Aruba Instant 6.2.1.0-3.3

Release Notes

Copyright

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. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. 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.

ARUBA
networks

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1

Release Overview

Aruba Instant 6.2.1.0-3.3 is a major software release that introduces new features, enhancements, and fixes to the issues identified in the previous releases.

For more information on features described in the following sections, see the *Aruba Instant 6.2.1.0-3.3 User Guide*.

Contents

- "What's New in this Release" on page 7 lists the new features introduced in this release.
- "Issues Fixed in this Release" on page 15 describes the issues fixed in this release of Aruba Instant.
- "Known Issues and Limitations" on page 17 describes the know issues and limitations identified in this release 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
End of Support information	www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/
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

Chapter 2

What’s New in this Release

This chapter provides a brief summary of the new features introduced in this release of Aruba Instant.

For more information on the features listed in section and the related configuration procedures, see *Aruba Instant 6.2.1.0-3.3 User Guide*.

New Features and Enhancements

Configuration of IAPs Using Instant CLI

In the current release, Instant supports scripting through Command Line Interface (CLI). You can access the Instant CLI through a Secure Shell (SSH).

To enable the SSH access to the Instant CLI, go to **System** > **Show advanced options** and select **Enabled** from the **Terminal access** drop-down list.

When you make configuration changes on a master in the CLI, all associated IAPs in the cluster inherit these changes and subsequently update their configurations. The changes configured in a CLI session are saved in the CLI context. The CLI does not support the configuration data exceeding a buffer size of 4K in a CLI session; therefore, Aruba recommends that you configure fewer changes at a time and apply the changes at regular intervals.

To apply changes at regular intervals, use the following command in the privileged mode:

```
(Instant Access Point)# commit apply
```

Sequence-Sensitive Commands

Instant CLI does not support positioning or precedence of sequence-sensitive commands. Therefore, Aruba recommends 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** command to remove the configuration.

Table 1 *Sequence-Sensitive Commands*

Sequence-Sensitive Command	Corresponding no command
opendns <username <password>	no opendns
rule <dest> <mask> <match> <protocol> <start-port> <end-port> {permit |deny | src-nat | dst-nat {<IPaddress> <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>

Table 1 *Sequence-Sensitive Commands*

Sequence-Sensitive Command	Corresponding no command

`set-role <attribute>{{equals| not-equals| startswith|`
`ends-with| contains} <operator> <role>| valueof}`
	`no set-role <attribute>{{equals| not-equals| starts-with| ends-with|`
	`contains} <operator>| value-of}`
	`no set-role`

`set-vlan <attribute>{{equals| not-equals| startswith|`
`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>`

RAP-155/155P Support

Instant supports RAP-155/155P in the current release. The RAP-155/155P support downlink connection on E1, E2, E3, and E4 ports. The RAP-155P supports PSE for 802.3at powered device (class 0-4) on one port (E1 or E2), or 802.3af powered DC IN (Power Socket) on two ports (E1 and E2).

Instant User Interface (UI) Enhancements

In the current release, the Instant UI is enhanced, and the menu options and configuration windows are reorganized. For more information on the new UI layout and menu categories, see *Aruba Instant 6.2.1.0-3.3 User Guide.*

Spectrum Load Balancing

Spectrum load balancing feature helps optimize network resources by balancing client load across channels and by dividing APs in a cluster into several logical AP RF neighborhood domains, which share the same clients. When the Spectrum load balancing feature is enabled, the Virtual Controller (VC) determines the distribution of clients and balances client load across channels, regardless of whether the AP is responding to the wireless clients' probe requests.

With this feature, the client load for an AP is determined based on the value specified for the SLB threshold. When the client load on an AP reaches or exceeds the SLB threshold in comparison to its neighbors, or if a neighboring AP on another channel does not have any clients, load balancing is enabled on that AP, to allow clients to connect to an available or less loaded channel. When the client count reaches or exceeds the threshold, the APs with load balancing enabled will not send probe response or authentication response to the new client requests.

You can enable spectrum load balancing by using the Instant UI or CLI. For more information, see *Aruba Instant 6.2.1.0-3.3 User Guide.*

WMM Traffic Management

The Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance specification based on the IEEE 802.11e wireless Quality of Service (QoS) standard. You can allocate WMM traffic share for the voice, video, best effort, and background access categories when configuring an SSID profile.

The following parameters can be configured for a WLAN SSID profile:

- **Background WMM share** — Allocates bandwidth for background traffic such as file downloads or print jobs.

- **Best effort WMM share** —Allocates bandwidth for best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS.
- **Video WMM share** —Allocates bandwidth for video traffic generated from video streaming.
- **Voice WMM share** —Allocates bandwidth for voice traffic generated from incoming and outgoing voice communication.

In a non-WMM or hybrid environment, where some clients are not WMM-capable, you can allocate higher values for Best effort WMM share and Voice WMM share to allocate a higher bandwidth to clients transmitting best effort and voice traffic.

You can configure WMM traffic management parameters by using Instant UI or CLI. For more information, see *Aruba Instant 6.2.1.0-3.3 User Guide*.

Role Derivation for Wired Clients

Instant now supports role derivation for wired network profiles. The administrators can configure roles and access rules for the user roles, and assign user roles to determine the network privileges for wired clients. You can also assign a pre-authentication role and enforce MAC authentication only roles for wired clients.

The pre-authentication role is assigned to the users in the following scenarios:

- When the Captive portal authentication fails in a guest wired network that has only the Captive Portal authentication enabled.
- When both MAC authentication and Captive portal authentication fail in a guest network that has both Captive portal and MAC authentication enabled.
- When the 802.1X authentication fails in an employee network that has the 802.1X authentication enabled.

The MAC authentication only role is assigned to the users in the following scenarios:

- When the MAC authentication is successful in a guest wired network that has both Captive portal and MAC authentication enabled.
- When the MAC authentication is successful and if the 802.1X authentication fails in an employee network that has both 802.1X and MAC authentication enabled.

The user roles can be configured by using the Instant UI or CLI.

Reboot After an IAP Upgrade

Instant now allows the users to defer rebooting of the IAP after a software upgrade. The users can choose to reboot the IAP after the upgrade or at a later time by navigating to **Maintenance > Firmware** and selecting or clearing the **Reboot all APs after upgrade** check box or by using the `upgrade-image2-no-reboot <ftp/tftp/http-URL>`. By default, all IAPs reboot after an upgrade.

Configurable SSID Status

The users can now disable an SSID and enable it when required. The disabled SSID is not removed from the network and will be indicated as a disabled SSID. All SSIDs are enabled by default.

You can configure SSID status by using Instant UI or CLI. For more information, see *Aruba Instant 6.2.1.0-3.3 User Guide*.

Broadcasting of Instant SSID Based on AirWave and Activate Availability

The IAPs boot with factory default configuration and will 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.

Read-Only Access to the Instant UI When AirWave is in the Management Mode

In the AirWave User Interface (UI), you can select either **Manage Read/Write** or M**onitoronly+Firmware Upgrades** as management modes. When the Management level is set to **Manage Read/Write**, the Instant UI is in the read-only mode. If Airwave Management Level is set to **Monitoronly**+**Firmware Upgrades** mode, the Instant UI changes to the read-write mode.

IAP-VPN Enhancements

Instant allows you to configure the DHCP address assignment modes for the branches connected to the corporate network through VPN. You can configure the range of DHCP 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.

You can configure Distributed, L2, Distributed, L3, Local, Local-L3 (NAT and L3 switching), and Centralized, L2 DHCP scopes and vendor-specific DHCP options for the DHCP scopes.

NOTE

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 IAP does not allow the administrators to assign the remaining IP addresses to another branch, although a lower value is configured for the client count.

The Instant UI is enhanced to provide a easy and flexible workflow for configuration and the **`show iap table`** command available on the controller now displays the branch name, ID, and subnet details. For more information on configuring DHCP scopes, see *Aruba Instant 6.2.1.0-3.3 User Guide*.

Support for Dual Ethernet Uplinks

Instant supports configuration of dual Ethernet uplinks for wired profiles. When the primary uplink on an existing Ethernet port fails, the IAP switches over to the uplink available on an alternate physical port. You can also set a priority for uplinks, so that the IAP can switch over to a higher priority uplink when required. By default, the Eth0 uplink is set as a high priority uplink.

Ethernet VLAN Assignment and VLAN Derivation

In the current release, the Virtual Controller can assign a guest VLAN for a wired network profile. You can also assign VLANs for wired clients based on the user roles configured wired network profile.

You can assign VLANs and configure VLAN derivation rules by using Instant UI or CLI. For more information, see *Aruba Instant 6.2.1.0-3.3 User Guide*.

VLAN Derivation Based on DHCP Option

You can now configure VLAN derivation rules based on a DHCP option. The **dhcp-option** is available in the list of attributes in the **New VLAN Assignment Rule** window. You can also configure VLAN derivation rules based on DHCP option for Captive portal authentication. When the Captive portal authentication is successful, the role derivation based on DHCP option assigns a new user role to the guest users, instead of the pre-authenticated role.

Protection from ARPs Attack

Instant allows you to enable firewall settings to protect against wired attacks, such as ARP attacks or malformed DHCP packets, and notify the administrator when these attacks are detected.

Captive Portal Enhancements

Access to the Internet When the External Captive Portal Server is Not Available

This feature allows the guest users to access the Internet when the external Captive portal is not available. When the external Captive portal is not available, the guest users are redirected to the URL specified in the SSID profile.

Configurable Accounting Modes for Guest Users

This feature allows you to configure the accounting mode for guest users to determine when to start and stop accounting for a captive portal SSID. 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.

Disable Captive Portal Authentication based on the Current Uplink Type

This feature allows you to disable redirection to the Captive portal based on the type of current uplink. The disable uplink option is available for both internal and external Captive portal splash pages.

8021X Authentication with Captive Portal Role

Instant now supports the configuration of access rules to enforce Captive portal authentication for an SSID that has 802.1X authentication enabled. You can configure rules to provide access to external Captive portal, internal Captive portal, or none, 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-acknowledged** and **External Authentication Text** splash page types.

Automatic Whitelisting of URLs

You can now enable or disable automatic whitelisting of the URLs when setting up a guest network by using the Instant UI or CLI. The **Automatic URL Whitelisting** check box is introduced in the **External-RADIUS Authentication** and **External Authentication Text** splash pages in the Instant UI to allow the users to enable or disable this feature.

On selecting the check box for the external Captive portal authentication, the URLs that the unauthenticated users are allowed to access are automatically whitelisted. In the current release, the automatic URL whitelisting is disabled by default.

You can also enable or disable the automatic whitelisting of URLs by using Instant CLI:

To disable automatic whitelisting of URLs:

```
auto-whitelist-disable
```

To re-enable automatic whitelisting of URLs:

```
no auto-whitelist-disable
```

Configurable VLAN for the Virtual Controller IP

Instant supports assigning a VLAN for the Virtual Controller (VC). You can configure the VC IP, VLAN, Mask, and Gateway. When the VC VLAN is not configured, the VC IP is configured with the default mask. When a new VLAN, mask and gateway are assigned, the VC IP is updated with the new mask configured.

Support for 512 User Entries in the Local User Database of IAPs

The local user database of APs can support up to 512 user entries except IAP-9x. IAP-9x supports only 256 user entries. If there are already 512 users, IAP-9x will not be able to join the cluster.

Support for Configuring Hotspot Profiles

Hotspot 2.0 is a Wi-Fi Alliance 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. The 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, Generic Advertisement Service (GAS) and Access Network Query Protocol (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.This feature supports the configuration hotspot profiles for a WLAN SSID profile.

A hotspot profile contains one or several advertisement profiles. You can configure the following advertisement profiles through the Instant CLI:

- NAI Realm profile
- Venue Name Profile
- Network Auth Profile
- Roaming Consortium Profile
- 3GPP Profile
- IP Address availability Profile
- Domain Name Profile
- Operator Friendly Name Profile
- Connection Capability Profile
- Operating Class Profile
- WAN Metrics Profile

NOTE

In the current release, Instant supports the hotspot profile configuration only through the CLI.

You can configure a hotspot profile and associate the advertisement profiles to use for a hotspot network connection or setup. The hotspot profile can be enabled on one or more SSID profile by creating a reference in the WLAN SSID profile.

Support for Policy Based Corporate Access and Source Based Routing

You can configure a policy based corporate access for client traffic in Instant. For example, you can configure an IAP to send all traffic on an SSID to the corporate network, while another SSID can be configured with direct access to the Internet for some services, protocols, or destinations.

You can also configure source based routing for client traffic by allowing traffic on one SSID to reach the Internet through a corporate network and another SSID to use an alternate uplink.

AirGroup Enhancements

AirGroup now enables a client to perform a location-based discovery. For example, when a client roams from one IAP cluster to another, it can discover devices available in the new cluster to which the client is currently connected.

The AirGroup users can also configure Bonjour Services in the guest VLAN. When enabled, the Bonjour devices are visible only in the guest VLAN and AirGroup will not discover or enforce policies in guest VLAN.

Support for SNMP Standard Tables

Instant now supports the standard SNMP IF-MIB and Q-BRIDGE MIB tables, and System MIB objects. The aiRadioTable and aiAccessPointTable are also enhanced to include objects to indicate the IAP status, memory, and the radio status of an IAP. For more information on the SNMP MIB objects and Instant MIB enhancements, see *Aruba Instant 6.2.1.0-3.3 MIB Reference Guide*.

The following issues from the previous releases are fixed in the current Aruba Instant release.

Issues Fixed in this Release

Authentication

Table 1 *Authentication Fixed Issue*

Bug ID	Description
75822	**Symptom:** The idle timeout value set on the RADIUS server could not take effect on an IAP. Changes to the control path have resolved this issue. **Scenario:** This issue occurred when different values for the idle timeout were configured on the RADIUS server and the IAP. This issue was found in IAPs running Aruba Instant 6.2.0.0-3.2.

VPN Configuration

Table 2 *VPN Configuration Fixed Issue*

Bug ID	Description
72166	**Symptom:** The clients in the VPN NAT mode could not ping large packets of data to the corporate IP address. Changes to the code base have resolved this issue. **Scenario:** This issue was not limited to a specific IAP model or Aruba Instant version.

Chapter 4

Known Issues and Limitations

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

Known Issues and Limitations in this Release

3G/4G

Table 1 *3G/4G Limitation*

Bug ID	Description
81329 83132	**Symptom:** RAP-108/109 and RAP-155 do not support the Sprint 3G/4G USB U600 driver. **Scenario:** This issue is found in RAP-108/109 and RAP-155 running ArubaOS 6.3.0.0. **Workaround:** None

SNMP

Table 2 *SNMP Known Issues*

Bug ID	Description
82353	**Symptom:** IAP-135 and RAP-108/109 display incorrect multicast packet counters. **Scenario:** This issue occurs when multicast traffic flows across the IAPs. This issue is found in IAP-135 and RAP-108/109 running Aruba Instant 6.2.1.0-3.3. **Workaround:** None
82752	**Symptom**: The value for the SNMP aiRadioPhyEvents counter is always displayed as **0**. **Scenario**: This issue is found in IAPs running Aruba Instant 6.2.1.0-3.3. **Workaround:** None
82637	**Symptom:** The SNMP ifTable entry does not match the SNMP traps generated for the GRE creation and deletion events. **Scenario:** This issue occurs when the GRE interface is configured or deleted from the IAP and is found in IAPs running Aruba Instant 6.2.1.0-3.3. **Workaround:** None

VLAN Configuration

Table 3 *VLAN Configuration Known Issues and Limitations*

Bug ID	Description
75496	**Symptom:** A slave IAP cannot connect to the master IAP when reconnecting to the network. **Scenario:** This issue occurs when the Ethernet uplink fails and switches over to another available uplink. This issue was observed in a hierarchical network topology when the native VLAN on a wired port was set to a value that is not equal to 1. This issue is found in IAPs running Aruba Instant version 6.2.0.0-3.2 or later. **Workaround:** None

Table 3 *VLAN Configuration Known Issues and Limitations*

Bug ID	Description
80849	**Symptom:** In a hierarchical topology, although the clients can obtain an IP address, the Virtual Controller Gateway IP address resolution fails. **Scenario:** This issue occurs when the master IAP assigns a guest VLAN IP address to the client. As the DHCP scope configuration on the slave IAP uses a different subnet, the Virtual Controller gateway IP address cannot be resolved. This issue is found in IAPs running Aruba Instant 6.2.1.0-3.3. **Workaround:** Manually configure the DHCP pool to ensure that the appropriate subnet is used for assigning IP addresses to the clients.
82754	**Symptom:** A client roaming from a slave IAP to the master IAP cannot access the Internet. **Scenario:** This issue occurs when a client, which is assigned an IP address from the local DHCP server, roams to the master IAP. This issue occurs because the IAPs do not support the combination of dynamic VLAN derivation and local DHCP pool. This issue is found in IAPs running Aruba Instant 6.2.1.0-3.3. **Workaround:** None