on a local network and define a group of friends or associates who are allowed to share them. AirGroup is primarily designed for colleges and other institutions. AirGroup uses zero configuration networking to allow Apple mobile devices, such as the AirPrint wireless printer service and the AirPlay mirroring service, to communicate over a complex access network topology.

AirWave Management Client

AirWave Management Client is a Windows software utility that enables client devices (such as a laptop) to act as passive RF sensors and augments the AirWave RAPIDS module.

ALE

Analytics and Location Engine. ALE gives visibility into everything the wireless network knows. This enables customers and partners to gain a wealth of information about the people on their premises. This can be very important for many different verticals and use cases. ALE includes a location engine that calculates associated and unassociated device location periodically using context streams, including RSSI readings, from WLAN controllers or Instant clusters.

ALG

Application Layer Gateway. ALG is a security component that manages application layer protocols such as SIP, FTP and so on.

AM

Air Monitor. AM is a mode of operation supported on wireless APs. When an AP operates in the Air Monitor mode, it enhances the wireless networks by collecting statistics, monitoring traffic, detecting intrusions, enforcing security policies, balancing wireless traffic load, self-healing coverage gaps, and more. However, clients cannot connect to APs operating in the AM mode.

AMON

Advanced Monitoring. AMON is used in Aruba WLAN deployments for improved network management, monitoring and diagnostic capabilities.

AMP

AirWave Management Platform. AMP is a network management system for configuring, monitoring, and upgrading wired and wireless devices on your network.

ANQP

Access Network Query Protocol. ANQP is a query and a response protocol for Wi-Fi hotspot services. ANQP includes information Elements (IEs) that can be sent from the AP to the client to identify the AP network and service provider. The IEs typically include information about the domain name of the AP operator, the IP addresses available at the AP, and information about potential roaming partners accessible through the AP. If the client responds with a request for a specific IE, the AP will send a Generic Advertisement Service (GAS) response frame with the configured ANQP IE information.

ANSI

American National Standards Institute. It refers to the ANSI compliance standards for products, systems, services, and processes.

API

Application Programming Interface. Refers to a set of functions, procedures, protocols, and tools that enable users to build application software.

app

Short form for application. It generally refers to the application that is downloaded and used on mobile devices.

ARM

Adaptive Radio Management. ARM dynamically monitors and adjusts the network to ensure that all users are allowed ready access. It enables full utilization of the available spectrum to support maximum number of users by intelligently choosing the best RF channel and transmit power for APs in their current RF environment.

ARP

Address Resolution Protocol. ARP is used for mapping IP network address to the hardware MAC address of a device.

Aruba Activate

Aruba Activate is a cloud-based service that helps provision your Aruba devices and maintain your inventory. Activate automates the provisioning process, allowing a single IT technician to easily and rapidly deploy devices throughout a distributed enterprise network.

ASCII

American Standard Code for Information Interchange. An ASCII code is a numerical representation of a character or an action.

B-RAS

Broadband Remote Access Server. A B-RAS is a server that facilitates and converges traffic from multiple Internet traffic resources such as cable, DSL, Ethernet, or Broadband wireless.

band

Band refers to a specified range of frequencies of electromagnetic radiation.

BGP

Border Gateway Protocol. BGP is a routing protocol for exchanging data and information between different host gateways or autonomous systems on the Internet.

BLE

Bluetooth Low Energy. The BLE functionality is offered by Bluetooth® to enable devices to run for long durations with low power consumption.

BMC

Beacon Management Console. BMC manages and monitors beacons from the BLE devices. The BLE devices are used for location tracking and proximity detection.

BPDU

Bridge Protocol Data Unit. A BPDU is a data message transmitted across a local area network to detect loops in network topologies.

BRE

Basic Regular Expression. The BRE syntax standards designed by the IEEE provides extension to the traditional Simple Regular Expressions syntax and allows consistency between utility programs such as grep, sed, and awk.

BSS

Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists of an AP and all its associated clients.

BSSID

Basic Service Set Identifier. The BSSID identifies a particular BSS within an area. In infrastructure BSS networks, the BSSID is the MAC address of the AP. In independent BSS or ad hoc networks, the BSSID is generated randomly.

BYOD

Bring Your Own Device. BYOD refers to the use of personal mobile devices within an enterprise network infrastructure.

CA

Certificate Authority or Certification Authority. Entity in a public key infrastructure system that issues certificates to clients. A certificate signing request received by the CA is converted into a certificate when the CA adds a signature generated with a private key. See digital certificate.

CAC

Call Admission Control. CAC regulates traffic volume in voice communications. CAC can also be used to ensure or maintain a certain level of audio quality in voice communications networks.

CALEA

Communications Assistance for Law Enforcement Act. To comply with the CALEA specifications and to allow lawful interception of Internet traffic by the law enforcement and intelligence agencies, the telecommunications carriers and manufacturers of telecommunications equipment are required to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

Campus AP

Campus APs are used in private networks where APs connect over private links (LAN, WLAN, WAN or MPLS) and terminate directly on controllers. Campus APs are deployed as part of the indoor campus solution in enterprise office buildings, warehouses, hospitals, universities, and so on.

captive portal

A captive portal is a web page that allows the users to authenticate and sign in before connecting to a public-access network. Captive portals are typically used by business centers, airports, hotel lobbies, coffee shops, and other venues that offer free Wi-Fi hotspots for the guest users.

CCA

Clear Channel Assessment. In wireless networks, the CCA method detects if a channel is occupied or clear, and determines if the channel is available for data transmission.

CDP

Cisco Discovery Protocol. CDP is a proprietary Data Link Layer protocol developed by Cisco Systems. CDP runs on Cisco devices and enables networking applications to learn about the neighboring devices directly connected to the network.

CDR

Call Detail Record. A CDR contains the details of a telephone or VoIP call, such as the origin and destination addresses of the call, the start time and end time of the call, any toll charges that were added through the network or charges for operator services, and so on.

CEF

Common Event Format. The CEF is a standard for the interoperability of event or log-generating devices and applications. The standard syntax for CEF includes a prefix and a variable extension formatted as key-value pairs.

CGI

Common Gateway Interface. CGI is a standard protocol for exchanging data between the web servers and executable programs running on a server to dynamically process web pages.

CHAP

Challenge Handshake Authentication Protocol. CHAP is an authentication scheme used by PPP servers to validate the identity of remote clients.

CIDR

Classless Inter-Domain Routing. CIDR is an IP standard for creating and allocating unique identifiers for networks and devices. The CIDR IP addressing scheme is used as a replacement for the older IP addressing scheme based on classes A, B, and C. With CIDR, a single IP address can be used to designate many unique IP addresses. A CIDR IP address ends with a slash followed by the IP network prefix, for example, 192.0.2.0/24.

ClearPass

ClearPass is an access management system for creating and enforcing policies across a network to all devices and applications. The ClearPass integrated platform includes applications such as Policy Manager, Guest, Onboard, OnGuard, Insight, Profile, QuickConnect, and so on.

ClearPass Guest

ClearPass Guest is a configurable ClearPass application for secure visitor network access management.

ClearPass Policy Manager

ClearPass Policy Manager is a baseline platform for policy management, AAA, profiling, network access control, and reporting. With ClearPass Policy Manager, the network administrators can configure and manage secure network access that accommodates requirements across multiple locations and multivendor networks, regardless of device ownership and connection method.

CLI

Command-Line Interface. A console interface with a command line shell that allows users to execute text input as commands and convert these commands to appropriate functions.

CN

Common Name. CN is the primary name used to identify a certificate.

CNA

Captive Network Assistant. CNA is a popup page shown when joining a network that has a captive portal.

CoA

Change of Authorization. The RADIUS CoA is used in the AAA service framework to allow dynamic modification of the authenticated, authorized, and active subscriber sessions.

CoS

Class of Service. CoS is used in data and voice protocols for classifying packets into different types of traffic (voice, video, or data) and setting a service priority. For example, voice traffic can be assigned a higher priority over email or HTTP traffic.

CPE

Customer Premises Equipment. It refers to any terminal or equipment located at the customer premises.

CPsec

Control Plane Security. CPsec is a secure form of communication between a controller and APs to protect the control plane communications. This is performed by means of using public-key self-signed certificates created by each master controller.

CPU

Central Processing Unit. A CPU is an electronic circuitry in a computer for processing instructions.

CRC

Cyclic Redundancy Check. CRC is a data verification method for detecting errors in digital data during transmission, storage, or retrieval.

CRL

Certificate Revocation List. CRL is a list of revoked certificates maintained by a certification authority.

cryptobinding

Short for cryptographic binding. A procedure in a tunneled EAP method that binds together the tunnel protocol and the tunneled authentication methods, ensuring the relationship between a collection of data assets. Cryptographic binding focuses on protecting the server; mutual cryptographic binding protects both peer and server.

CSA

Channel Switch Announcement. The CSA element enables an AP to advertise that it is switching to a new channel before it begins transmitting on that channel. This allows the clients, which support CSA, to transition to the new channel with minimal downtime.

CSMA/CA

Carrier Sense Multiple Access / Collision Avoidance. CSMA/CA is a protocol for carrier transmission in networks using the 802.11 standard. CSMA/CA aims to prevent collisions by listening to the broadcasting nodes, and informing devices not to transmit any data until the broadcasting channel is free.

CSR

Certificate Signing Request. In PKI systems, a CSR is a message sent from an applicant to a CA to apply for a digital identity certificate.

CSV

Comma-Separated Values. A file format that stores tabular data in the plain text format separated by commas.

CTS

Clear to Send. The CTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See RTS.

CW

Contention Window. In QoS, CW refers to a window set for access categories based on the type of traffic. Based on the type and volume of the traffic, the minimum and maximum values can be calculated to provide a wider window when necessary.

DAI

Dynamic ARP inspection. A security feature that validates ARP packets in a network.

DAS

Distributed Antenna System. DAS is a network of antenna nodes strategically placed around a geographical area or structure for additional cellular coverage.

dB

Decibel. Unit of measure for sound or noise and is the difference or ratio between two signal levels.

dBm

Decibel-Milliwatts. dBm is a logarithmic measurement (integer) that is typically used in place of mW to represent receive-power level. AMP normalizes all signals to dBm, so that it is easy to evaluate performance between various vendors.

DCB

Data Center Bridging. DCB is a collection of standards developed by IEEE for creating a converged data center network using Ethernet.

DCE

Data Communication Equipment. DCE refers to the devices that establish, maintain, and terminate communication network sessions between a data source and its destination.

DCF

Distributed Coordination Function. DCF is a protocol that uses carrier sensing along with a four-way handshake to maximize the throughput while preventing packet collisions.

DDMO

Distributed Dynamic Multicast Optimization. DDMO is similar to Dynamic Multicast Optimization (DMO) where the multicast streams are converted into unicast streams on the AP instead of the controller, to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DES

Data Encryption Standard. DES is a common standard for data encryption and a form of secret key cryptography, which uses only one key for encryption and decryption.

designated router

Designated router refers to a router interface that is elected to originate network link advertisements for networks using the OSPF protocol.

destination NAT

Destination Network Address Translation. Destination NAT is a process of translating the destination IP address of an end route packet in a network. Destination NAT is used for redirecting the traffic destined to a virtual host to the real host, where the virtual host is identified by the destination IP address and the real host is identified by the translated IP address.

DFS

Dynamic Frequency Selection. DFS is a mandate for radio systems operating in the 5 GHz band to be equipped with means to identify and avoid interference with Radar systems.

DFT

Discrete Fourier Transform. DFT converts discrete-time data sets into a discrete-frequency representation. See FFT.

DHCP

Dynamic Host Configuration Protocol. A network protocol that enables a server to automatically assign an IP address to an IP-enabled device from a defined range of numbers configured for a given network.

DHCP snooping

DHCP snooping enables the switch to monitor and control DHCP messages received from untrusted devices that are connected to the switch.

digital certificate

A digital certificate is an electronic document that uses a digital signature to bind a public key with an identity—information such as the name of a person or an organization, address, and so forth.

Digital wireless pulse

A wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance. Ultra Wideband radio can carry a huge amount of data over a distance up to 230 ft at very low power (less than 0.5 mW), and has the ability to carry signals through doors and other obstacles that tend to reflect signals at more limited bandwidths and a higher power.

Disconnect-Ack

Disconnect-Ack is a NAS response packet to a Disconnect-Request, which indicates that the session was disconnected.

Disconnect-Nak

Disconnect-Nak is NAS response packet to a Disconnect-Request, which indicates that the session was not disconnected.

Disconnect-Request

Disconnect-Request is a RADIUS packet type sent to a NAS requesting that a user or session be disconnected.

distribution certificate

Distribution certificate is used for digitally signing iOS mobile apps to enable enterprise app distribution. It verifies the identity of the app publisher.

DLNA

Digital Living Network Alliance. DLNA is a set of interoperability guidelines for sharing digital media among multimedia devices.

DMO

Dynamic Multicast Optimization. DMO is a process of converting multicast streams into unicast streams over a wireless link to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DN

Distinguished Name. A series of fields in a digital certificate that, taken together, constitute the unique identity of the person or device that owns the digital certificate. Common fields in a DN include country, state, locality, organization, organizational unit, and the “common name”, which is the primary name used to identify the certificate.

DNS

Domain Name System. A DNS server functions as a phone book for the intranet and Internet users. It converts human-readable computer host names into IP addresses and IP addresses into host names. It stores several records for a domain name such as an address 'A' record, name server (NS), and mail exchanger (MX) records. The Address 'A' record is the most important record that is stored in a DNS server, because it provides the required IP address for a network peripheral or element.

DOCSIS

Data over Cable Service Interface Specification. A telecommunication standard for Internet access through cable modem.

DoS

Denial of Service. DoS is any type of attack where the attackers send excessive messages to flood traffic and thereby preventing the legitimate users from accessing the service.

DPD

Dead Peer Detection. A method used by the network devices to detect the availability of the peer devices.

DPI

Deep Packet Inspection. DPI is an advanced method of network packet filtering that is used for inspecting data packets exchanged between the devices and systems over a network. DPI functions at the Application layer of the Open Systems Interconnection (OSI) reference model and enables users to identify, categorize, track, reroute, or stop packets passing through a network.

DRT

Downloadable Regulatory Table. The DRT feature allows new regulatory approvals to be distributed for APs without a software upgrade or patch.

DS

Differentiated Services. The DS specification aims to provide uninterrupted quality of service by managing and controlling the network traffic, so that certain types of traffic get precedence.

DSCP

Differentiated Services Code Point. DSCP is a 6-bit packet header value used for traffic classification and priority assignment.

DSL

Digital Subscriber Line. The DSL technology allows the transmission of digital data over telephone lines. A DSL modem is a device used for connecting a computer or router to a telephone line that offers connectivity to the Internet.

DSSS

Direct-Sequence Spread Spectrum. DSSS is a modulation technique used for reducing overall signal interference. This technique multiplies the original data signal with a pseudo random noise spreading code. Spreading of this signal makes the resulting wideband channel more noisy, thereby increasing the resistance to interference. See FHSS.

DST

Daylight Saving Time. DST is also known as summer time that refers to the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

DTE

Data Terminal Equipment. DTE refers to a device that converts user information into signals or re-converts the received signals.

DTIM

Delivery Traffic Indication Message. DTIM is a kind of traffic indication map. A DTIM interval determines when the APs must deliver broadcast and multicast frames to their associated clients in power save mode.

DTLS

Datagram Transport Layer Security. DTLS communications protocol provides communications security for datagram protocols.

dynamic authorization

Dynamic authorization refers to the ability to make changes to a visitor account's session while it is in progress. This might include disconnecting a session or updating some aspect of the authorization for the session.

dynamic NAT

Dynamic Network Address Translation. Dynamic NAT maps multiple public IP addresses and uses these addresses with an internal or private IP address. Dynamic NAT helps to secure a network by

masking the internal configuration of a private network.

EAP

Extensible Authentication Protocol. An authentication protocol for wireless networks that extends the methods used by the PPP, a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

EAP-FAST

EAP – Flexible Authentication Secure Tunnel (tunneled).

EAP-GTC

EAP – Generic Token Card. (non-tunneled).

EAP-MD5

EAP – Method Digest 5. (non-tunneled).

EAP-MSCHAP

EAP Microsoft Challenge Handshake Authentication Protocol.

EAP-MSCHAPv2

EAP Microsoft Challenge Handshake Authentication Protocol Version 2.

EAP-PEAP

EAP–Protected EAP. A widely used protocol for securely transporting authentication data across a network (tunneled).

EAP-PWD

EAP-Password. EAP-PWD is an EAP method that uses a shared password for authentication.

EAP-TLS

EAP–Transport Layer Security. EAP-TLS is a certificate-based authentication method supporting mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints. See RFC 5216.

EAP-TTLS

EAP–Tunneled Transport Layer Security. EAP-TTLS is an EAP method that encapsulates a TLS session, consisting of a handshake phase and a data phase. See RFC 5281.

EAPoL

Extensible Authentication Protocol over LAN. A network port authentication protocol used in IEEE 802.1X standards to provide a generic network sign-on to access network resources.

ECC

Elliptical Curve Cryptography or Error correcting Code memory. Elliptical Curve Cryptography is a public-key encryption technique that is based on elliptic curve theory used for creating faster, smaller, and more efficient cryptographic keys. Error Correcting Code memory is a type of computer data storage that can detect and correct the most common kinds of internal data corruption. ECC

memory is used in most computers where data corruption cannot be tolerated under any circumstances, such as for scientific or financial computing.

ECDSA

Elliptic Curve Digital Signature Algorithm. ECDSA is a cryptographic algorithm that supports the use of public or private key pairs for encrypting and decrypting information.

EDCA

Enhanced Distributed Channel Access. The EDCA function in the IEEE 802.11e Quality of Service standard supports differentiated and distributed access to wireless medium based on traffic priority and Access Category types. See WMM and WME.

EIGRP

Enhanced Interior Gateway Routing Protocol. EIGRP is a routing protocol used for automating routing decisions and configuration in a network.

EIRP

Effective Isotropic Radiated Power or Equivalent Isotropic Radiated Power. EIRP refers to the output power generated when a signal is concentrated into a smaller area by the Antenna.

ESI

External Services Interface. ESI provides an open interface for integrating security solutions that solve interior network problems such as viruses, worms, spyware, and corporate compliance.

ESS

Extended Service Set. An ESS is a set of one or more interconnected BSSs that form a single sub network.

ESSID

Extended Service Set Identifier. ESSID refers to the ID used for identifying an extended service set.

Ethernet

Ethernet is a network protocol for data transmission over LAN.

EULA

End User License Agreement. EULA is a legal contract between a software application publisher or author and the users of the application.

FCC

Federal Communications Commission. FCC is a regulatory body that defines standards for the interstate and international communications by radio, television, wire, satellite, and cable.

FFT

Fast Fourier Transform. FFT is a frequency analysis mechanism that aims at faster conversion of a discrete signal in time domain into a discrete frequency domain representation. See also DFT.

FHSS

Frequency Hopping Spread Spectrum. FHSS is transmission technique that allows modulation and transmission of a data signal by rapidly switching a carrier among many frequency channels in a

random but predictable sequence. See also DSSS.

FIB

Forwarding Information Base. FIB is a forwarding table that maps MAC addresses to ports. FIB is used in network bridging, routing, and similar functions to identify the appropriate interface for forwarding packets.

FIPS

Federal Information Processing Standards. FIPS refers to a set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies, and by government contractors and vendors who work with these agencies.

firewall

Firewall is a network security system used for preventing unauthorized access to or from a private network.

FQDN

Fully Qualified Domain Name. FQDN is a complete domain name that identifies a computer or host on the Internet.

FQLN

Fully Qualified Location Name. FQLN is a device location identifier in the format: APname.Floor.Building.Campus.

frequency allocation

Use of radio frequency spectrum as regulated by governments.

FSPL

Free Space Path Loss. FSPL refers to the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space (usually air), with no obstacles nearby to cause reflection or diffraction.

FTP

File Transfer Protocol. A standard network protocol used for transferring files between a client and server on a computer network.

GARP

Generic Attribute Registration Protocol. GVRP is a LAN protocol that allows the network nodes to register and de-register attributes, such as network addresses, with each other.

GAS

Generic Advertisement Service. GAS is a request-response protocol, which provides Layer 2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps in determining a wireless network infrastructure before associating clients, and allows clients to send queries to multiple 802.11 networks in parallel.

gateway

Gateway is a network node that allows traffic to flow in and out of the network.

Gbps

Gigabits per second.

GBps

Gigabytes per second.

GET

GET refers HTTP request method or an SNMP operation method. The GET HTTP request method submits data to be processed to a specified resource. The GET SNMP operation method obtains information from the Management Information Base (MIB).

GHz

Gigahertz.

GMT

Greenwich Mean Time. GMT refers to the mean solar time at the Royal Observatory in Greenwich, London. GMT is the same as Coordinated Universal Time (UTC) standard, written as an offset of UTC +/- 00:00.

goodput

Goodput is the application level throughput that refers to the ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes.

GPS

Global Positioning System. A satellite-based global navigation system.

GRE

Generic Routing Encapsulation. GRE is an IP encapsulation protocol that is used to transport packets over a network.

GTC

Generic Token Card. GTC is a protocol that can be used as an alternative to MSCHAPv2 protocol. GTC allows authentication to various authentication databases even in cases where MSCHAPv2 is not supported by the database.

GVRP

GARP VLAN Registration Protocol or Generic VLAN Registration Protocol. GARP is an IEEE 802.1Q-compliant protocol that facilitates VLAN registration and controls VLANs within a larger network.

H2QP

Hotspot 2.0 Query Protocol.

hot zone

Wireless access area created by multiple hotspots that are located in close proximity to one another. Hot zones usually combine public safety APs with public hotspots.

hotspot

Hotspot refers to a WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can

look up a local hotspot, contact it, and get connected through its network to reach the Internet.

HSPA

High-Speed Packet Access.

HT

High Throughput. IEEE 802.11n is an HT WLAN standard that aims to achieve physical data rates of close to 600 Mbps on the 2.4 GHz and 5 GHz bands.

HTTP

Hypertext Transfer Protocol. The HTTP is an application protocol to transfer data over the web. The HTTP protocol defines how messages are formatted and transmitted, and the actions that the w servers and browsers should take in response to various commands.

HTTPS

Hypertext Transfer Protocol Secure. HTTPS is a variant of the HTTP that adds a layer of security on the data in transit through a secure socket layer or transport layer security protocol connection.

IAS

Internet Authentication Service. IAS is a component of Windows Server operating systems that provides centralized user authentication, authorization, and accounting.

ICMP

Internet Control Message Protocol. ICMP is an error reporting protocol. It is used by network devices such as routers, to send error messages and operational information to the source IP address when network problems prevent delivery of IP packets.

IDS

Intrusion Detection System. IDS monitors a network or systems for malicious activity or policy violations and reports its findings to the management system deployed in the network.

IEEE

Institute of Electrical and Electronics Engineers.

IGMP

Internet Group Management Protocol. Communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.

IGMP snooping

IGMP snooping prevents multicast flooding on Layer 2 network by treating multicast traffic as broadcast traffic. Without IGMP snooping, all streams could be flooded to all ports on that VLAN. When multicast flooding occurs, end-hosts that happen to be in the same VLAN would receive all the streams only to be discarded without snooping.

IGP

Interior Gateway Protocol. IGP is used for exchanging routing information between gateways within an autonomous system (for example, a system of corporate local area networks).

IGRP

Interior Gateway Routing Protocol. IGRP is a distance vector interior routing protocol used by routers to exchange routing data within an autonomous system.

IKE

Internet Key Exchange. IKE is a key management protocol used with IPsec protocol to establish a secure communication channel. IKE provides additional feature, flexibility, and ease of configuration for IPsec standard.

IKEv1

Internet Key Exchange version 1. IKEv1 establishes a secure authenticated communication channel by using either the pre-shared key (shared secret), digital signatures, or public key encryption. IKEv1 operates in Main and Aggressive modes. See RFC 2409.

IKEv2

Internet Key Exchange version 2. IKEv2 uses the secure channel established in Phase 1 to negotiate Security Associations on behalf of services such as IPsec. IKEv2 uses pre-shared key and Digital Signature for authentication. See RFC 4306.

IoT

Internet of Things. IoT refers to the internetworking of devices that are embedded with electronics, software, sensors, and network connectivity features allowing data exchange over the Internet.

IPM

Intelligent Power Monitoring. IPM is a feature supported on certain APs that actively measures the power utilization of an AP and dynamically adapts to the power resources.

IPS

Intrusion Prevention System. The IPS monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, log the information, attempt to block the activity, and report it.

IPsec

Internet Protocol security. IPsec is a protocol suite for secure IP communications that authenticates and encrypts each IP packet in a communication session.

IPSG

Internet Protocol Source Guard. IPSG restricts IP address from untrusted interface by filtering traffic based on list of addresses in the DHCP binding database or manually configured IP source bindings. It prevents IP spoofing attacks.

IrDA

An industry-sponsored organization set up in 1993 to create international standards for the hardware and software used in infrared communication links. In this special form of radio transmission, a focused ray of light in the infrared frequency spectrum, measured in terahertz (THz), or trillions of hertz (cycles per second), is modulated with information and sent from a transmitter to a receiver over a relatively short distance.

ISAKMP

Internet Security Association and Key Management Protocol. ISAKMP is used for establishing Security Associations and cryptographic keys in an Internet environment.

ISP

Internet Service Provider. An ISP is an organization that provides services for accessing and using the Internet.

JSON

JavaScript Object Notation. JSON is an open-standard, language-independent, lightweight data-interchange format used to transmit data objects consisting of attribute–value pairs. JSON uses a "self-describing" text format that is easy for humans to read and write, and that can be used as a data format by any programming language.

Kbps

Kilobits per second.

KBps

Kilobytes per second.

keepalive

Signal sent at periodic intervals from one device to another to verify that the link between the two devices is working. If no reply is received, data will be sent by a different path until the link is restored. A keepalive can also be used to indicate that the connection should be preserved so that the receiving device does not consider it timed out and drop it.

L2TP

Layer-2 Tunneling Protocol. L2TP is a networking protocol used by the ISPs to enable VPN operations.

LACP

Link Aggregation Control Protocol. LACP is used for the collective handling of multiple physical ports that can be seen as a single channel for network traffic purposes.

LAG

Link Aggregation Group . A LAG combines a number of physical ports together to make a single high-bandwidth data path. LAGs can connect two switches to provide a higher-bandwidth connection to a public network.

LAN

Local Area Network. A LAN is a network of connected devices within a distinct geographic area such as an office or a commercial establishment and share a common communications line or wireless link to a server.

LCD

Liquid Crystal Display. LCD is the technology used for displays in notebook and other smaller computers. Like LED and gas-plasma technologies, LCDs allow displays to be much thinner than the cathode ray tube technology.

LDAP

Lightweight Directory Access Protocol. LDAP is a communication protocol that provides the ability to access and maintain distributed directory information services over a network.

LDPC

Low-Density Parity-Check. LDPC is a method of transmitting a message over a noisy transmission channel using a linear error correcting code. An LDPC is constructed using a sparse bipartite graph.

LEAP

Lightweight Extensible Authentication Protocol. LEAP is a Cisco proprietary version of EAP used in wireless networks and Point-to-Point connections.

LED

Light Emitting Diode. LED is a semiconductor light source that emits light when an electric current passes through it.

LEEF

Log Event Extended Format. LEEF is a type of customizable syslog event format. An extended log file contains a sequence of lines containing ASCII characters terminated by either the sequence LF or CRLF.

LI

Lawful Interception. LI refers to the procedure of obtaining communications network data by the Law Enforcement Agencies for the purpose of analysis or evidence.

LLDP

Link Layer Discovery Protocol. LLDP is a vendor-neutral link layer protocol in the Internet Protocol suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, which is principally a wired Ethernet.

LLDP-MED

LLDP–Media Endpoint Discovery. LLDP-MED facilitates information sharing between endpoints and network infrastructure devices.

LMS

Local Management Switch. In multi-controller networks, each controller acts as an LMS and terminates user traffic from the APs, processes, and forwards the traffic to the wired network.

LNS

L2TP Network Server. LNS is an equipment that connects to a carrier and handles the sessions from broadband lines. It is also used for dial-up and mobile links. LNS handles authentication and routing of the IP addresses. It also handles the negotiation of the link with the equipment and establishes a session.

LTE

Long Term Evolution. LTE is a 4G wireless communication standard that provides high-speed wireless communication for mobile phones and data terminals. See 4G.

MAB

MAC Authentication Bypass. Endpoints such as network printers, Ethernet-based sensors, cameras, and wireless phones do not support 802.1X authentication. For such endpoints, MAC Authentication Bypass mechanism is used. In this method, the MAC address of the endpoint is used to authenticate the endpoint.

MAC

Media Access Control. A MAC address is a unique identifier assigned to network interfaces for communications on a network.

MAM

Mobile Application Management. MAM refers to software and services used to secure, manage, and distribute mobile applications used in enterprise settings on mobile devices like smartphones and tablet computers. Mobile Application Management can apply to company-owned mobile devices as well as BYOD.

Mbps

Megabits per second

MBps

Megabytes per second

MCS

Modulation and Coding Scheme. MCS is used as a parameter to determine the data rate of a wireless connection for high throughput.

MD4

Message Digest 4. MD4 is an earlier version of MD5 and is an algorithm used to verify data integrity through the creation of a 128-bit message digest from data input.

MD5

Message Digest 5. The MD5 algorithm is a widely used hash function producing a 128-bit hash value from the data input.

MDAC

Microsoft Data Access Components. MDAC is a framework of interrelated Microsoft technologies that provides a standard database for Windows OS.

MDM

Mobile Device Management. MDM is an administrative software to manage, monitor, and secure mobile devices of the employees in a network.

mDNS

Multicast Domain Name System. mDNS provides the ability to perform DNS-like operations on the local link in the absence of any conventional unicast DNS server. The mDNS protocol uses IP multicast User Datagram Protocol (UDP) packets, and is implemented by the Apple Bonjour and Linux NSS-mDNS services. mDNS works in conjunction with DNS Service Discovery (DNS-SD), a companion zero-configuration technique specified. See RFC 6763.

MFA

Multi-factor Authentication. MFA lets you require multiple factors, or proofs of identity, when authenticating a user. Policy configurations define how often multi-factor authentication will be required, or conditions that will trigger it.

MHz

Megahertz

MIB

Management Information Base. A hierarchical database used by SNMP to manage the devices being monitored.

microwave

Electromagnetic energy with a frequency higher than 1 GHz, corresponding to wavelength shorter than 30 centimeters.

MIMO

Multiple Input Multiple Output. An antenna technology for wireless communications in which multiple antennas are used at both source (transmitter) and destination (receiver). The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed.

MISO

Multiple Input Single Output. An antenna technology for wireless communications in which multiple antennas are used at the source (transmitter). The antennas are combined to minimize errors and optimize data speed. The destination (receiver) has only one antenna.

MLD

Multicast Listener Discovery. A component of the IPv6 suite. It is used by IPv6 routers for discovering multicast listeners on a directly attached link.

MPDU

MAC Protocol Data Unit. MPDU is a message exchanged between MAC entities in a communication system based on the layered OSI model.

MPLS

Multiprotocol Label Switching. The MPLS protocol speeds up and shapes network traffic flows.

MPPE

Microsoft Point-to-Point Encryption. A method of encrypting data transferred across PPP-based dial-up connections or PPTP-based VPN connections.

MS-CHAP

Microsoft Challenge Handshake Authentication Protocol. MS-CHAP is Password-based, challenge-response, mutual authentication protocol that uses MD4 and DES encryption.

MS-CHAPv1

Microsoft Challenge Handshake Authentication Protocol version 1. MS-CHAPv1 extends the user authentication functionality provided on Windows networks to remote workstations. MS-CHAPv1 supports only one-way authentication.

MS-CHAPv2

Microsoft Challenge Handshake Authentication Protocol version 2. MS-CHAPv2 is an enhanced version of the MS-CHAP protocol that supports mutual authentication.

MSS

Maximum Segment Size. MSS is a parameter of the options field in the TCP header that specifies the largest amount of data, specified in bytes, that a computer or communications device can receive in a single TCP segment.

MSSID

Mesh Service Set Identifier. MSSID is the SSID used by the client to access a wireless mesh network.

MSTP

Multiple Spanning Tree Protocol. MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree.

MTU

Maximum Transmission Unit. MTU is the largest size packet or frame specified in octets (eight-bit bytes) that can be sent in networks such as the Internet.

MU-MIMO

Multi-User Multiple-Input Multiple-Output. MU-MIMO is a set of multiple-input and multiple-output technologies for wireless communication, in which users or wireless terminals with one or more antennas communicate with each other.

MVRP

Multiple VLAN Registration Protocol. MVRP is a Layer 2 network protocol used for automatic configuration of VLAN information on switches.

mW

milliWatts. mW is 1/1000 of a Watt. It is a linear measurement (always positive) that is generally used to represent transmission.

NAC

Network Access Control. NAC is a computer networking solution that uses a set of protocols to define and implement a policy that describes how devices can secure access to network nodes when they initially attempt to connect to a network.

NAD

Network Access Device. NAD is a device that automatically connects the user to the preferred network, for example, an AP or an Ethernet switch.

NAK

Negative Acknowledgement. NAK is a response indicating that a transmitted message was received with errors or it was corrupted, or that the receiving end is not ready to accept transmissions.

NAP

Network Access Protection. The NAP feature in the Windows Server allows network administrators to define specific levels of network access based on identity, groups, and policy compliance. The NAP

Agent is a service that collects and manages health information for NAP client computers. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

NAS

Network Access Server. NAS provides network access to users, such as a wireless AP, network switch, or dial-in terminal server.

NAT

Network Address Translation. NAT is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

NetBIOS

Network Basic Input/Output System. A program that lets applications on different computers communicate within a LAN.

netmask

Netmask is a 32-bit mask used for segregating IP address into subnets. Netmask defines the class and range of IP addresses.

NFC

Near-Field Communication. NFC is a short-range wireless connectivity standard (ECMA-340, ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they touch or are brought closer (within a few centimeters of distance). The standard specifies a way for the devices to establish a peer-to-peer (P2P) network to exchange data.

NIC

Network Interface Card. NIC is a hardware component that allows a device to connect to the network.

Nmap

Network Mapper. Nmap is an open-source utility for network discovery and security auditing. Nmap uses IP packets to determine such things as the hosts available on a network and their services, operating systems and versions, types of packet filters/firewalls, and so on.

NMI

Non-Maskable Interrupt. NMI is a hardware interrupt that standard interrupt-masking techniques in the system cannot ignore. It typically occurs to signal attention for non-recoverable hardware errors.

NMS

Network Management System. NMS is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework.

NOE

New Office Environment. NOE is a proprietary VoIP protocol designed by Alcatel-Lucent Enterprise.

NTP

Network Time Protocol. NTP is a protocol for synchronizing the clocks of computers over a network.

OAuth

Open Standard for Authorization. OAuth is a token-based authorization standard that allows websites or third-party applications to access user information, without exposing the user credentials.

OCSP

Online Certificate Status Protocol. OCSP is used for determining the current status of a digital certificate without requiring a CRL.

OFDM

Orthogonal Frequency Division Multiplexing. OFDM is a scheme for encoding digital data on multiple carrier frequencies.

OID

Object Identifier. An OID is an identifier used to name an object. The OIDs represent nodes or managed objects in a MIB hierarchy. The OIDs are designated by text strings and integer sequences and are formally defined as per the ASN.1 standard.

OKC

Opportunistic Key Caching. OKC is a technique available for authentication between multiple APs in a network where those APs are under common administrative control. Using OKC, a station roaming to any AP in the network will not have to complete a full authentication exchange, but will instead just perform the 4-way handshake to establish transient encryption keys.

onboarding

The process of preparing a device for use on an enterprise network, by creating the appropriate access credentials and setting up the network connection parameters.

OpenFlow

OpenFlow is an open communications interface between control plane and the forwarding layers of a network.

OpenFlow agent

OpenFlow agent. OpenFlow is a software module in Software-Defined Networking (SDN) that allows the abstraction of any legacy network element, so that it can be integrated and managed by the SDN controller. OpenFlow runs on network devices such as switches, routers, wireless controllers, and APs.

Optical wireless

Optical wireless is combined use of conventional radio frequency wireless and optical fiber for telecommunication. Long-range links are provided by using optical fibers; the links from the long-range endpoints to end users are accomplished by RF wireless or laser systems. RF wireless at Ultra High Frequencies and microwave frequencies can carry broadband signals to individual computers at substantial data speeds.

OSI

Open Systems Interconnection. OSI is a reference model that defines a framework for communication between the applications in a network.

OSPF

Open Shortest Path First. OSPF is a link-state routing protocol for IP networks. It uses a link-state routing algorithm and falls into the group of interior routing protocols that operates within a single Autonomous System (AS).

OSPFv2

Open Shortest Path First version 2. OSPFv2 is the version 2 of the link-state routing protocol, OSPF. See RFC 2328.

OUI

Organizationally Unique Identifier. Synonymous with company ID or vendor ID, an OUI is a 24-bit, globally unique assigned number, referenced by various standards. The first half of a MAC address is OUI.

OVA

Open Virtualization Archive. OVA contains a compressed installable version of a virtual machine.

OVF

Open Virtualization Format. OVF is a specification that describes an open-standard, secure, efficient, portable and extensible format for packaging and distributing software for virtual machines.

PAC

Protected Access Credential. PAC is distributed to clients for optimized network authentication. These credentials are used for establishing an authentication tunnel between the client and the authentication server.

PAP

Password Authentication Protocol. PAP validates users by password. PAP does not encrypt passwords for transmission and is thus considered insecure.

PAPI

Process Application Programming Interface. PAPI controls channels for ARM and Wireless Intrusion Detection System (WIDS) communication to the master controller. A separate PAPI control channel connects to the local controller where the SSID tunnels terminate.

PBR

Policy-based Routing. PBR provides a flexible mechanism for forwarding data packets based on polices configured by a network administrator.

PDU

Power Distribution Unit or Protocol Data Unit. Power Distribution Unit is a device that distributes electric power to the networking equipment located within a data center. Protocol Data Unit contains protocol control Information that is delivered as a unit among peer entities of a network.

PEAP

Protected Extensible Authentication Protocol. PEAP is a type of EAP communication that addresses security issues associated with clear text EAP transmissions by creating a secure channel encrypted and protected by TLS.

PEF

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFNG

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFV

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PFS

Perfect Forward Secrecy. PFS refers to the condition in which a current session key or long-term private key does not compromise the past or subsequent keys.

PHB

Per-hop behavior. PHB is a term used in DS or MPLS. It defines the policy and priority applied to a packet when traversing a hop (such as a router) in a DiffServ network.

PIM

Protocol-Independent Multicast. PIM refers to a family of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the Internet.

PIN

Personal Identification Number. PIN is a numeric password used to authenticate a user to a system.

PKCS#n

Public-key cryptography standard n. PKCS#n refers to a numbered standard related to topics in cryptography, including private keys (PKCS#1), digital certificates (PKCS#7), certificate signing requests (PKCS#10), and secure storage of keys and certificates (PKCS#12).

PKI

Public Key Infrastructure. PKI is a security technology based on digital certificates and the assurances provided by strong cryptography. See also certificate authority, digital certificate, public key, private key.

PLMN

Public Land Mobile Network. PLMS is a network established and operated by an administration or by a Recognized Operating Agency for the specific purpose of providing land mobile telecommunications services to the public.

PMK

Pairwise Master Key. PMK is a shared secret key that is generated after PSK or 802.1X authentication.

PoE

Power over Ethernet. PoE is a technology for wired Ethernet LANs to carry electric power required for the device in the data cables. The IEEE 802.3af PoE standard provides up to 15.4 W of power on each port.

PoE+

Power over Ethernet+. PoE+ is an IEEE 802.3at standard that provides 25.5W power on each port.

POST

Power On Self Test. An HTTP request method that requests data from a specified resource.

PPP

Point-to-Point Protocol. PPP is a data link (layer 2) protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption, and compression.

PPPoE

Point-to-Point Protocol over Ethernet. PPPoE is a method of connecting to the Internet, typically used with DSL services, where the client connects to the DSL modem.

PPTP

Point-to-Point Tunneling Protocol. PPTP is a method for implementing virtual private networks. It uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

private key

The part of a public-private key pair that is always kept private. The private key encrypts the signature of a message to authenticate the sender. The private key also decrypts a message that was encrypted with the public key of the sender.

PRNG

Pseudo-Random Number Generator. PRNG is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers.

PSK

Pre-shared key. A unique shared secret that was previously shared between two parties by using a secure channel. This is used with WPA security, which requires the owner of a network to provide a passphrase to users for network access.

PSU

Power Supply Unit. PSU is a unit that supplies power to an equipment by converting mains AC to low-voltage regulated DC power.

public key

The part of a public-private key pair that is made public. The public key encrypts a message and the message is decrypted with the private key of the recipient.

PVST

Per-VLAN Spanning Tree. PVST provides load balancing of VLANs across multiple ports resulting in optimal usage of network resources.

PVST+

Per-VLAN Spanning Tree+. PVST+ is an extension of the PVST standard that uses the 802.1Q trunking technology.

QoS

Quality of Service. It refers to the capability of a network to provide better service and performance to a specific network traffic over various technologies.

RA

Router Advertisement. The RA messages are sent by the routers in the network when the hosts send multicast router solicitation to the multicast address of all routers.

Radar

Radio Detection and Ranging. Radar is an object-detection system that uses radio waves to determine the range, angle, or velocity of objects.

RADIUS

Remote Authentication Dial-In User Service. An Industry-standard network access protocol for remote authentication. It allows authentication, authorization, and accounting of remote users who want to access network resources.

RAM

Random Access Memory.

RAPIDS

Rogue Access Point identification and Detection System. An AMP module that is designed to identify and locate wireless threats by making use of all of the information available from your existing infrastructure.

RARP

Reverse Address Resolution Protocol. RARP is a protocol used by a physical machine in a local area network for determining the IP address from the ARP table or cache of the gateway server.

Regex

Regular Expression. Regex refers to a sequence of symbols and characters defining a search pattern.

Registration Authority

Type of Certificate Authority that processes certificate requests. The Registration Authority verifies that requests are valid and comply with certificate policy, and authenticates the user's identity. The Registration Authority then forwards the request to the Certificate Authority to sign and issue the certificate.

Remote AP

Remote APs extend corporate network to the users working from home or at temporary work sites. Remote APs are deplyed at branch office sites and are connected to the central network on a WAN link.

REST

Representational State Transfer. REST is a simple and stateless architecture that the web services use for providing interoperability between computer systems on the Internet. In a RESTful web service, requests made to the URI of a resource will elicit a response that may be in XML, HTML, JSON or some other defined format.

RF

Radio Frequency. RF refers to the electromagnetic wave frequencies within a range of 3 kHz to 300 GHz, including the frequencies used for communications or Radar signals.

RFC

Request For Comments. RFC is a commonly used format for the Internet standards documentss.

RFID

Radio Frequency Identification. RFID uses radio waves to automatically identify and track the information stored on a tag attached to an object.

RIP

Routing Information Protocol. RIP prevents the routing loops by limiting the number of hops allowed in a path from source to destination.

RJ45

Registered Jack 45. RJ45 is a physical connector for network cables.

RMA

Return Merchandise Authorization. RMA is a part of the product returning process that authorizes users to return a product to the manufacturer or distributor for a refund, replacement, or repair. The customers who want to return a product within its Warranty period contact the manufacturer to initiate the product returning process. The manufacturer or the seller generates an authorization number for the RMA, which is used by the customers, when returning a product to the warehouse.

RMON

Remote Monitoring. RMON provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed LANs.

RoW

Rest of World. RoW or RW is an operating country code of a device.

RSA

Rivest, Shamir, Adleman. RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

RSSI

Received Signal Strength Indicator. RSSI is a mechanism by which RF energy is measured by the circuitry on a wireless NIC (0-255). The RSSI is not standard across vendors. Each vendor determines its own RSSI scale/values.

RSTP

Rapid Spanning Tree Protocol. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this.

RTCP

RTP Control Protocol. RTCP provides out-of-band statistics and control information for an Real-Time Transport Protocol session.

RTLS

Real-Time Location Systems. RTLS automatically identifies and tracks the location of objects or people in real time, usually within a building or other contained area.

RTP

Real-Time Transport Protocol. RTP is a network protocol used for delivering audio and video over IP networks.

RTS

Request to Send. RTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See CTS.

RTSP

Real Time Streaming Protocol. RTSP is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.

RVI

Routed VLAN Interface. RVI is a switch interface that forwards packets between VLANs.

RW

Rest of World. RoW or RW is an operating country code of a device.

SA

Security Association. SA is the establishment of shared security attributes between two network entities to support secure communication.

SAML

Security Assertion Markup Language. SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication.

SCEP

Simple Certificate Enrollment Protocol. SCEP is a protocol for requesting and managing digital certificates.

SCP

Secure Copy Protocol. SCP is a network protocol that supports file transfers between hosts on a network.

SCSI

Small Computer System Interface. SCSI refers to a set of interface standards for physical connection and data transfer between a computer and the peripheral devices such as printers, disk drives, CD-ROM, and so on.

SD-WAN

Software-Defined Wide Area Network. SD-WAN is an application for applying SDN technology to WAN connections that connect enterprise networks across disparate geographical locations.

SDN

Software-Defined Networking. SDN is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of the modern data center.

SDR

Server Derivation Rule. An SDR refers to a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on the rules defined under a server group. The SDRs override the default authentication roles and VLANs defined in the AAA and Virtual AP profiles.

SDU

Service Data Unit. SDU is a unit of data that has been passed down from an OSI layer to a lower layer and that has not yet been encapsulated into a PDU by the lower layer.

SFP

The Small Form-factor Pluggable. SFP is a compact, hot-pluggable transceiver that is used for both telecommunication and data communications applications.

SFP+

Small Form-factor Pluggable+. SFP+ supports up to data rates up to 16 Gbps.

SFTP

Secure File Transfer Protocol. SFTP is a network protocol that allows file access, file transfer, and file management functions over a secure connection.

SHA

Secure Hash Algorithm. SHA is a family of cryptographic hash functions. The SHA algorithm includes the SHA, SHA-1, SHA-2 and SHA-3 variants.

SIM

Subscriber Identity Module. SIM is an integrated circuit that is intended to securely store the International Mobile Subscriber Identity (IMSI) number and its related key, which are used for identifying and authenticating subscribers on mobile telephony devices.

SIP

Session Initiation Protocol. SIP is used for signaling and controlling multimedia communication session such as voice and video calls.

SIRT

Security Incident Response Team. SIRT is responsible for reviewing as well as responding to computer security incident reports and activity.

SKU

Stock Keeping Unit. SKU refers to the product and service identification code for the products in the inventory.

SLAAC

Stateless Address Autoconfiguration. SLAAC provides the ability to address a host based on a network prefix that is advertised from a local network router through router advertisements.

SMB

Server Message Block or Small and Medium Business. Server Message Block operates as an application-layer network protocol mainly used for providing shared access to files, printers, serial ports, and for miscellaneous communications between the nodes on a network.

SMS

Short Message Service. SMS refers to short text messages (up to 140 characters) sent and received through mobile phones.

SMTP

Simple Mail Transfer Protocol. SMTP is an Internet standard protocol for electronic mail transmission.

SNIR

Signal-to-Noise-Plus-Interference Ratio. SNIR refers to the power of a central signal of interest divided by the sum of the interference power and the power of the background noise. SINR is defined as the power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.

SNMP

Simple Network Management Protocol. SNMP is a TCP/IP standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMPv1

Simple Network Management Protocol version 1. SNMPv1 is a widely used network management protocol.

SNMPv2

Simple Network Management Protocol version 2. SNMPv2 is an enhanced version of SNMPv1, which includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications.

SNMPv2c

Community-Based Simple Network Management Protocol version 2. SNMPv2C uses the community-based security scheme of SNMPv1 and does not include the SNMPv2 security model.

SNMPv3

Simple Network Management Protocol version 3. SNMPv3 is an enhanced version of SNMP that includes security and remote configuration features.

SNR

Signal-to-Noise Ratio. SNR is used for comparing the level of a desired signal with the level of background noise.

SNTP

Simple Network Time Protocol. SNTP is a less complex implementation of NTP. It uses the same , but does not require the storage of state over extended periods of time.

SOAP

Simple Object Access Protocol. SOAP enables communication between the applications running on different operating systems, with different technologies and programming languages. SOAP is an XML-based messaging protocol for exchanging structured information between the systems that support web services.

SoC

System on a Chip. SoC is an Integrated Circuit that integrates all components of a computer or other electronic system into a single chip.

source NAT

Source NAT changes the source address of the packets passing through the router. Source NAT is typically used when an internal (private) host initiates a session to an external (public) host.

SSH

Secure Shell. SSH is a network protocol that provides secure access to a remote device.

SSID

Service Set Identifier. SSID is a name given to a WLAN and is used by the client to access a WLAN network.

SSL

Secure Sockets Layer. SSL is a computer networking protocol for securing connections between network application clients and servers over the Internet.

SSO

Single Sign-On. SSO is an access-control property that allows the users to log in once to access multiple related, but independent applications or systems to which they have privileges. The process authenticates the user across all allowed resources during their session, eliminating additional login prompts.

STBC

Space-Time Block Coding. STBC is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas and to exploit the various received versions of the data to improve the reliability of data transfer.

STM

Station Management. STM is a process that handles AP management and user association.

STP

Spanning Tree Protocol. STP is a network protocol that builds a logical loop-free topology for Ethernet networks.

SU-MIMO

Single-User Multiple-Input Multiple-Output. SU-MIMO allocates the full bandwidth of the AP to a single high-speed device during the allotted time slice.

subnet

Subnet is the logical division of an IP network.

subscription

A business model where a customer pays a certain amount as subscription price to obtain access to a product or service.

SVP

SpectraLink Voice Priority. SVP is an open, straightforward QoS approach that has been adopted by most leading vendors of WLAN APs. SVP favors isochronous voice packets over asynchronous data packets when contending for the wireless medium and when transmitting packets onto the wired LAN.

SWAN

Structured Wireless-Aware Network. A technology that incorporates a Wireless Local Area Network (WLAN) into a wired Wide Area Network (WAN). SWAN technology can enable an existing wired network to serve hundreds of users, organizations, corporations, or agencies over a large geographic area. SWAN is said to be scalable, secure, and reliable.

TAC

Technical Assistance Center.

TACACS

Terminal Access Controller Access Control System. TACACS is a family of protocols that handles remote authentication and related services for network access control through a centralized server.

TACACS+

Terminal Access Controller Access Control System+. TACACS+ provides separate authentication, authorization, and accounting services. It is derived from, but not backward compatible with, TACACS.

TCP

Transmission Control Protocol. TCP is a communication protocol that defines the standards for establishing and maintaining network connection for applications to exchange data.

TCP/IP

Transmission Control Protocol/ Internet Protocol. TCP/IP is the basic communication language or protocol of the Internet.

TFTP

Trivial File Transfer Protocol. The TFTP is a software utility for transferring files from or to a remote host.

TIM

Traffic Indication Map. TIM is an information element that advertises if any associated stations have buffered unicast frames. APs periodically send the TIM within a beacon to identify the stations that are using power saving mode and the stations that have undelivered data buffered on the AP.

TKIP

Temporal Key Integrity Protocol. A part of the WPA encryption standard for wireless networks. TKIP is the next-generation Wired Equivalent Privacy (WEP) that provides per-packet key mixing to address the flaws encountered in the WEP standard.

TLS

Transport Layer Security. TLS is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections above the Transport Layer by using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

TLV

Type-length-value or Tag-Length-Value. TLV is an encoding format. It refers to the type of data being processed, the length of the value, and the value for the type of data being processed.

ToS

Type of Service. The ToS field is part of the IPv4 header, which specifies datagrams priority and requests a route for low-delay, high-throughput, or a highly reliable service.

TPC

Transmit Power Control. TPC is a part of the 802.11h amendment. It is used to regulate the power levels used by 802.11a radio cards.

TPM

Trusted Platform Module. TPM is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.

TSF

Timing Synchronization Function. TSF is a WLAN function that is used for synchronizing the timers for all the stations in a BSS.

TSPEC

Traffic Specification. TSPEC allows an 802.11e client or a QoS-capable wireless client to signal its traffic requirements to the AP.

TSV

Tab-Separated Values. TSV is a file format that allows the exchange of tabular data between applications that use different internal data formats.

TTL

Time to Live. TTL or hop limit is a mechanism that sets limits for data expiry in a computer or network.

TTY

TeleTypeWriter. TTY-enabled devices allow telephones to transmit text communications for people who are deaf or hard of hearing as well as transmit voice communication.

TXOP

Transmission Opportunity. TXOP is used in wireless networks supporting the IEEE 802.11e Quality of Service (QoS) standard. Used in both EDCA and HCF Controlled Channel Access modes of operation, TXOP is a bounded time interval in which stations supporting QoS are permitted to transfer a series of frames. TXOP is defined by a start time and a maximum duration.

U-APSD

Unscheduled Automatic Power Save Delivery. U-APSD is a part of 802.11e and helps considerably in increasing the battery life of VoWLAN terminals.

UAM

Universal Access Method. UAM allows subscribers to access a wireless network after they successfully log in from a web browser.

UCC

Unified Communications and Collaboration. UCC is a term used to describe the integration of various communications methods with collaboration tools such as virtual whiteboards, real-time audio and video conferencing, and enhanced call control capabilities.

UDID

Unique Device Identifier. UDID is used to identify an iOS device.

UDP

User Datagram Protocol. UDP is a part of the TCP/IP family of protocols used for data transfer. UDP is typically used for streaming media. UDP is a stateless protocol, which means it does not acknowledge that the packets being sent have been received.

UDR

User Derivation Rule. UDR is a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on MAC address, BSSID, DHCP-Option, encryption type, SSID, and the location of a user. For example, for an SSID with captive portal in the initial role, a UDR can be configured for scanners to provide a role based on their MAC OUI.

UHF

Ultra high frequency. UHF refers to radio frequencies between the range of 300 MHz and 3 GHz. UHF is also known as the decimeter band as the wavelengths range from one meter to one decimeter.

UI

User Interface.

UMTS

Universal Mobile Telecommunication System. UMTS is a third generation mobile cellular system for networks. See 3G.

UPnP

Universal Plug and Play. UPnp is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi APs, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

URI

Uniform Resource Identifier. URI identifies the name and the location of a resource in a uniform format.

URL

Uniform Resource Locator. URL is a global address used for locating web resources on the Internet.

USB

Universal Serial Bus. USB is a connection standard that offers a common interface for communication between the external devices and a computer. USB is the most common port used in the client devices.

UTC

Coordinated Universal Time. UTC is the primary time standard by which the world regulates clocks and time.

UWB

Ultra-Wideband. UWB is a wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance.

VA

Virtual Appliance. VA is a pre-configured virtual machine image, ready to run on a hypervisor.

VBR

Virtual Beacon Report. VBR displays a report with the MAC address details and RSSI information of an AP.

VHT

Very High Throughput. IEEE 802.11ac is an emerging VHT WLAN standard that could achieve physical data rates of close to 7 Gbps for the 5 GHz band.

VIA

Virtual Intranet Access. VIA provides secure remote network connectivity for Android, Apple iOS, Mac OS X, and Windows mobile devices and laptops. It automatically scans and selects the best secure connection to the corporate network.

VLAN

Virtual Local Area Network. In computer networking, a single Layer 2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them through one or more routers; such a domain is referred to as a Virtual Local Area Network, Virtual LAN, or VLAN.

VM

Virtual Machine. A VM is an emulation of a computer system. VMs are based on computer architectures and provide functionality of a physical computer.

VoIP

Voice over IP. VoIP allows transmission of voice and multimedia content over an IP network.

VoWLAN

Voice over WLAN. VoWLAN is a method of routing telephone calls for mobile users over the Internet using the technology specified in IEEE 802.11b. Routing mobile calls over the Internet makes them free, or at least much less expensive than they would be otherwise.

VPN

Virtual Private Network. VPN enables secure access to a corporate network when located remotely. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

VRD

Validated Reference Design. VRDs are guides that capture the best practices for a particular technology in field.

VRF

VisualRF. VRF is an AirWave Management Platform (AMP) module that provides a real-time, network-wide views of your entire Radio Frequency environment along with floor plan editing capabilities. VRF also includes overlays on client health to help diagnose issues related to clients, floor plan, or a specific location.

VRF Plan

VisualRF Plan. A stand-alone Windows client used for basic planning procedures such as adding a floor plan, provisioning APs, and generating a Bill of Materials report.

VRRP

Virtual Router Redundancy Protocol. VRRP is an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN.

VSA

Vendor-Specific Attribute. VSA is a method for communicating vendor-specific information between NASs and RADIUS servers.

VTP

VLAN Trunking Protocol. VTP is a Cisco proprietary protocol for propagating VLANs on a LAN.

W-CDMA

Wideband Code-Division Multiple Access. W-CDMA is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices.

walled garden

Walled garden is a feature that allows blocking of unauthorized users from accessing network resources.

WAN

Wide Area Network. WAN is a telecommunications network or computer network that extends over a large geographical distance.

WASP

Wireless Application Service Provider. WASP provides a web-based access to applications and services that would otherwise have to be stored locally and makes it possible for customers to access the service from a variety of wireless devices, such as a smartphone or Personal Digital Assistant (PDA).

WAX

Wireless abstract XML. WAX is an abstract markup language and a set of tools that is designed to help wireless application development as well as portability. Its tags perform at a higher level of abstraction than that of other wireless markup languages such as HTML, HDML, WML, XSL, and more.

web service

Web services allow businesses to share and process data programmatically. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

WEP

Wired Equivalent Privacy. WEP is a security protocol that is specified in 802.11b and is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN.

WFA

Wi-Fi Alliance. WFA is a non-profit organization that promotes Wi-Fi technology and certifies Wi-Fi products if they conform to certain standards of interoperability.

Wi-Fi

Wi-Fi is a technology that allows electronic devices to connect to a WLAN network, mainly using the 2.4 GHz and 5 GHz radio bands. Wi-Fi can apply to products that use any 802.11 standard.

WIDS

Wireless Intrusion Detection System. WIDS is an application that detects the attacks on a wireless network or wireless system.

WiMAX

Worldwide Interoperability for Microwave Access. WiMAX refers to the implementation of IEEE 802.16 family of wireless networks standards set by the WiMAX forum.

WIP

Wireless Intrusion Protection. The WIP module provides wired and wireless AP detection, classification, and containment. It detects Denial of Service (DoS) and impersonation attacks, and prevents client and network intrusions.

WIPS

Wireless Intrusion Prevention System. WIPS is a dedicated security device or integrated software application that monitors the radio spectrum of WLAN network for rogue APs and other wireless threats.

WISP

Wireless Internet Service Provider. WISP allows subscribers to connect to a server at designated hotspots using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers called stations, to access the Internet and the web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.

WISPr

Wireless Internet Service Provider Roaming. The WISPr framework enables the client devices to roam between the wireless hotspots using different ISPs.

WLAN

Wireless Local Area Network. WLAN is a 802.11 standards-based LAN that the users access through a wireless connection.

WME

Wireless Multimedia Extension. WME is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE) and background (AC_BK). See WMM.

WMI

Windows Management Instrumentation. WMI consists of a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification.

WMM

Wi-Fi Multimedia. WMM is also known as WME. It refers to a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK).

WPA

Wi-Fi Protected Access. WPA is an interoperable wireless security specification subset of the IEEE 802.11 standard. This standard provides authentication capabilities and uses TKIP for data encryption.

WPA2

Wi-Fi Protected Access 2. WPA2 is a certification program maintained by IEEE that oversees standards for security over wireless networks. WPA2 supports IEEE 802.1X/EAP authentication or PSK technology, but includes advanced encryption mechanism using CCMP that is referred to as AES.

WSDL

Web Service Description Language. WSDL is an XML-based interface definition language used to describe the functionality provided by a web service.

WSP

Wireless Service Provider. The service provider company that offers transmission services to users of wireless devices through Radio Frequency (RF) signals rather than through end-to-end wire communication.

WWW

World Wide Web.

X.509

X.509 is a standard for a public key infrastructure for managing digital certificates and public-key encryption. It is an essential part of the Transport Layer Security protocol used to secure web and email communication.

XAuth

Extended Authentication. XAuth provides a mechanism for requesting individual authentication information from the user, and a local user database or an external authentication server. It provides a method for storing the authentication information centrally in the local network.

XML

Extensible Markup Language. XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

XML-RPC

XML Remote Procedure Call. XML-RPC is a protocol that uses XML to encode its calls and HTTP as a transport mechanism. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

ZTP

Zero Touch Provisioning. ZTP is a device provisioning mechanism that allows automatic and quick provisioning of devices with a minimal or at times no manual intervention.