Aruba Instant 6.2.0.0-3.2

ARUBA networks

Release Notes

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1 Release Overview 5
Chapter Overview 5
Contacting Support 5

Chapter 2 What's New in this Release 7
New Features and Enhancements 7
Fast Failover with Two Tunnels 7
WISPr Authentication 7
SSH Support on Instant APs 7
RAP-108/109 Support 8
Aruba AirGroup Support 8
Wi-Fi Uplink 8
Local Probe Request Threshold 8
Maximum Clients Threshold 9
Access Control List (ACL) per SSID 9
Authentication Survivability 9
Additional Authentication Methods per SSID 9
IAP and Client Information Sync Enhancements 10
IAP Functions Without Uplink 10
Preference to an IAP with 3G/4G Card for Master Election 10
Preference to an IAP with Non-Default IP for Master Election 11
RTLS Enhancement 11
GVRP Based VLAN Configuration 11
RAPNG over HTTP 11
SNMP Support for Uplink Management Events 11
Daylight Savings Time Configuration 12
Basic Wired 802.1X Authentication 12
MAC OUI Role Derivation for Open and PSK SSIDs 12
VLAN Pooling 12
Known Issues and Limitations 13
The following are known issues and limitations in this release of Aruba Instant. 13
AirGroup 13
Authentication 13
Mobility 13
Spectrum 13
VPN Configuration 14
Security Limitation 14

Chapter 3 Features Added in the Previous Releases 15
New Features and Enhancements in Aruba Instant 6.1.3.4-3.1 15
4G LTE Modem Support 15
Mobility Access Switch (MAS) Integration 15
GRE Tunnel Enhancements 16
Disable Provisioning SSID 16
DHCP Based Role Derivation 16
Video Dynamic Multicast Optimization (DMO) 16
Multimedia ALG (Facetime, OCS) 16
AirWave Primary/Backup 17

Deny Inter User Bridging and Deny Local Routing 17
DHCP Relay Agent and Option 82 17
Enhancements to Internal DHCP Server for Clients 17
Captive Portal Redirect URL 18
Uplink Switching based on VPN Status 18
Image URL Upgrade Support 18
Wired Bridging on Ethernet 0 of an Instant AP 18
Uplink Management VLAN 18
Instant AP Wired Authentication 19
Captive Portal Localization of the Instant AP 19
Layer-3 Mobility 19
Spectrum Monitor for IAP 19
New Options in ACL Configuration 20
Hierarchical Mode of Deployment 20
Number of SSIDs Supported 20
PPPoE Support 21
DNS Support for RAP/CAP Conversion 21

Chapter 4 Known Issues in Previous Releases 23

Access Point 23
Mobility 23
Security 23

Chapter 1

Release Overview

Aruba Instant 6.2.0.0-3.2 is a major software release that introduces new features and fixes to some previously known issues. For details on all of the features described in the following sections, see the Aruba Instant 6.2.0.0-3.2 User Guide.

Chapter Overview

- "What's New in this Release" on page 7 lists the new features introduced in this release.
- "Features Added in the Previous Releases" on page 15 describes the new features that were added in the previous release of Aruba Instant.
- "Known Issues in Previous Releases" on page 23 lists the known issues reported in previous releases of Aruba Instant.

Contacting Support

Main Site	arubanetworks.com
Support Site	support.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 Telephones	arubanetworks.com/support-services/aruba-support-program/contact-support/
Software Licensing Site	licensing.arubanetworks.com/login.php
Wireless Security Incident Response Team (WSIRT)	arubanetworks.com/support/wsirt.php
Support Email Addresses	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

This chapter provides a brief summary of the new features included in this version of Aruba Instant and also includes a list of all the bugs fixed and new known issues identified in this release.

New Features and Enhancements

Fast Failover with Two Tunnels

With this feature, an Instant AP (IAP) creates a backup VPN tunnel to the controller along with the primary tunnel, and maintains both the primary and backup tunnel separately. If the primary tunnel fails, the IAP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.

WISPr Authentication

Instant now supports authentication for Wireless Internet Service Provider roaming (WISPr). WISPr authentication allows a smart client to authenticate on the network, when they roam between wireless internet service providers (ISP), even if the wireless hotspot uses an ISP with whom the client may not have an account.

If you are a hotspot operator using WISPr authentication and a client that has an account with your ISP attempts to access the Internet at your hotspot, your ISP's WISPr AAA server authenticates that client directly and allows the client access on the network. If, however, the client only has an account with a *partner* ISP, then your ISP's WISPr AAA server forwards that 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 your hotspot's own ISP as per their service agreements. The IAP assigns the default WISPr user role to the client when your ISP sends an authentication message to the IAP.

Instant supports the following smart clients:

- iPass
- Boingo

These smart clients enable client authentication and roaming between hotspots by embedding iPass Generic Interface Specification (GIS) *redirect*, *authentication*, and *logoff* messages within HTML messages that are sent to the IAP.

To configure WISPr authentication, go to **Settings > Advanced > WISPr** tab in the Instant UI. Once configured, WISPr authentication may be enabled or disabled in the **Networks > New WLAN > Access** tab.

SSH Support on Instant APs

Instant supports terminal access for diagnostic purposes only. Telnet access to the CLI has been deprecated as of this release. When the Terminal Access option is enabled, only SSH access to the CLI will be possible.

To enable or disable the SSH access, go to **Settings > Show Advanced options > Terminal access**.

RAP-108/109 Support

Aruba Instant now supports RAP-108/109.

Aruba AirGroup Support

Aruba Instant now supports AirGroup™ services. Aruba AirGroup is a unique enterprise-class capability that leverages zero configuration networking to enable Bonjour® services like Apple® AirPrint and AirPlay from mobile devices. Bonjour, the trade name for the zeroconf implementation introduced by Apple, is the most common example. 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.

AirGroup solution supports both wired and wireless devices. Wired devices which support the Bonjour services are made part of the AirGroup when the VLANs of the devices are terminated on the Virtual Controller.

ClearPass Policy Manager and ClearPass Guest Features

AirGroup also supports Aruba ClearPass Policy Manager (CPPM).

With Aruba CPPM:

- Users, such as students in dorm rooms can register their personal devices and define a group of users who are allowed to share the users' registered devices.
- Administrators can register and manage an organization's shared devices like printers and conference room Apple TVs. An administrator can grant global access to each device, or restrict access according to the username, role, or user location.

To enable AirGroup in the Instant UI, go to **Settings > Air Group**.

Wi-Fi Uplink

The Wi-Fi uplink feature is supported for all the IAP models but only the master IAP can establish the uplink. This feature allows the master IAP to establish Wi-Fi uplinks to **PSK-CCMP**, **PSK-TKIP**, and **open** SSIDs.

- For single radio IAPs, the radio can be used to serve both wireless clients and Wi-Fi uplink.
- For dual radio IAPs, one radio is used for both Wi-Fi uplink and to serve wireless clients, and the other radio only serves wireless clients.

To configure a Wi-Fi uplink, go to **Settings > Advanced > Uplink > WiFi** in the Instant UI.

Local Probe Request Threshold

This feature allows you to control whether or not a BSSID of an IAP should respond when a client sends a broadcast probe request frame to search for all available SSIDs. The supported range of Received Signal Strength Indication (RSSI) values is 0-100 dB.

To configure this feature, click **New > New WLAN > Show advanced options > Local probe request threshold** in the Instant UI.

Maximum Clients Threshold

Instant now allows you to configure clients for each BSSID on a WLAN. The supported range is 0 - 255 and the default value is 64.

To configure this feature, go to **New > New WLAN > Show advanced options > Max clients threshold** in the Instant UI.

Access Control List (ACL) per SSID

This release of Instant supports configuration of up to 64 access rules.

Authentication Survivability

This feature provides authentication and authorization survivability against remote link failure for Aruba Instant when working with ClearPass Policy Manager. When enabled, this feature allows Instant to authenticate the previously connected clients using EAP-PEAP authentication even when connectivity to ClearPass Policy Manager is temporarily lost.

To enable Authentication Survivability in the Instant UI, go to **New > New WLAN > Security tab > Authentication survivability**.

Additional Authentication Methods per SSID

In previous releases, Aruba Instant supported MAC, 802.1X, and captive portal authentications on different SSIDs. The network administrator could choose only one of these authentication methods for a SSID. This version of Aruba Instant supports the following additional methods of authentication on a SSID:

- MAC + 802.1X Authentication
- MAC + Captive Portal Authentication

You can also apply these authentication methods to a wired profile.

MAC + 802.1X Authentication

This authentication method has the following features:

- MAC authentication occurs before 802.1X authentication

  The administrator is allowed to 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 done first. If MAC authentication fails, 802.1X authentication will not begin. If MAC authentication succeeds, 802.1X authentication is carried out. If 802.1X authentication succeeds, 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 an administrator to create a **mac-auth-only** role (similar to **machine-auth-only** role concept) for role-based access rules when MAC authentication is enabled for 802.1X authentication. The **mac-auth-only** role is assigned to a client if MAC authentication succeeds and 802.1X authentication fails. If 802.1X authentication succeeds, the role will be overwritten by the final role. The **mac-auth-only** is supported only for wireless clients.

- L2 authentication fail-through

  Allows an administrator to enable the **l2-authentication-failthrough** mode. If this option is enabled and MAC authentication fails, 802.1X authentication is still allowed. If this option is disabled, 802.1X authentication is not allowed. The **l2-authentication-failthrough** option is disabled by default.

To configure MAC + 802.1X authentication, go to the **Network > WLAN > Access** tab of the Aruba Instant UI.

MAC + Captive Portal Authentication

This authentication method has the following features:

- 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.
- If the captive portal splash page type is **none**, MAC authentication cannot be enabled.
- MAC authentication only role— You can use the WLAN wizard to configure the **mac-auth-only** role in the role-based access rule configuration section when MAC authentication is enabled with captive portal authentication.

To configure MAC + captive portal authentication, go to the **Network > WLAN > Access** tab of the Aruba Instant UI.

IAP and Client Information Sync Enhancements

This release improves the process to detect and sync the client information between the Virtual Controller and slave IAP that the clients associated with.

IAP Functions Without Uplink

This feature operates in the following scenarios:

- IAP boots up without uplink.
- All the physical uplinks are down after the boot up.

The following table shows the status of the IAP before and after the implementation of this feature.

Table 1 *IAP status before and after this feature*

Scenario	IAP Status Before	IAP Status After
IAP boots up without uplink.	• IAP functions as a mesh point. • IAP tries to boot, but fails.	• IAP functions as a mesh point. • IAP boots up with default IP or static IP and then performs master election and load configuration. Thus IAP can setup a local network for its clients.
All the physical uplinks turn down after the boot up completes.	Clients cannot access internet or local network.	IAP keeps its local network available for the clients.

In both these scenarios IAP functions as mentioned below:

- IAP retries all the physical uplinks in **standalone mode**, **uplink enforced**, or **PPPoE configured** mode. If a physical uplink is up, IAP uses this physical uplink.
- If IAP reboot time (due to an uplink failure) is more than 5 minutes, the IAP boots again except when it is in standalone mode where the **uplink is enforced** and **PPPoE configured**.

Preference to an IAP with 3G/4G Card for Master Election

The Master Election Protocol prefers an Instant AP with 3G/4G card, when electing a Virtual Controller (VC) for the Instant network during initial startup. The VC is selected as follows:

- If there is more than one IAP with 3G/4G cards, one of these is dynamically elected as the VC.

- When an IAP without 3G/4G card is elected as the VC, but is up for less than 5 minutes, another IAP with 3G/4G card in the network will be elected as the VC to replace the previous VC. The VC that is down reboots.
- When an IAP without 3G/4G card is already elected as the VC and is up for more than 5 minutes, the VC will not be replaced until it goes down.

Preference to an IAP with Non-Default IP for Master Election

The Master Election Protocol prefers the Instant AP with a non-default IP, when electing a Virtual Controller (VC) for the Instant network during initial startup. If there is more than one IAP with non-default IP in the network, all IAPs with default IP automatically reboot and the DHCP process is used to assign new IP addresses.

RTLS Enhancement

Real-time Asset Location Server (RTLS) feature is enhanced to send mobile unit reports to the Aeroscout RTLS server for the client stations that are not associated to any IAP (unassociated stations). The Aeroscout RTLS server is now able to locate unassociated stations.

To configure RTLS, go to **Settings > RTLS** in the Instant UI.

GVRP Based VLAN Configuration

This release of Instant supports GARP VLAN Registration Protocol (GVRP). Configuring GVRP in AurbaOS Mobility Access Switch (MAS) enables the switch to dynamically register or de-register VLAN information received from a GVRP applicant such as an IAP. GVRP support also enables the switch to propagate the registered VLAN information to the neighboring switches in the network.

The associated static VLANs used in the wired and wireless profiles are propagated to the upstream MAS using GVRP messages.

RAPNG over HTTP

You can use an HTTP connection instead of an HTTPS when the communication between the RAP next generation (RNG) and IAP is through a VPN. This avoids the overhead of using the HTTPS connection and improves the overall performance.

SNMP Support for Uplink Management Events

This release includes SNMP traps for reporting the 3G/4G uplink changes. The SNMP trap includes five objects as follows:

- **wlsxTrapAPMACAddress**— This object is used to indicate the wired MAC address of an IAP, for which the trap is being raised.
- **wlsxTrapAPPreviousUplinkType**— This object is used to indicate the type of uplink used before the trap is being raised, including:
  - Ethernet
  - 3G/4G
  - PPPoE
  - Wi-Fi Uplink
- **wlsxTrapAPPreviousUplinkActiveTime**— This object is used to indicate the duration for which the previous uplink was used.
- **wlsxTrapAPActiveUplinkType**— This object is used to indicate the type of the current used uplink which is currently used, including:

- Ethernet
- 3G/4G
- PPPoE
- Wi-Fi Uplink

- **wlsxTrapAPUplinkChangeReason**— This object is used to indicate the reason for the change in the uplink configuration. This may be due to the following reasons:
  - Physical link down
  - VPN link down
  - Preemption

Daylight Savings Time Configuration

Instant allows you to enable daylight saving time on IAPs if the time zone you selected supports the daylight saving time. This feature ensures IAPs reflecting the seasonal time changes in the region they serve.

Basic Wired 802.1X Authentication

In previous releases, IAP supported the Captive portal and MAC-authentication wired authentication methods. This version of Aruba Instant introduces a new authentication method, IAP Wired 802.1X for wired clients.

MAC OUI Role Derivation for Open and PSK SSIDs

In a MAC address, the first three octets are known as Organizationally Unique Identifier (OUI), is purchased from the Institute of Electrical and Electronics Engineers, Incorporated (IEEE) Registration Authority. 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.

IAP uses the OUI part of the MAC address to identify device manufacturers and assigns a desired role for users who have completed 802.1X authentication and MAC authentication.

VLAN Pooling

This release of Aruba Instant supports VLAN pooling for wireless clients. VLAN pooling allows a single SSID to be mapped to multiple VLANs wherein each client is randomly assigned a VLAN from a pool of VLANs on the same SSID, thereby automatically partitioning a single broadcast domain of clients into multiple VLANs.

To configure VLAN pooling, go to **New WLAN > WLAN Settings > Static**.

Select **Static** to specify a single VLAN, a comma separated list of VLANs, or a range of VLANs for all clients on the new WLAN network.

Known Issues and Limitations

The following are known issues and limitations in this release of Aruba Instant.

AirGroup

Table 2 *AirGroup Known Issue*

Bug ID	Description
76911	**Symptom:** AirGroup server discovery does not work consistently when there are mesh APs in the topology. **Scenario:** This issue occurs in a Mesh topology when the AirGroup feature is enabled. **Workaround:** Do not enable the AirGroup feature when there are one or more mesh point APs in a deployment.

Authentication

Table 3 *Authentication Known Issue*

Bug ID	Description
75822	**Symptom:** The **Idle-Timeout** value returned by the RADIUS server does not take effect. **Scenario:** This issue occurs when a RADIUS server is used for authentication and the **Idle-Timeout** value is configured on this RADIUS server. **Workaround:** Configure a low **Inactivity-Timeout** value on the IAP.

Mobility

Table 4 *Mobility Known Issues*

Bug ID	Description
74309	**Symptom:** After modifying a distributed Layer-3 subnet to use a new value, the old subnet is not deleted. **Scenario:** This issue occurs when a distributed L3 subnet is modified in the IAP. This issue is found in IAPs running 6.2.0.0-3.2.0.0 version in the distributed L3 network topology. **Workaround:** As both subnet routes point to the same internal IP address, no workaround is required.

Spectrum

Table 5 *Spectrum Known Issues*

Bug ID	Description
74190	**Symptom:** The Spectrum Channel utilization and Quality monitoring page in the Instant UI displays a blank page. **Scenario:** This issue is found when a device in the vicinity of the IAP generated a lot of non-WiFi interference. It is observed on all IAP models supporting spectrum monitoring running Aruba Instant 6.2.0.0-3.2 or above possibly caused in a single AP network. **Workaround:** None

VPN Configuration

Table 6 *VPN Configuration Known Issues*

Bug ID	Description
72166	**Symptom:** The clients in the VPN NAT mode cannot ping large packets—2000, 5000, and 10000 bytes, to the corporate IP address. However, the clients in DL3 mode can ping large packets. **Scenario:** This issue is found in the Virtual Controllers running AurbaOS 6.1.0.0 or later. **Workaround:** None.
76564	**Symptom:** The Generic Routing Encapsulation (GRE) tunnel does not come up after swapping the master and slave IAPs. **Scenario:** This issue was found in IAP-105 running 6.2.0.0-3.2.0.0. This issue occurred when the Per-AP tunnel was configured in an IAP cluster and the tunnel was disabled from slave, followed by the swapping of master and slave IAPs. **Workaround:** Reconfigure the tunnel in the new master and then reboot the master.

Security Limitation

Table 7 *Security Limitation*

Bug ID	Description
64388	**Symptom:** The DHCP offer packets are dropped and do not reach the client, preventing the client from being assigned an IP address. **Scenario:** When multiple WEP-encrypted BSS share the same Tx key ID and have different Tx key values configured, the latest BSS created overrides the others. If any of these BSS are deleted, all other BSS lose the multicast TX key and this results in DHCP offer packets getting dropped. This issue was found in all IAPs running Aruba Instant 6.1.2.3-2.0.0.3. **Workaround:** Use different Tx key IDs for different BSS.

Chapter 3

Features Added in the Previous Releases

This chapter provides a list of the new features included in the previous version of Aruba Instant.

New Features and Enhancements in Aruba Instant 6.1.3.4-3.1

4G LTE Modem Support

Instant AP now supports the use of 4G USB modems to provide internet backhaul to an Aruba Instant network. Previously, Aruba Instant only supported 3G modems. 4G USB modems extend client connectivity to places where an Ethernet uplink is not feasible. This feature enables RAP-3 to automatically choose a network that is available in an area. 4G takes precedence over 3G when RAP-3 tries to auto-select the network.

The 3G and 4G USB modems can be provisioned only on RAP-3.

This release of Aruba Instant supports only the Pantech UML 290 4G card.

To use a UML290 4G modem:

1. Power off the RAP-3.
2. Plug the 4G modem into the USB port of the RAP-3.
3. Power on the RAP-3.

The RAP-3 is designed to automatically recognize the UML290 4G modem. Once recognized, the modem appears under **Settings > Advanced > Uplink** tab. In cases where the modem is not recognized, the modem can be manually configured by selecting the country and ISP settings in the Aruba Instant UI. If the modem used does not belong to any of the countries and ISPs available in the UI drop-down list, you can manually configure the modem by entering low-level settings of the modem individually, under **Settings > Advanced > Uplink > 3G/4G** tab in the Aruba Instant UI.

Mobility Access Switch (MAS) Integration

With this release, the Instant AP can be integrated with a MAS by plugging the AP directly to the MAS port.To enable this integration, go to **Settings > General** and select **Enabled** in the Aruba Instant UI.

For more information on MAS, see the ***ArubaOS 7.1.3 User Guide***.

The two major MAS integration features are as follows:

PoE Prioritization - When an Instant AP is plugged directly into the MAS port, the MAS should increase the PoE priority of the port. This is done only if the PoE priority is set by default in the MAS.

Rogue AP Containment - When a rogue AP is detected by Aruba Instant, it sends the MAC Address of the rogue AP to the MAS. The MAS blacklists the MAC address of the rogue AP and turns off the PoE on the port.

The PoE Prioritization and Rogue AP Containment features will be available for ArubaOS 7.2 release on **Aruba's Mobility Access Switches**.

GRE Tunnel Enhancements

A new parameter, **Per-AP tunnel** is now available while configuring the GRE tunnel. The IAPs can create GRE tunnels from all the APs instead of creating only from the AP that is acting as the Virtual Controller. The traffic going to the corporate is send via the L2 GRE tunnel from the AP itself and does not have to be forwarded through the Virtual Controller. A new parameter, **GRE type** is now available to enable a configurable GRE protocol type.

By default, the **Per-AP tunnel** option is disabled in the Aruba Instant UI.

To configure the **GRE type** parameter, go to **VPN > Tunneling > Controller**, select **GRE** from the **Protocol** drop-down list, and enter the value for GRE type in the **GRE type** text box.

To enable the **Per-AP tunnel** parameter, go to **VPN > Tunneling > Controller** and select **Enabled** from the **Per-AP tunnel** drop-down list.

Disable Provisioning SSID

Aruba Instant now allows you to disable the instant provisioning SSID. This SSID is enabled by default, and can only be disabled or reenabled through an AP console connection. Use the `factory_reset` command to reset an IAP to its factory-default settings, and then use the `setenv disable_prov_ssid 1` and `saveenv` commands to disable the provisioning SSID. To enable the provisioning SSID, use the `factory_reset` command.

DHCP Based Role Derivation

Aruba Instant now allows you to assign user roles based on attributes communicated in the DHCP exchange or 802.1X authentication types. The newly added attributes are:

- DHCP-Option
- 802.1X-Authentication-Type

Video Dynamic Multicast Optimization (DMO)

Aruba Instant now supports Dynamic Multicast Optimization for video. With DMO enabled, the IAP converts multicast traffic into unicast over the wireless link. DMO enhances the quality and reliability of streaming video, while preserving the bandwidth available to non-video clients.

To enable this feature, go to **New WLAN> WLAN Settings > Dynamic multicast optimization**.

For more information on Video DMO, see the Aruba Instant 6.2.0.0-3.2 User Guide.

Multimedia ALG (Facetime, OCS)

Aruba Instant now has the added ability to identify and prioritize voice and video traffic from applications like Microsoft Office Communications Server (OCS) and Apple Facetime.

To configure these settings, go to **PEF > Roles > New > Classify media** in the Aruba Instant UI.

AirWave Primary/Backup

Aruba Instant now allows you to define the IP address of a backup AirWave server in the Aruba Instant UI. The backup server provides connectivity when the primary server is down. If the IAP cannot send data to the primary server, the Virtual Controller switches to the backup server automatically.

To configure this feature, go to **Settings > Admin > AirWave** in the Aruba Instant UI.

Deny Inter User Bridging and Deny Local Routing

- **Deny Inter User Bridging**— This feature allows you to deny traffic between two clients which are directly connected to the same IAP or are on the same Aruba Instant network.
- **Deny Local Routing**— This feature allows you to deny local routing traffic between clients which are connected to the same IAP or are on the same Aruba Instant network.

To enable or disable these features, go to **Settings > General** in the Aruba Instant UI.

DHCP Relay Agent and Option 82

Aruba Instant now includes DHCP Relay Agent and DHCP Option 82 enhancements to the L2 Centralized mode. When a DHCP server is configured with a DHCP Relay agent, the client's Broadcast DHCP Discover packet is not sent to the corporate network, instead the Virtual Controller acts as the DHCP Relay and unicasts DHCP packets to the corporate DHCP server. Enable DHCP Option 82 to allow clients to send DHCP packets with the Option 82 string.

The Option 82 string is available only in the Alcatel (ALU) format. The ALU format for the Option 82 string consists of the following:

- Remote Circuit ID— AP-MAC; SSID; SSID-Type
- Remote Agent— IDUE-MAC

The Option 82 is specific to Alcatel and is not configurable in this version of Aruba Instant.

The following table describes the behavior of the DHCP Relay Agent and Option 82 in the IAP.

Table 1 *DHCP Relay and Option 82*

DHCP Relay	Option 82	Behavior
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 broadcasted with the ALU-specific Option 82 string
Disabled	Disabled	DHCP packet not relayed, but broadcasted without the ALU-specific Option 82 string

To enable these features, go to **VPN > DHCP Server > New** in the Aruba Instant UI.

Enhancements to Internal DHCP Server for Clients

For networks using Virtual Controller IP assignment, the default size of the IP address pool has been increased to 512. You can also customize the DHCP pool's subnet and address range. The largest address pool supported is 2048.

Captive Portal Redirect URL

With this release, users can be redirected to a specific URL (instead of the original URL) after successful captive portal authentication.

To specify the URL, go to **New WLAN > Security > Redirect URL** in the Aruba Instant UI.

Uplink Switching based on VPN Status

Aruba Instant now supports switching uplinks based on the VPN status when deploying mixed uplinks (eth0, 3G, etc). This feature is automatically enabled when a VPN is configured in the IAP.

Image URL Upgrade Support

Aruba Instant now allows you to obtain the image file [(Orion (IAP-105/92/93) and/or Cassiopeia (IAP-134/135)] from a TFTP, FTP and HTTP URL.

To obtain the image file from a TFTP, FTP or HTTP URL, go to **Maintenance > Firmware > Image URL** in the Aruba Instant UI.

The following examples describe the image file format for two different classes of IAPs:

TFTP:

- URL for IAP-135/134: tftp://10.64.147.8/ArubaInstant_Cassiopeia_6.1.3.4-3.1.0.0_xxxx
- URL for IAP-105/92/93: tftp://10.64.147.8/ArubaInstant_Orion_6.1.3.4-3.1.0.0_xxxx

FTP:

- ftp://10.64.147.8/ArubaInstant_Cassiopeia_6.1.3.4-3.1.0.0_xxxx
- ftp://10.64.147.8/ArubaInstant_Orion_6.1.3.4-3.1.0.0_xxxx

HTTP:

- http://10.64.160.42/ArubaInstant_Cassiopeia_6.1.3.4-3.1.0.0_xxxx
- http://10.64.160.42/ArubaInstant_Orion_6.1.3.4-3.1.0.0_xxxx

Wired Bridging on Ethernet 0 of an Instant AP

Aruba Instant now supports wired bridging on the Ethernet 0 port of an Instant AP. Enabling wired bridging on this port of the IAP makes the port available as a downlink wired bridge and allows client access via the port. You can also use the port to connect a wired device when a 3G uplink is used.

To configure this feature, in the Aruba Instant UI, select the IAP in the **Access Point** window. Click on the **edit** link to open the **Edit Access Point** window. The parameter **Eth0 Bridging** is available in the **Uplink** tab.

Reboot the IAP after the bridging is set for the configuration to take effect.

Uplink Management VLAN

Aruba Instant now supports a management VLAN for the uplink traffic on an IAP. After an IAP is provisioned with this parameter, all management traffic sent from the IAP is tagged with the management VLAN.

To configure this feature, in the Aruba Instant UI, select the IAP in the **Access Point** window. Click the **edit** link to open the **Edit Access Point** window. The parameter **Uplink Management VLAN** is available in the **Uplink** tab.

This configuration requires an IAP reboot to take effect.

Instant AP Wired Authentication

Aruba Instant now supports wired authentication on the Ethernet uplink (Ethernet 0) and downlink (Ethernet 1/Ethernet 2) ports of an Instant AP.

Aruba Instant supports the following authentication methods:

- MAC Authentication
- Captive Portal Authentication

To configure wired authentication, click the **Wired** link on the upper right corner of the Aruba Instant UI, then click on the **Network assignments** drop-down lists to apply an existing Ethernet downlink profile to the Ethernet ports.

Configure bridging on the Ethernet uplink (Ethernet 0) port before you apply a profile.

The devices (SIP phone / printer) connected to the wired ports are now authenticated using the profile that is applied to the port. A list of all the wired users is available in the **Wired** window.

Wired authentication does not support WEP, WPA, and WPA2 encryption.

Captive Portal Localization of the Instant AP

Aruba Instant now supports captive portal customization using double-byte characters. Traditional Chinese, Simplified Chinese, and Korean are a few languages that use double-byte characters.

In the Aruba Instant UI, use the **Networks** window to edit an existing SSID for guest access or click on the **New** link to create a new SSID. In the **Security** tab, select the option **Internal-Authenticated** or **Internal-Acknowledged** for the **Splash page type** to display a preview of the splash page for the captive portal. Click on the banner, term, or policy in the splash page preview to modify the text in the red box. This field accepts double-byte characters or a combination of English and double-byte characters.

Layer-3 Mobility

Layer-3 mobility is now supported on Instant AP. This allows a client to roam between APs on the same network but different client subnets, while preserving its IP address and existing data sessions.

To configure the L3 mobility settings, go to **Settings > Advanced > L3 Mobility** in the Aruba Instant UI.

Spectrum Monitor for IAP

Additional modes of operation are now available for an IAP:

- Spectrum Monitor: IAP gathers spectrum data but does not service clients
- Hybrid IAP: The IAP performs spectrum analysis and serves clients

The Aruba Instant UI allows you to view the spectrum data gathered by an IAP such as device list, channel metrics, and channel details. Alerts are sent to the Virtual Controller when a new non Wi-Fi device is found or when a non Wi-Fi device is deleted from the spectrum data.

You can convert an IAP into a spectrum monitor by performing the following steps:

1. In the Aruba Instant UI, select the **Access Point** and click **edit**.
2. In the **Radio** tab, select **Spectrum Monitor** from the **Mode** drop-down list.

You can convert the IAPs in an Aruba Instant network into hybrid IAPs by performing the following steps:

1. Click the **RF** link at the upper right corner of the Instant UI.
2. Click **Show advanced options** to view the **Radio** tab.
3. To enable a spectrum monitor on the 802.11g radio band, in the **2.4 GHz radio** profile, select **Enabled** from the **Background Spectrum Monitoring** drop-down list.
4. To enable a spectrum monitor on the 802.11a radio band, in the **5 GHz radio** profile, select **Enabled** from the **Background Spectrum Monitoring** drop-down list.

The spectrum monitor feature is available only for IAP-104, IAP-105, IAP-134, and IAP-135. The spectrum mode does not work with mesh.

New Options in ACL Configuration

While creating a new ACL rule, in addition to the log and blacklist options, you can now specify the following options in the Aruba Instant UI:

- Disable scanning: Pause ARM scanning on the IAP when a session is flagged with VoIP. This feature takes effect only if **ARM scanning** is enabled from the **ARM** tab of the **RF** page.
- Classify media: Used to prioritize video and voice traffic. When enabled, deep packet inspection is performed on all non-NATed traffic, and the traffic is marked as follows:
  - Video: Priority 5 (Critical)
  - Voice: Priority 6 (Internetwork Control)
- DSCP tag: Value of the DSCP bits marked in the IP header of a packet matching the rule when it leaves the IAP. This tag is used to prioritize traffic. The supported range is 0-63. The higher the value, the higher the priority.
- 802.1p priority: Value of 802.1p priority bits marked in the frame of a packet matching the rule when it leaves the IAP. The supported range is 0-7. The higher the value, the higher the priority.

Hierarchical Mode of Deployment

An IAP can now be connected to the downlink wired port of another IAP (ethX). The upstream IAP has to be an IAP-130 series device or a RAP-3 (which has more than one wired port). For any single Ethernet port platform like, IAP-90 or IAP-100 series devices, you can also provision it to use enet0_bridging, so that eth0 is converted to a downlink wired port. For single Ethernet port platform deployments, the root AP must use the 3G uplink.

Number of SSIDs Supported

The number of SSIDs that you can configure in the IAP has increased. IAP-175 and IAP-100 series devices support up to 8 SSIDs. RAP-3, IAP-90 series, and IAP-130 series devices support up to 16 SSIDs.

To configure, go to **Settings > Advanced > General**, and enable **Extended SSID** in the Aruba Instant UI. Once this option is enabled, the number of SSIDs that are active on each IAP depends on the IAP platform.

This configuration requires an IAP reboot to take effect.

Enabling the Extended SSID option disables the mesh.

PPPoE Support

Aruba Instant now supports PPPoE in both normal IAP and VPN-IAP deployments. In this release, PPPoE supports only single IAP deployments.

To configure the PPPoE settings, go to **Settings > Advanced > Uplink** in the Aruba Instant UI.

This configuration requires an IAP reboot to take effect.

When you use the PPPoE feature do not configure the IP address of the Virtual Controller. Uplink redundancy with the PPPoE link is not supported in this release.

Dynamic Radius Proxy is not supported in a single IAP deployment.

DNS Support for RAP/CAP Conversion

You now have the option to specify a fully qualified domain name of the mobility controller instead of its IP address when converting an IAP to a Campus or Remote AP.

Chapter 4

Known Issues in Previous Releases

This chapter provides a list of the known issues and limitations identified in the previous release of Aruba Instant.

Access Point

Table 1 *Access Point Known Issues*

Bug ID	Description
64338	If two WEP-encrypted SSIDs have more than one BSS sharing the same **Tx key** index value, DHCP offer packets are sometimes dropped, preventing clients from getting an IP address. IAP radios support only four key-cache slots for WEP multicast encryption. When there is an overflow, the last BSS overrides the others and this results in all the other BSS losing the multicast **Tx key**. This issue was observed in IAP-105 (6.1.2.3-2.0.0.3 version).

Mobility

Table 2 *Mobility Limitation*

Bug ID	Description
70212	The Mobility Trail in the home network of the Aruba Instant UI does not show foreign IAP information for clients roaming across L3 boundaries.

Security

Table 3 *Security Limitation*

Bug ID	Description
71508, 75610	DHCP configured in the Mobile Device Access Control (MDAC) environment does not support the configuration of a captive portal. This issue is seen in all Instant AP models running Aruba Instant 6.2.0.0-3.2. **Workaround**: Do not configure the DHCP-option in guest SSID with Captive Portal authentication.