ArubaOS 6.3.0.1

ARUBA networks

Release Notes

Copyright Information

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 fro 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.

ArubaOS 6.3.0.1 is a software patch release that introduces fixes to the issues identified in the previous releases. For details on the features described in the following sections, see the *ArubaOS 6.3 User Guide*, *ArubaOS 6.3 CLI Reference Guide*, and *ArubaOS 6.3 MIB Reference Guide*.

NOTE

See the Upgrade Procedures on page 64 for instructions on how to upgrade your controller to this release.

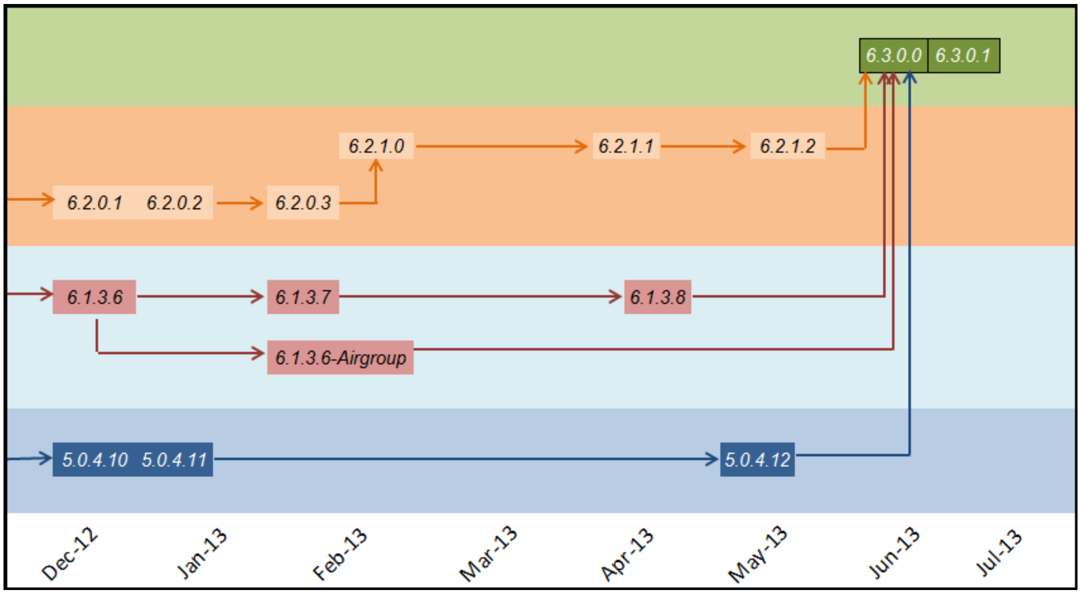
Chapter Overview

- What's New in this Release on page 12 describes the new fixes, known issues, and enhancements introduced in this release.
- Features Added in Previous 6.3 Releases on page 17 provides description of features and enhancements added in ArubaOS 6.3.
- Resolved Issues from Previous Releases on page 43 lists issues fixed in ArubaOS 6.3.
- Known Issues and Limitations on page 57 provides description and workaround for the outstanding issues in ArubaOS 6.3.
- Upgrade Procedures on page 64 covers the procedures for upgrading a controller to ArubaOS 6.3.

Release Mapping

The following illustration shows the patch and maintenance releases that are included in their entirety in ArubaOS 6.3.0.1:

Figure 1 *ArubaOS Releases and Code Stream Integration*



Supported Browsers

The following browsers are officially supported for use with the ArubaOS 6.3.0.1 WebUI:

- Microsoft Internet Explorer 9.x and 10.x on Windows XP, Windows Vista, Windows 7, and Windows 8
- Mozilla Firefox 17 or higher on Windows XP, Windows Vista, Windows 7, and MacOS
- Apple Safari 5.1.7 or higher on MacOS

Contacting Support

Table 1: *Contact Information*

Website Support	
Main Site	http://www.arubanetworks.com
Support Site	https://support.arubanetworks.com
Airheads Social Forums and Knowledge Base	http://community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	http://www.arubanetworks.com/support-services/aruba-support-program/contact-support/
Support Email Addresses	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
Wireless Security Incident Response Team (WSIRT)	wsirt@arubanetworks.com

This chapter lists the regulatory updates, resolved issues, and known issues in ArubaOS 6.3.0.1.

Regulatory Updates

The following table describes regulatory enhancements introduced in ArubaOS 6.3.0.1.

NOTE

Contact your local Dell sales representative on device availability and support for the countries listed in the following table.

Table 2: *Regulatory Domain Updates*

Regulatory Domain	Change
Colombia, Macedonia, Brazil	Added support for RAP-3WN and RAP-3WNP
Ukraine	Added support for AP-175P
Venezuela	Added support for AP-175AC
Canada	Opened DFS channels for AP-175P/AC/DC
Trinidad and Tobago	Added support for AP-135, AP-135P, and AP-175P
Uganda, Brazil, Malaysia	Added support for AP-175AC
Singapore, Dominican Republic, Puerto Rico, Hong Kong, Japan	Added support for AP-224 and AP-225

Resolved Issues

The following issues are resolved in ArubaOS 6.3.0.1:

AP–Wireless

Table 3: *AP–Wireless Fixed Issues*

Bug ID	Description
80426 77834 81672 85186 85381 85396 85400 85658 85713 85186 86821	**Symptom:** An Access Point (AP) crashed and rebooted frequently and the log files for the event listed the reason for the crash as **kernel panic**. **Scenario:** This issue occurred in Remote AP (RAP) or Campus AP (CAP) with CPsec enabled, when the VPN tunnel terminated and re-established with traffic on the tunnel. This issue was observed in AP-134, AP-135, and RAP-155 models.
85806	**Symptom:** Excessive jitter was observed in Blackberry devices for voice calls when the Wireless Multimedia UAPSD (Unscheduled Automatic Power Save Delivery) option from the **Configuration** > **Wireless** > **AP Configuration** > **Select AP** > **SSID profile** > **Advanced** tab from the WebUI was enabled. This issue is fixed in ArubaOS 6.2.1.3 by enhancing the packet queuing mechanism for UAPSD hardware transmit queues to reduce the packet loss. **Scenario:** This issue was triggered by high packet loss in a UAPSD enabled configuration. This issue was observed in AP-125, AP-105, and AP-124 models running ArubaOS 6.1.3.6.

Base OS Security

Table 4: *Base OS Security Fixed Issues*

Bug ID	Description
72093	**Symptom**: A controller dropped a portion of the **show run** command output when it is sent using ssh/telnet connections with teraterm client. An increase in the socket buffer size resolved this issue. **Scenario**: This issue was observed in the teraterm client in ArubaOS 6.3.
83776 50984	**Symptom**: Atheros clients did not support multiple relay counters using Wi-Fi Protected Access - Temporal Key Integrity Protocol (WPA-TKIP) encryption and was unable to connect to the network, after upgrading to ArubaOS 6.1.3.7. This issue is fixed by disabling use of multiple Traffic Identifier (TID) for WPA-TKIP. **Scenario**: This issue was observed when Wireless Multimedia Extensions (WMM) was enabled and Atheros clients did not support multiple relay counters.
85471	**Symptom:** When multiple IPsec tunnels using a specific encryption method (AES256 and AES128) sent data on FIPS 7200 Series controllers it triggered a datapath crash. This issue is fixed in ArubaOS 6.3.0.1. **Scenario**: Multiple simultaneous tunnels using AES encryption may trigger the crash. This issue occurred on 7200 Series controllers that run ArubaOS 6.3-FIPS. Non-FIPS, M3, 3000 Series, and 600 Series FIPS platforms are not affected.
85688	**Symptom**: The Virtual Intranet Access VPN (VIA-VPN) Authentication using RSA SecureID was not functioning for both **New PIN** and **Next Tokencode** modes. This issue was resolved by making changes to the code that maintains the state of radius exchange. **Scenario**: This issue was observed in ArubaOS 6.3.0.0 while performing VIA-VPN authentication with a RSA server using RSA SecureID.

Mobility

Table 5: *Mobility Fixed Issues*

Bug ID	Description
85366	**Symptom**: After an inter controller roaming, dual stacked wireless client's IPv6 traffic flow stopped after few seconds due to IPv6 neighbor resolution failure, but IPv4 traffic continued to flow. This issue is resolved by proper handling of Neighbor Solicitation (NS) from the roamed client at the home agent (HA). **Scenario**: The neighbor solicitation (NS) packets received at home agent (HA) from the roamed client over L2-GRE mobility tunnels were not handled properly in certain cases leading to loss of the received NS packets. This issue was observed when two wireless clients roamed within the same IP subnet and the L3 mobility and IPv6 features were enabled on the controller.

Startup Wizard

Table 6: *Startup Wizard Fixed Issues*

Bug ID	Description
85312	**Symptom:** An error message **Error: Very high throughput must be enabled to enable 80 MHz channel usage** appeared on the **Finish** page of the Campus WLAN wizard. This issue was resolved by enabling the throughput before enabling 40MHz and 80MHz, and disabling 80MHz and 40MHz, before disabling the throughput. **Scenario:** This error occured when a WLAN is configured with a, a+n, b/g, or b/g+n radio types.
85573	**Symptom:** An error message was displayed on the **Finish** page of the **Controller Wizard** when trying to configure a Dynamic Host Configuration Protocol (DHCP) pool that exceeds the maximum configurable address of a platform. The validation did not occur on the **VLAN and IP Interfaces** page. To resolve this issue, the sum of the configured addresses and the addresses are calculated, if it is greater than the maximum number of addresses, a validation message is displayed. **Scenario:** This issue occured on any controller running ArubaOS 6.3.

Switch-Platform

Table 7: *Switch Platform Fixed Issues*

Bug ID	Description
81555 81014 80956 83239	**Symptom**: A controller crashed and rebooted after upgrading the software from ArubaOS 6.1.3.6 to ArubaOS 6.1.3.7. The log files for the event listed the reason for the crash as **watchdog timeout**. The interrupt handler for packet parsing was modified to ensure that CPU was not overwhelmed with the traffic packets. **Scenario**: In a high traffic deployment, a race condition triggered the controller crash and this issue was not specific to any controller models.

UI Monitoring

Table 8: *UI Monitoring Fixed Issues*

Bug ID	Description
85784 76383	**Symptom**: The **Dashboard** > **Security** page of the WebUI was not loaded in Microsoft IE 8 (Internet Explorer) or lower versions and displayed a JavaScript error. This issue is fixed in ArubaOS 6.2.1.3 for all the browsers. **Scenario**: This issue was triggered by JSON (JavaScript Object Notation) parser in IE. This issue was observed in ArubaOS 6.2.1.2 and not specific to any controller or release version.

WMM

Table 9: *WMM Fixed Issues*

Bug ID	Description
68503 68162 74323 81953 83518 83978 85818	**Symptom**: When the same Differentiated Service Code Point (DSCP) value is mapped to two different access categories, the lower of the two is used for the downstream traffic. This issue was resolved, by mapping the higher value to the downstream traffic. **Scenario**: This issue was observed on controllers running ArubaOS 6.2 or lower in Tunnel and D-Tunnel modes.

Known Issues

The following issues have been identified since the last release. For a list of known issues found in previous versions of ArubaOS, see Known Issues and Limitations.

ARM

Table 10: *ARM Known Issues*

Bug ID	Description
87026	**Symptom:** The mode-aware Adaptive Radio Management (ARM) turned off more APs in G band and APs were turned into AP Air Monitors (APMs) in a high density deployment. This issue is found when two-hop neighbor of an AP is associated with more than one Virtual AP (VAP). **Scenario:** This issue was triggered when a radio was associated to multiple VAPs, the Signal-to-Noise Ratio (SNR) of the radio was counted many times when the neighbor's view of the coverage index was calculated. This issue was observed in ArubaOS 6.2.1.2 and is not specific to any AP or controller model. **Workaround:** Disable the OTA ARM update using the **rf arm-profile** command in **ARM** profile to avoid this issue.

Switch Platform

Table 11: *Switch Platform Known Issues*

Bug ID	Description

85685	**Symptom:** The FPAPPS process crashes when there is a severe interface, VLAN, and VRRP flapping.
	Scenario: Set the VLAN status **UP** statically by adding the following command at the interface level on all VLANs:
	`(host) (config) #interface vlan 1001`
	`(host) (config-subif)#operstate up`
	Workaround: None.

Features Added in Previous 6.3 Releases

The following features were added in ArubaOS 6.3:

Level of Support Per Feature lists new features that are fully supported in ArubaOS 6.3 release.

Table 12: *Level of Support Per Feature*

Feature	Level of Support
● 802.11ac ● Client Match (ARM 3.0) ● AirGroup ● AP - AP-220 Series - RAP-155/155P ● Serviceability Enhancement - AP Serviceability - Controller Serviceability ● IAP-VPN Scaling ● Centralized Licensing ● AP Fast Failover	Fully Supported
All other new features	Beta Quality

Features Not Supported Per Platform lists features that are considered beta-quality in the ArubaOS 6.3 release. These features may be supported in a future release.

Table 13: *Features Not Supported Per Platform*

Platform	Features Not Supported
AP-220 Series Access Point	● A-MSDU Rx in Tunnel Mode and Spectrum ● Cell Size Reduction ● Crypto Offload Optimization ● Ethernet Link Aggregation ● Jumbo Frames ● MESH ● Per VAP STBC Control ● Packet Capture Raw Mode support ● RAP Mode ● TurboQAM
RAP-155 and RAP-155P	● Jumbo Frames ● Spectrum
600 Series Controller	● AirGroup ● AppRF ● IF-MAP ● IAP-VPN
650, 3200, 3400 controllers	● AP Image Preload
All Controller Models	● RF Plan/Locate

Supported IPv6 Address Range

As per Internet Assigned Numbers Authority (IANA), Aruba controllers support the following ranges of IPv6 addresses:

- Global unicast–2000::/3
- Unique local unicast–fc00::/7
- Link local unicast–fe80::/10

Upgrading to ArubaOS 6.3.0.1

Memory Requirements

All Aruba controllers store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the controller. Loading multiple large files can consume flash space quickly. To maintain the reliability of your WLAN network, Aruba recommends the following compact memory best practices:

- Issue the **show memory** command to confirm that there is at least 40 MB of free memory available for an upgrade using the CLI, or at least 60 MB of free memory available for an upgrade using the WebUI. Do not proceed unless this much free memory is available. To recover memory, reboot the controller. After the controller comes up, upgrade immediately.
- Issue the **show storage** command to confirm that there is at least 60 MB of flash available for an upgrade using the CLI, or at least 75 MB of flash available for an upgrade using the WebUI.

CAUTION

In certain situations, a reboot or a shutdown could cause the controller to lose the information stored in its compact flash card. To avoid such issues, it is recommended that you issue the **halt** command before power cycling.

If the output of the **show storage** command indicates that insufficient flash memory space is available, you must free up additional memory. Any controller logs. crash data or and flash backups should be copied to a location off the controller, then deleted from the controller to free up flash space. You can delete the following files from the controller to free memory before upgrading:

- **Crash Data:** Issue the **tar crash** command to compress crash files to a file named **crash.tar**.
- **Flash Backups:** Back up critical data in the flash directory to a file named **flash.tar.gz**, then issue the command **tar clean flash** to delete the file from the controller.
- **Log files:** Issue the **tar logs** command to compress log files to a file named **logs.tar**. Copy the **logs.tar** file to an external server, then issue the command **tar clean logs** to delete the file from the controller.

Upgrading to ArubaOS 6.3 with Airwave

For ArubaOS 6.3, you must use AMP Server version 7.7.

Upgrading the 600 Series Controllers to ArubaOS 6.3.0.1.

Customers upgrading the 600 Series controllers must note the following:

- The local file upgrade option in the WebUI does not work when upgrading the W-600 Series controller.Use other upgrade options. See bug ID 77542 in Table 65 for details.
- Upon upgrading to ArubaOS 6.3, the internal AP of the 651 controller will be disabled. The 651 will appear as 650 in ArubaOS and function as 650.
- Ensure that memory and flash requirements are met before starting the upgrade process. See section Memory Requirements on page 66 for details.

- User scalability on both the 620 controller and the 650 controller has been revised down to 128 and 150 users, respectively.
- The following ArubaOS 6.3 features are not supported on the 600 Series controllers.
  - AppRF

CAUTION

For information about AppRF feature, see the "Firewall" section of the "Dashboard Monitoring" chapter in *ArubaOS 6.3 User Guide*.

  - AirGroup
  - ClearPass Profiling with IF-MAP
  - IAP-VPN

Adaptive Radio Management (ARM)

Client Match

The ARM client match feature continually monitors a client's RF neighborhood to provide ongoing client bandsteering and load balancing, and enhanced AP reassignment for roaming mobile clients. This feature is recommended over the legacy bandsteering and spectrum load balancing features, which, unlike client match, do not trigger AP changes for clients already associated to an AP.

When this feature is enabled on an AP, that AP is responsible for measuring the RF health of its associated clients. The AP receives and collects information about clients in its neighborhood, and periodically sends this information to the controller. The controller aggregates information it receives from all APs using client match, and maintains information for all associated clients in a database. The controller shares this database with the APs (for their associated clients) and the APs use the information to compute the client-based RF neighborhood and determine which APs should be considered candidate APs for each client. When the controller receives a client steer request from an AP, the controller identifies the optimal AP candidate and manages the client’s relocation to the desired radio. This is an improvement from previous releases, where the ARM feature was managed exclusively by APs, without the larger perspective of the client's RF neighborhood.

The following client/AP mismatch conditions are managed by the client match feature:

- **Load Balancing:** Client match balances clients across APs on different channels, based upon the client load on the APs and the SNR levels the client detects from an underutilized AP. If an AP radio can support additional clients, the AP participates in client match load balancing and clients can be directed to that AP radio, subject to predefined SNR thresholds.
- **Sticky Clients:** The client match feature also helps mobile clients that tend to stay associated to an AP despite low signal levels. APs using client match continually monitor the client's RSSI as it roams between APs, and move the client to an AP when a better radio match can be found. This prevents mobile clients from remaining associated to an APs with less than ideal RSSI, which can cause poor connectivity and reduce performance for other clients associated with that AP.
- **Steering/Band Balancing**: 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 AP detects that the client has a good RSSI from the 5 GHz radio, the controller will attempt to steer 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 AP retains a suitable distribution of clients on each of its radios. The client match feature is enabled through the AP's 802.11a and 802.11g RF Management Profiles. Although default client match settings are recommended for most users, advanced client match settings can be configured using the rf dot11a-radio-profile and rf dot11g-radio-profile commands in the command-line interface.

NOTE

The client match feature is enabled through the AP's 802.11a and 802.11g RF Management Profiles. Although default client match settings are recommended for most users, advanced client match settings can be configured using the rf arm-profile commands in the command-line interface.

Support for New 802.11 Standards - 802.11r/v

Support for 802.11r Standard

ArubaOS provides support for Fast BSS Transition as part of the 802.11r implementation. Fast BSS Transition mechanism minimizes the delay when a client transitions from one BSS to another within the same ESS. Fast BSS Transition establishes security and QoS states at the target AP before or during a re-association. This minimizes the time required to resume data connectivity when a BSS transition happens. For more information on configuring Fast BSS Transition, see *ArubaOS 6.3 User Guide*.

802.11v Support

ArubaOS provides support for BSS Transition Management which is part of the 802.11v implementation. BSS Transition Management enables an AP to request a voice client to transition to a specific AP, or suggest a set of preferred APs to a voice client, due to network load balancing or BSS termination. This helps the voice client to choose an AP for transition that provides the best service as it roams.

Interaction between 802.11k and 802.11v clients

For 802.11k capable clients, the client management framework uses the actual beacon report generated by the client in response to a beacon report request sent by the AP. This beacon report replaces the virtual beacon report for that client.

For 802.11v capable clients, the controller uses the 802.11v BSS Transition message to steer clients to the desired AP upon receiving a client steer trigger from the AP.

Channel Quality Aware Adaptive Radio Management

This release of ArubaOS provides support for Channel Quality Aware in ARM. The channel quality is measured based on the channel utilization. Channel Quality Aware enables ARM to select channels for the APs based on the channel quality. When the channel quality of an AP goes down and remains below the threshold value for a specified wait time, the ARM moves the AP to a better channel. For more information on configuring Channel Quality Aware, see *ArubaOS 6.3 User Guide*.

AP Platform

This section describes AP Platform features added in this release.

Support for the RAP-155

The RAP-155 and RAP-155P are dual-radio, dual-band wireless AP that offer wired and wireless network access, zero-touch provisioning, identity-based access control, policy based forwarding, air monitoring, and wireless intrusion protection across the 2.4 GHz and 5 GHz (802.11a/b/g and 802.11n) bands.

The RAP-155 and RAP-155P ship with the Aruba Instant software. Therefore, out of the box, the RAP-155 and RAP-155P operate as a Virtual Controller (VC) or an Instant AP. However, the RAP-155 and RAP-155P can be converted to operate as a Remote AP (RAP).

Support for the AP-220 Series

NOTE

On the AP-220 Series, regardless of what is configured on the controller, the DTIM value for all Virtual APs (VAP) is set to three (3).

NOTE

For this release, the AP-220 Series has a basic rate of 5.5 mbps set for 802.11g. However, this is not reflected in the output of commands such as **show configuration**.

NOTE

In ArubaOS 6.3, the MPDU Aggregation option under the HT SSID Profile does not affect the AP-220 Series AP. This means that aggregation is always enabled on the AP-220 Series and disabling the MPDU Aggregation option will have no effect. If you need to disable aggregation, you must disable High Throughput and Very High Throughput in the 802.11a and 802.11g radio profiles under RF Management.

The new AP-220 Series of access points support 802.11ac on the 5 GHz band using 80 MHz channels. The following new features and configuration parameters have been introduced to support configuration of Very High Throughput (VHT) settings.

Table 14: *WLAN HT-SSID Profile Settings for VHT*

Parameter	Description
80MHz-enable	Enables or disables the use of 80 MHz channels on Very High Throughput (VHT) APs.
very-high-throughput-enable	Enable/Disable support for Very High Throughput (802.11ac)on the SSID. Default: Enabled
vht-supported-mcs-map	Modulation Coding Scheme (MCS) values or ranges of values for spatial streams 1 through 3. Valid values for the maximum MCS settings are 7, 8, 9 or a dash (-) if a spatial stream is not supported. If a MCS is not valid for a particular combination of bandwidth and number of spatial streams, it will not be used. Default: 9,9,9
vht-txbf-explicit-enable	Enable or disable VHT Explicit Transmit Beamforming. When this feature is enabled, the AP requests information about the MIMO channel and uses that information to transmit data over multiple transmit streams using a calculated steering matrix. The result is higher throughput due to improved signal at the beamformee (the receiving client). If this setting is disabled, all other transmit beamforming settings will not take effect. Default: Enabled
vht-txbf-sounding-interval	Time interval in seconds between channel information updates between the AP and the beamformee client. Default 25 seconds

RF 802.11a/g Radio Profiles

The following parameters were added to the RF 802.11a radio profile:

Table 15: *802.11a Radio Settings for VHT*

Parameter	Description
very-high-throughput-enable	Enable/Disable support for Very High Throughput (802.11ac) on the radio. Default: Enabled

RF ARM Profile Changes

The following parameter was added to the RF ARM profile:

Table 16: *RF ARM Settings for VHT*

Parameter	Description
80MHz-support	If enabled, this feature allows ARM to assign 80 MHz channels on APs that support VHT. Default: Enabled

Regulatory Domain Profile Changes

The following parameters was added to the regulatory domain profile:

Table 17: *Regulatory Domain Settings for VHT*

Parameter	Description
valid-11a-80mhz-channel-group	This parameter defines which 80MHz channels on the "a" band are available for assignment by ARM and for controller to randomly assign if user has not specified a channel. The channel numbers below correspond to channel center frequency. ● Possible choices in US: 42, 58, 106, 122, 138, 155 ● Possible choices in EU: 42, 58, 106, 122 ● Possible choices in JP: 42, 58, 106, 122 ● Possible choices global: 42, 58, 106, 122, 138, 155

Define RTLS and Aeroscout Servers by Domain Name

In the previous versions of ArubaOS, you could define the Real-time locating systems (RTLS) and Aeroscout servers only by their IP address. This release of ArubaOS allows you to define the RTLS and Aeroscout servers by their domain name as well. The **ip-addr** field in the RTLS and Aeroscout configuration command has now been changed to **ip-or-dns**.

Spanning Tree Support on AP-93H and Multi-Port Remote APs

Starting from ArubaOS 6.3.0.1, the mobility controller supports Spanning Tree Protocol (STP) on AP-93H and multi-port Remote APs. This feature is an enhancement to the existing STP and supports APs with 3 or more ports. Now, you can enable or disable STP on ap-system profile and ap-wired port profile.

NOTE

STP is enabled only on wired ports of an AP. STP works only on downlink ports (eth1-<n>).

Sign-On for Airwave and Controller WebUI

This feature provides a simplified way of connecting to all controllers managed by Airwave Management Platform (AMP). AMP authorized users only need to logon once to the AMP WebUI to gain access to the this WebUI.

1. Go to the Airwave Management Platform WebUI.
2. Navigate to **AMP Setup > Authentication > Single Sign-on**.
3. Click the **Yes** button and click **Save**.

AP Serviceability Enhancements

The following enhancements have been added to improve AP troubleshooting, and should be used under the supervision of Aruba Technical Support.

- **Client Activity Statistics**: Use the **show ap client trail-info** command to view client activity, including reasons for client deauthentication, the history of how that client moved between different APs, and any alerts or errors encountered.

- **Throughput tests**: Iperf throughput tests can be run between the AP-105, AP-130 Series or AP-220 Series access points and M3 or 3000 Series controllers, using the **ap perf-test client | server** commands. Test results can be displayed in the CLI using the command **show perf-test reports**. For more information on configuring and running Iperf throughput tests, refer to the What's New section of the ArubaOS *6.3 CLI Reference Guide*.
- **Client Packet Tracing**: Use the **ap debug client-trace start** and **ap debug client-trace stop** commands to start or stop tracking management packets from a client MAC address. Client tracing information gathered using this command can be displayed in the output of the command **show ap debug-client trace**.
- **Additional AP Radio Statistics:** The output of the **show ap debug radio-stats** command has been enhanced with additional debugging statistics. For full details on the information shown in the output of this CLI command, refer to the ArubaOS *6.3 CLI Reference Guide*.

Extended VLAN Support on Virtual AP

This release of ArubaOS extends support for up to a maximum of 256 VLANs per virtual AP.

Configurable Heartbeat Interval

The AP system profile includes a heartbeat interval parameter that allows you to set the interval between hearbeat messages between a remote or campus AP and its associated controller . An increase in the heartbeat interval increases the time it will take for an AP to detect the loss in connectivity to the controller, but can reduce internet bandwidth consumed by a remote AP.

AirGroup

AirGroup is a unique enterprise-class capability that leverages zero configuration networking to allow mobile device technologies, such as the AirPrint wireless printer service and the AirPlay mirroring service, to communicate over a complex access network topology.

With AirGroup:

- End users can register their personal devices and define a group of other users, such as friends and roommates, who are allowed to share their 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 limit access to users with a specified user name, role, or user location.

For more information on AirGroup, see the *ArubaOS 6.3 User Guide*.

Instant AP VPN Support

Improved DHCP Pool Management

Instant AP (IAP) allows you to configure the DHCP address assignment for the branches connected to the corporate network through VPN. In distributed DHCP mode, ArubaOS 6.3 allows designated blocks of IP addresses for static IP users by excluding them from the DHCP scope. In addition, it allows creation of scope of any required size, thereby enabling more efficient utilization of IP address across branches. For more information on DHCP Pool Management for IAP-VPN, see *ArubaOS 6.3 User Guide*.

Instant AP VPN OSPF Scaling

This release of ArubaOS provides support for each IAP VPN to define a separate subnet derived from corporate intranet pool to allow IAP VPN devices to work independently. For more information on Instant AP VPN OSPF scaling, see *ArubaOS 6.3 User Guide*.

Instant AP VPN Scalability Limits

ArubaOS provides enhancements to the scalability limits for the IAP VPN branches terminating on the controller.

The following table provides the IAP VPN scalability information for various controller platforms:

Table 18: *Instant AP VPN Scalability Limits*

Platforms	Branches	Routes	L3 Mode Users	NAT Users	Total L2 Users
3600	8000	8000	N/A	N/A	64000
M3	8000	8000			64000
7210	8000	8000			64000
7220	16000	16000			64000
7240	32000	32000			64000

- **Branches**–The number of IAP VPN branches that can be terminated on a given controller platform.
- **Routes**–The number of L3 routes supported on the controller.
- **L3 mode and NAT mode users**–The number of trusted users supported on the controller. There is no scale impact on the controller. They are limited only by the number of clients supported per Instant AP.
- **L2 mode users**–The number of L2 mode users are limited to 64000 across all platforms.

IPv6

This section describes features related to IPv6.

Wired Client Support on IPv6 AP

This release of ArubaOS provides support for a wired client to connect to the Ethernet interface of an IPv6 enabled AP.

DHCPv6 Server

DHCPv6 feature enables network administrators to configure stateful/stateless options and manage dynamic IPv6 users connecting to a network. You can also configure domain name server using DHCPv6. For more information on configuring DHCPv6, see *ArubaOS 6.3 User Guide*.

DHCPv6 server supports stateless configuration of clients with options apart from the network addresses described in RFC 3736.

IPv6 L3 Mobility

This release of ArubaOS supports IPv6 L3 Mobility functionality. The existing L3 mobility solution has been enhanced to support dual stacked (IPv4 and IPv6) and pure IPv6 mobile clients. The IPv6 L3 mobility allows the wireless clients to retain their IPv4 or IPv6 addresses across different VLANs within a controller and between different controllers. In the previous release, the Aruba Mobility Controllers supported the L3 mobility only for single stacked IPv4 clients.

RADIUS Over IPv6

This release of ArubaOS provides support for RADIUS server over IPv6. You can configure an IPv6 host or specify an FQDN that can resolve to an IPv6 address for the RADIUS authentication. By default, the RADIUS server is in IPv4 mode. You must enable the RADIUS server in IPv6 mode to resolve the specified FQDN to IPv6 address.

NOTE

You can only configure the global IPv6 address as the host for the RADIUS server in IPv6 mode.

For more information on configuring an IPv6 host for the RADIUS server, see *ArubaOS 6.3 User Guide*.

TACACS Over IPv6

ArubaOS provides support for TACACS server over IPv6. You can configure the global IPv6 address as the host for the TACACS authentication. For more information on configuring an IPv6 host for the TACACS server, see *ArubaOS 6.3 User Guide*.

Platform

This section describes Platform features added in this release.

4G Backhaul Support for 600 Series Controllers

ArubaOS 6.3 introduces support for wireless uplink using 4G networks on the 600 Series controller. This feature is only supported when used with a Pantech UML290 4G USB modem. No new commands have been added to support this feature; instead, the existing 600 Series wireless uplink configuration steps are used.

Centralized Image Upgrade

The centralized image upgrade feature introduced in ArubaOS 6.3 allows the master controller to automatically upgrade its associated local controllers by sending an image from a image server to one or more local controllers. If your master controller supports different local controller models, you can upload different image types to the server, and the centralized image upgrade feature will send the local controller only the type of image that controller supports.

This feature can be configured on a master controller only, and supports up to 100 simultaneous downloads. You can configure a centralized image upgrade using the **Maintenance > Controller > Image Management**. page in the WebUI, or using the commands **upgrade-profile** (config mode), **upgrade verify** and **upgrade-target** (enable mode) in the command-line interface.

Centralized Licensing

Centralized licensing simplifies licensing management by distributing AP, PEFNG, RF PRotect, xSec and ACR licenses installed on one controller to other controllers on the network. One controller to act as a centralized license database for all other controllers connected to it, allowing all controllers to share a pool of unused licenses. The primary and backup licensing server can share single set of licenses, eliminating the need for a redundant license set on the backup server. Local licensing client controllers maintain information sent from the licensing server even if licensing client controller and licensing server controller can no longer communicate.

You can use the centralized licensing feature in a master-local topology with a redundant backup master, or in a multi-master network where all the masters can communicate with each other (for example, if they are all connected to a single Airwave server). In the master-local topology, the master controller acts as the primary licensing server, and the redundant backup master acts as the backup licensing server. In a multi-master network, one controller must be designated as a primary server and a second controller configured as a backup licensing server.

Enable and configure this feature using the **Configuration > Controller** > **Centralized Licenses** tab in the WebUI, or using the **licensing profile** commands in the command-line interface.

Primary and Backup Licensing Servers

Centralized licensing allows the primary and backup licensing server controllers share a single set of licenses. If you do not enable this feature, the master and backup master controller each require separate, identical license sets. The two controllers acting as primary and backup license servers must use the same version of ArubaOS, and must be connected on the same broadcast domain using the Virtual Router Redundancy Protocol (VRRP). Other client controllers on the network connect to the licensing server using the VRRP virtual IP address configured for that set of redundant servers. By default, the primary licensing server uses the configured virtual IP address. However, if the controller acting as the primary licensing server becomes unavailable, the secondary licensing server will take ownership of the virtual IP address, allowing licensing clients to retain seamless connectivity to a licensing server.

NOTE

Only one backup licensing server can be defined for each primary server.

Communication between the License Server and License Clients

When you enable centralized licensing, information about the licenses already installed on the individual client controllers are sent to the licensing server, where they are added into the server's licensing table. The information in this table is then shared with all client controllers as a pool of available licenses. When a client controller uses a license in the available pool, it communicates this change to the licensing server master controller, which updates the table before synchronizing it with the other clients.

Client controllers do not share information about factory-installed or built-in licenses to the licensing server. A controller using the centralized licensing feature will use its built-in licenses before it consumes available licenses from the license pool. As a result, when a client controller sends the licensing server information about the licenses that client is using, it only reports licenses taken from the licensing pool, and disregards any built-in licenses used. For example, if a controller has a built-in 16-AP license and twenty connected APs, it will disregard the built-in licenses being used, and will report to the licensing server that it is using only four AP licenses from the license pool.

When centralized licensing is first enabled on the licensing server, its licensing table only contains information about the licenses installed on that server. When the clients contact the server, the licensing server adds the client licenses to the licensing table, then it sends the clients back information about the total available licenses for each license type. In the following example, the licenses installed on two client controllers are imported into the license table on the license server. The licensing server then shares the total number of available licenses with other controllers on the network.

When new AP associates with a licensing client, the client sends updated licensing information to the server. The licensing server then recalculates the available total, and sends the revised license count back to the clients. If a client uses an AP license from the license pool, it also consumes a PEFNG and RF Protect license from the pool, even if that AP has not enabled any features that would require that license.

Jumbo Frame Support

Jumbo frame functionality can be configured on Aruba 7200 Series controllers to support up to 9216 bytes of payload. Jumbo frames are larger than the standard Ethernet frame size of 1518 bytes, which includes the Layer 2 header and Frame Check Sequence (FCS). This feature is disabled by default.

NOTE

ArubaOS supports jumbo frames between 11ac APs and 7200 Series controllers only.

AP Image Preload

The AP image preload feature minimizes the downtime required for a upgrade by allowing the APs associated to that controller to download the new images before the controller actually starts running the new version.

NOTE

This feature is not supported on the 650, 3200, and 3400 controllers.

This feature allows you to select the maximum number of APs that are allowed to preload the new software image at any one time, thereby reducing the possibility that the controller may get overloaded or that network traffic may be impacted by all APs on the controller attempting to download a new image at once.

APs can continue normal operation while they are downloading their new software version. When the download completes, the AP sends a message to the controller, informing it that the AP has either successfully downloaded the new software version, or that the preload has failed for some reason. If the download fails, the AP will retry the download after a brief waiting period.

You can allow every AP on a controller to preload a new software version, or create a custom list of AP groups or individual APs that can use this feature. If a new AP associates to the controller while the AP image download feature is active, the will check that AP’s name and group to see if it appears in the preload list. If an AP is on the list, (and does not already have the specified image in its Flash memory) that AP will start preloading its image.

Enable and configure this feature using the **Maintenance > WLAN > Preload AP Image** page in the WebUI, or using the **ap image-preload** commands in the command-line interface.

GRE Tunnel Redundancy

This release of ArubaOS provides redundancy for L3 generic routing encapsulation (GRE) tunnels. This feature enables automatic redirection of the user traffic to a standby tunnel when the primary tunnel goes down. For more information on configuring a tunnel-group, see *ArubaOS 6.3 User Guide*.

VLAN Derivation from Named VLAN Pools

Named VLANs can be configured under user rule, server derivation, user derivation, and VSA in this release.

Previously, only single VLAN ID names supported the above.

NOTE

You cannot modify a VLAN name so choose the name carefully.

Named VLANs (single VLAN IDs or VLAN pools) can only be assigned to tunnel mode VAP’s and wired profiles. They can also be assigned to user roles, user rule derivation, server derivation, and VSA for tunnel and bridge mode.

For tunnel mode, VLAN pools that have the assignment type “hash” and “even” are supported.

For bridge mode only VLAN pools with the assignment type “hash” are supported. If a VLAN pool with “even” assignment is assigned to a user rule, user role, server derivation or VSA, then the “hash” assignment is applied and the following message displays:

```
vlan pool assignment type EVEN not supported for bridge. Applying HASH algorithm to retrieve v
lan-id
```

Note that L2 roaming is not supported with even VLAN assignment.

Enhanced Support for Data Downloads to Dump Servers

Starting with ArubaOS 6.3, remote APs and campus APs associated to a controller using control plane security can use the TFTP protocol to send packet log and crash file data to the dump server defined in that AP’s system profile.

Previous releases allowed only campus APs that communicated to the controller without security certificates to send data to the dump server.

Controller Serviceability

The following enhancements have been added to improve controller troubleshooting, and should be used under the supervision of Aruba Technical Support.

- **Command and login history**: Use the **show audit-trail all** command to view show, action, and configuration commands that were executed on the controller. Additionally, the last 100 commands will be saved to the controller in file called **Audittrail-History.log**.
- **Reboot and upgrade history**: The **show boot history** command shows a list of the last 50 reboots and upgrades and includes when, why, from where, and by whom the upgrade/reboot was executed.
- **Packet capture**: The existing packet capture functionality has been enhanced to provide finer granularity. The **packet-capture controlpath** command and its parameters only capture packets destined for the controller. The **packet-capture datapath** command and its parameters capture packets being forwarded by the controller, such as Wi-Fi packets. The **packet-capture destination** allows you to send the packet capture log to specific destination.

  Captured packets that are saved locally can be viewed using the **show packet-capture** command.
- **Running versus Start-up Configuration**: Use the **show configuration diff** command to view the difference between the current running configuration and the configuration since the last save.
- **Ping and Traceroute enhancements**: New parameters have been added the ping and ping ipv6 commands to provide greater granularity. There parameters include **packet-size**, **source**, **count** (number of ping packets) and **df-flag** (do not fragment). The **source** parameter has been added to the **traceroute** command, allowing you to set a source IP address.
- **Netstat with Process ID**: The **show netstat** command output now includes process IDs and owners attached to the port.
- **IP Route**: The **counters** parameter has been added to the **show ip route** command. This parameter displays the number of routes present, categorized by type.

DHCP Lease Limit

The following table provides the maximum number of DHCP leases supported per controller platform.

Table 19: *DHCP Lease Limit*

Platform	Maximum number of DHCP Leases Supported
620	256
650/651	512
3200	512
3400	512
3600, M3	512
7210	5000
7220	10000
7240	15000

Security

ClearPass Profiling with IF-MAP Updates

This feature is used in conjunction with ClearPass Policy Manager. It sends HTTP User Agent Strings and mDNS broadcast information to ClearPass so that it can make more accurate decisions about what types of devices are connecting to the network.

To enable and configure this feature in the WebUI using the **CPPM IF-MAP** profile, or using the **ifmap** commands in the command-line interface.

Customizable Control Plane Access Control

Control Plane Access Control provides a generic way to restrict how protocols and services from specific hosts and subnets to the controller are used. Rules that you set using the ACL Whitelist on the WebUI or the firewall cp CLI command are applied to all traffic on the controller regardless of the ingress port or VLAN.

User-defined rules take precedence over internal cp-firewall rules. User-defined rules that contradict internal rules are not allowed, but a rule can be applied to a subset of addresses or ports defined in the internal rules.

Customize Control Plane Access Control in the **Configuration > Stateful Firewall > ACL White List** page of the WebUI, or using the the **firewall cp** commands in the command-line interface.

Enhancements in ArubaOS XML API

In this release of ArubaOS, the XML API functionalities such as addition, deletion, role change, querying, authentication, and blacklisting has been extended to support IPv6 users in addition to IPv4 users.

NOTE

The XML API server is configured using only the IPv4 address.

Enhanced MultiMode Modem Provisioning

ArubaOS 6.3 introduces a new method of provisioning a multimode USB modem (such as a Verizon UML290) for a remote AP. These changes simplify modem provisioning for both 3G and 4G networks.

The previous modem configuration procedure required that you define a driver for a 3G modem in the **USB modem** field in the AP provisioning profile, or define a driver for a 4G modem in the **4G USB type** field. Starting with ArubaOS 6.3, you can configure drivers for both a 3G or a 4G modem using the **USB field**, and the 4**G USB Type** field is deprecated.

Support for New Modem Types

ArubaOS 6.3 introduces support for the Sierra Wireless 4G LTE USB modems with remote APs (RAP). The supported Sierra Wireless 4G LTE USB modems are 313U, 319U, 320U, and 330U.

CAUTION

For this release, Sierra Wireless 4G LTE USB modems are supported in LTE mode only.

NOTE

Advanced mode for Cellular Network Preference is not supported on the Sierra Wireless 4G LTE USB modems.

Firewall Local-Valid-User Enhancement

In versions prior to 6.3 of ArubaOS, you could allow user creation of a member IP address of a VLAN interface when **firewall local-valid-user** was enabled. This would happen even if the valid-user ACL denied that IP address. This command has been enhanced and now behaves as follows:

- If the valid-user Access Control List (ACL) has a matching Access Control Entry (ACE) with a permit rule, the controller allows the creation of user entry, whether or not **firewall local-valid-user** is enabled.
- If the valid-user ACL has a matching ACE with a deny rule, the controller denies the user entry creation even if the **firewall local-valid-user** is enabled.
- If the valid-user ACL does not have a matching ACE and the **firewall local-valid-user** is enabled, the controller allows the creation of a user entry.

The valid-ser ACL now takes precedence over the **firewall local-valid user** knob if an explicit permit or deny rule has been created. If no such rule is created, the controller will act on whether or not the **firewall local-valid-user** is enabled.

High Availability: Fast Failover

ArubaOS 6.3 introduces the High Availability: Fast Failover feature. This WLAN redundancy solution allows a campus AP to rapidly fail over from an active to a standby controller without needing to rebootstrap, and significantly reduces network downtime and client traffic disruption during network upgrades or unexpected failures. APs using the High Availability: Fast Failover feature regularly communicate with the standby controller, so the standby controller has only a light workload to process if an AP failover occurs. This results in very rapid failover times, and a shorter client reconnect period. Previous redundancy solutions (like a backup-LMS) put a heavy load on the backup controller during failover, resulting in slower failover performance.

NOTE

This feature supports failover for campus APs in tunnel forwarding mode only. It does not support failover for remote APs or campus APs in bridge forwarding mode.

A controller using this feature can have one of three high availability roles – active, standby or dual. An **active** controller serves APs, but cannot act as a failover standby controller for any AP except the ones that it serves as active. A **standby** controller acts as a failover backup controller, but cannot be configured as the primary controller for any AP. A **dual** controller can support both roles, and acts as the active controller for one set of APs, and also acts as a standby controller for another set of APs.

The High Availability: Fast Failover feature supports redundancy models with an active controller pair, or an active/standby deployment model with one backup controller supporting one or more active controllers. Each of these clusters of active and backup controllers comprises a high-availability group. Note that all active and backup controllers within a single high-availability group must be deployed in a single master-local topology.

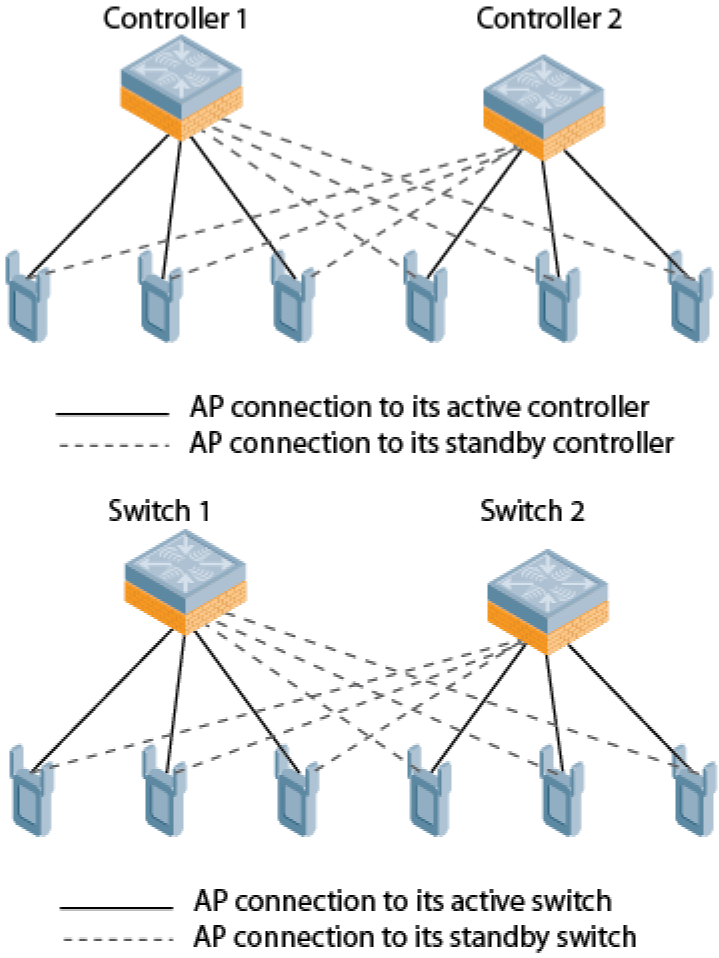
High Availability groups support the following deployment modes.

- Active/Active Deployment model on page 30
- 1:1 Active/Standby Deployment model on page 31
- N:1 Active/Standby Deployment model on page 32

Active/Active Deployment model

In this model, two controllers are deployed in dual mode. Controller one acts as standby for the APs served by controller two, and vice-versa. Each controller in this deployment model supports approximately 50% of its total AP capacity, so if one controller fails, all the APs served by that controller would fail over to the other controller, thereby providing high availability redundancy to all APs in the cluster.

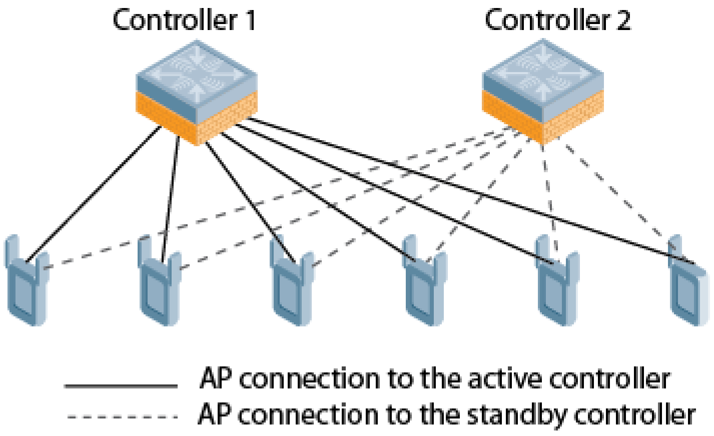
Figure 2 *Active-Active HA Deployment*

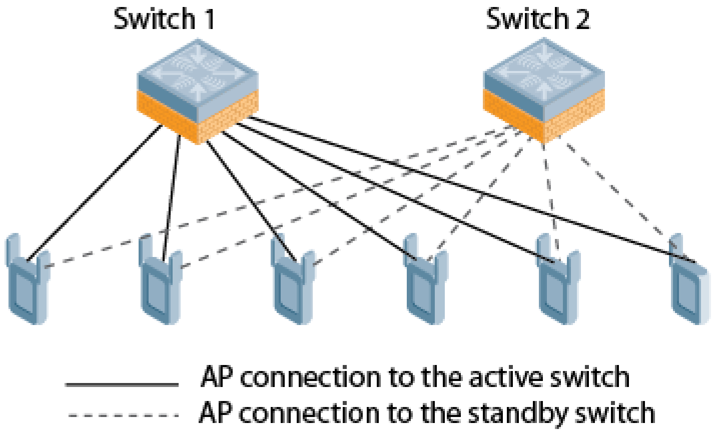

Controller 1
Controller 2
AP connection to its active controller
AP connection to its standby controller
Switch 1
Switch 2
AP connection to its active switch
AP connection to its standby switch

1:1 Active/Standby Deployment model

In this model, the controller in active mode supports up to 100% of its rated capacity of APs, while the other controller in standby mode is idle. If the active controller fails, all APs served by the active controller would failover to the standby controller.

Figure 3 *1:1 Active/Standby Deployment*


Controller 1
Controller 2
AP connection to the active controller
AP connection to the standby controller


Switch 1
Switch 2
AP connection to the active switch
AP connection to the standby switch

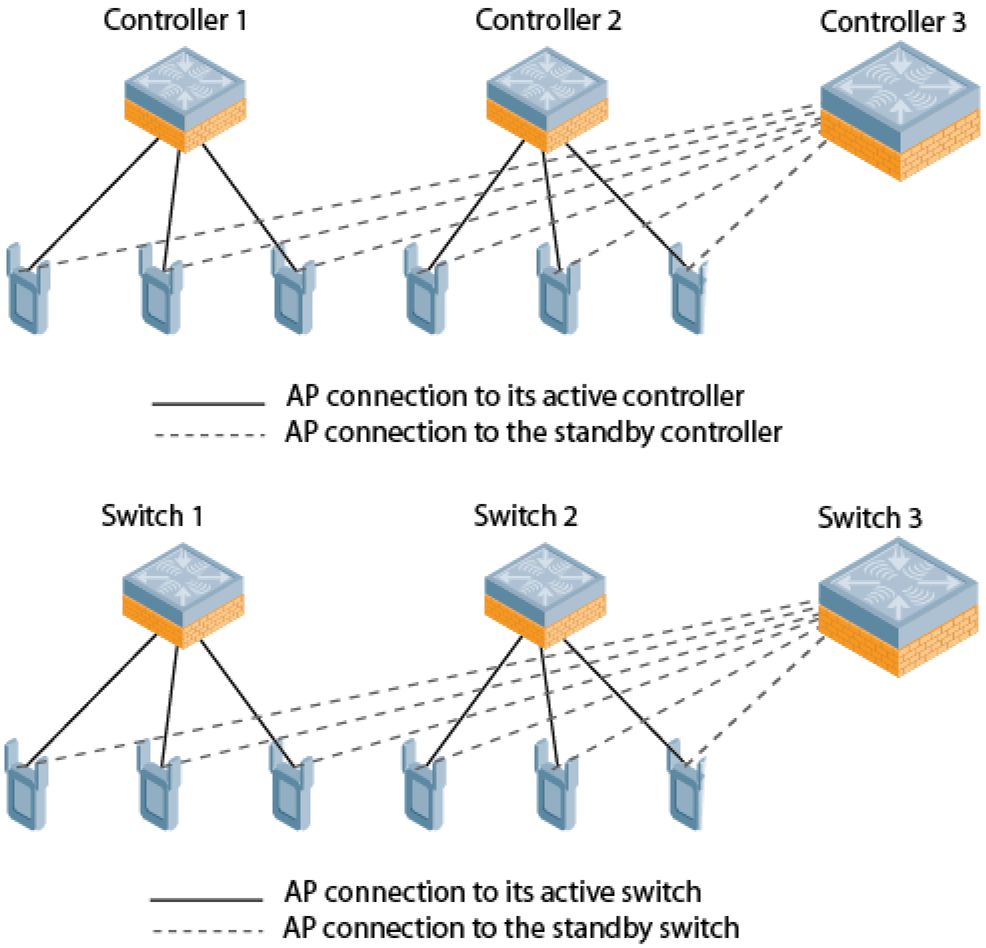
N:1 Active/Standby Deployment model

In this model, each controller in active mode supports up to 100% of its rated capacity of APs, while one other controller is idle in standby mode. If an active controller fails, all APs served by the active controller would failover to the standby controller.

> NOTE
>
> This model requires that the AP capacity of the standby controller is able to support the total number of APs distributed across all active controllers in the cluster.

In the cluster shown in the example below, two active controllers use a single higher-capacity standby controller.

Figure 4 *1:1 Active/Standby Deployment*


Controller 1
Controller 2
Controller 3
AP connection to its active controller
AP connection to the standby controller
Switch 1
Switch 2
Switch 3
AP connection to its active switch
AP connection to the standby switch

AP Communication with Controllers

The High Availability: Fast Failover features works across Layer-3 networks, so there is no need for a direct Layer-2 connection between controllers in a high-availability group.

By default, an AP's active controller is the controller to which the AP first connects when it comes up. Other dual mode or standby mode controllers in the same High Availability group become potential standby controllers for that AP. This feature does not require that the active controller act the configuration master for the local standby controller. A master controller in a master-local deployment can act as an active or a standby controller.

When the AP first connects to its active controller, that controller sends the AP the IP address of a standby controller, and the AP attempts to connect to the standby controller. If an AP that is part of a cluster with multiple backup controllers fails to connect to the first standby controller, the active controller will select a new standby controller for that AP, and the AP will attempt to connect to that standby controller. APs using control plane security establish an IPsec tunnel to their standby controllers. APs that are not configured to use control plane security send clear, unencrypted information to the standby controller. An AP will failover to its backup controller if it fails to contact its active controller through regular heartbeats and keepalive messages, or if the user manually triggers a failover using the WebUI or CLI.

Configure the High Availability feature in the WebUI using the **Configuration > Advanced Services > All Profiles > HA profile** page or using the ha-group-profile in the command-line interface.

RADIUS Accounting Support for RAP's Bridge-Mode VAP

This release supports RADIUS accounting for bridge mode. The bridge feature allows you to route the traffic flow only to the internet and not to the corporate network. Only the 802.1x authentication request is sent to the corporate network. This feature is useful for guest users.

RADIUS Override of User-Derived Roles

This feature introduces a new RADIUS vendor specific attribute (VSA) named "Aruba-No-DHCP-Fingerprint," value 14. This attribute signals the RADIUS Client (controller) to ignore the DHCP Fingerprint user role and VLAN change post L2 authentication. This feature applies to both CAP and RAP in tunnel mode and for the L2 authenticated role only.

Remote AP Whitelist Synchronization Across Controllers

ArubaOS 6.3 introduces Remote AP (RAP) whitelist synchronization across controllers. This feature is an enhancement to the previous RAP Whitelist Database feature, which could grant valid remote APs secure access to the network, or to revoke access from suspected rogue APs, but had to be configured locally on each individual controller. This enhanced remote AP whitelist database allows whitelist entries configured on a master or local controller to be synchronized across that master-local cluster of controllers.

Configure the remote AP whitelist using the **Wireless > AP Installation > whitelist** page in the WebUI, or using the whitelist-db rap commands in the command-line interface.

Integration with Activate

ArubaOS allows controllers to synchronize their remote AP whitelists with the Activate cloud-based services. When you configure Activate whitelist synchronization, the controller will securely contact the Activate server and download the contents of the whitelist on the Activate server to the whitelist on the controller. The controller and the Activate server must have layer-3 connectivity to communicate. By default, this feature will both add new remote AP entries to the controller whitelist and delete any obsolete entries on the controller whitelist that were not on the Activate server whitelist. Select the add-only option to allow this feature to add or modify entries, but not delete any existing entries.

MSCHAPv2 Authentication Support for VIA

A new protocol support MSCHAPv2 is introduced for authenticating VIA users. The VIA authentication request is sent to the controller from a backend server. IKE relays the VIA user's authentication request from VIA client to a backend server. This server acts as the authentication client, and relays the information to the authentication server on behalf of the VIA user. In previous releases, only PAP protocol was used to authenticate VIA users. In this release, the backend server can either use PAP or MSCHAPv2 for RADIUS authentication, depending upon the configuration provided in the **auth-profile** for VIA. By default, PAP is used for VIA authentication. For more information on VIA configurations, see *ArubaOS 6.3 User Guide*.

Support for Profile Based User Idle Timeout Configuration

This release of ArubaOS provides support for configuring the user idle time out value for authentication profiles apart from the global configuration under the AAA timers. This option is added both in the CLI and WebUI for the following profiles:

- `aaa profile <profile>`
- `aaa authentication captive-portal <profile>`
- `aaa authentication vpn default`
- `aaa authentication via connection-profile <profile>`

You can configure the client idle timeout value for the authentication profiles in seconds. For more information on configuring the user idle timeout value on the authentication profiles, see *ArubaOS 6.3 User Guide*.

NOTE

The user idle timeout configuration on the AAA profile is not applicable to RAPs connected in bridge-mode.

802.11 Suite-B

The bSec protocol is a pre-standard protocol that has been proposed to the IEEE 802.11 committee as an alternative to 802.11i. The main difference between bSec and standard 802.11i is that bSec implements Suite B algorithms wherever possible. Notably, AES-CCM is replaced by AES-GCM, and the Key Derivation Function (KDF) of 802.11i is upgraded to support SHA-256 and SHA-384. In order to provide interoperability with standard Wi-Fi software drivers, bSec is implemented as a shim layer between standard 802.11 Wi-Fi and a Layer-3 protocol such as IP. An Aruba controller configured to advertise a bSec SSID will advertise an open network, however only bSec frames will be permitted on the network.

The bSec protocol requires that you use VIA 2.1.1 or greater on the client device. Consult VIA documentation for more information on configuring and installing VIA.

The bSec protocol is available in 128-bit mode and 256-bit mode. The number of bits specifies the length of the AES-GCM encryption key. Using United States Department of Defense classification terminology,
bSec-128 is suitable for protection of information up to the SECRET level, while bSec-256 is suitable for protection of information up to the TOP SECRET level.

Banner Message for Management Authentication

When using X.509 certificates for management authentication, if a banner message has been configured on the controller it displays before the user can login. Click on a "login" button after viewing the banner message to complete the login process.

IKEv1 Aggressive Mode

A configuration knob has been added to prevent the use of IKEv1 aggressive mode. To configure, use **crypto-local isakmp disable-aggressive-mode**. Note that master-local communication by default uses IPsec aggressive mode when a PSK is used for authentication between controllers. You need to convert master-local communication to certificate-based IPsec authentication before disabling aggressive mode.

WebUI over SSL Enhancement

When you connect to the WebUI using HTTPS (TCP port 443), the controller continues using port 443 and no longer redirects to port 4343.

Delegated Trust Model for OCSP

ArubaOS 6.3 supports the Delegated Trust Model (in addition to the Direct Trust Model) to verify digitally signed OCSP responses. Unlike the Direct Trust Model, the Delegated Trust Model no longer requires the OCSP responder certificates to be explicitly available on the controller.

Certificate Expiration Alert

A feature has been added that sends alerts when installed certificates, which correspond to trust chains, OCSP responder certificates, and any other certificates installed on the device. By default, the system sends this alert 60 days before the expiration of the installed credentials. This alert is then repeated periodically on a weekly or biweekly basis. This alerts consist of two SNMP traps:

- wlsxCertExpiringSoon
- wlsxCertExpired

Chained Certificates on a RAP

Chained certificates on remote APs (that is, certificates from a multi-level PKI) need to be in a particular order inside the file. The RAP's certificate must be first, followed by the certificate chain in order, and then followed by the private key for the certificate. For example, with a root CA, a single intermediate CA, and a root CA, the PEM or PKCS12 file must contain the following parts, *in this order*:

NOTE

If this order is not followed, certificate validation errors occur. This order also applies to server certificates.

1. RAP Certificate
2. Intermediate CA
3. Root CA
4. Private key

Custom Certificate Support for Remote APs

As Suite-B mandates using the AES-GCM encryption and ECDSA certificates for security, this feature allows you to upload custom RSA and ECDSA certificates to a RAP. This allows custom certificates to be used for IKEv2 negotiation which establishes a tunnel between the RAP and the controller. Feature support includes the ability to:

- Upload a single CA certificate and RAP certificate which have either elliptical crypto key parameters with ECDSA or RSA parameters for signing and verification.
- Store the certificate in the flash of the RAP
- Delete certificates
- Generate a CSR paired with a private key generation for the RAP. The private key is stored in the flash and the CSR can be exported out of the RAP to get it signed by the CA.

If there is a custom certificate present in the flash when rebooting, this feature creates a suite B tunnel with the controller if the certificates uploaded are using EC algorithms. Otherwise it creates a tunnel using standard RAP IPSec parameters.

Administering Suite-B Support

If a custom ECDSA certificate is present in the flash of a certificate-based RAP, it is automatically designated as a Suite-B RAP. On the controller side, tunnel creation uses the server certificate as a default VPN server certificate.

Administering Suite-B support for a RAP includes these steps which are described in the following sections:

1. Setting the Default Server Certificate
2. Import a custom certificate
3. Generate a Certificate Signing Request (CSR)
4. Upload the certificate

Setting the Default Server Certificate

To set the default server certificate that is presented to the RAP as the default VPN server certificate, use the CLI command **crypto-local isakmp server-certificate .**

To add the CA certificate to verify the RAP certificate, use the CLI command **crypto-local isakmp ca-certificate.**

Importing a Custom Certificate

Certificates can only be imported to the controller using the WebUI. On the WebUI, navigate to **Configuration > Management > Certificates** and upload the certificate. To use imported certificates to create a tunnel, navigate to **Configuration > Advanced Services > Emulate VPN Services.**

Generating a CSR

The RAP console page allows you to generate a CSR. This is done through a private key which can be generated and saved to the RAP flash. A corresponding CSR is exported so it can be signed by the required CA to use as the RAP certificate. This RAP certificate can then be uploaded using the **Upload** button on the RAP Console page.

The subject of the RAP certificate needs to be the MAC address of the RAP, and nothing more. Note that this is case insensitive.

If you create a CSR on the RAP and then have a certificate issued by a CA, you must have the certificate in PEM format before uploading it to the RAP.

Uploading the Certificate

NOTE

When using the “rapconsole.arubanetworks.com” page on a bridge/split-tunnel RAP to manage certificates on the RAP, a blank page or a page that does not have the Certificates tabs on it may display. The RAP provisioning page that is standard on the RAP may conflict with the “rapconsole” page and thus confuse the browser. If this occurs, clear your browser cache first or use two different browsers.

The Upload button on the RAP console page that lets you upload the certificates to the RAP flash. The certificate needs to be in PEM format and uploading the RAP certificate requires that the corresponding private key is present in the RAP flash. Or, use the PKCS12 bundle where the chain includes the RAP private key with the RAP and CA certificates are optionally password protected.

Support for Certificates on USB Flash Drives

This release now supports the USB storing of the RAP certificate. This ensures that the RAP certificate is activated only when the USB with the corresponding certificate is connected to the RAP. Likewise, the RAP certificate is deactivated when the USB is removed from the RAP. In this case, the USB that is connected to the RAP is an actual storage device and does not act as a 3G/4G RAP.

The RAP supports only PKCS12-encoded certificates that are present in the USB. This certificate contains all the information that is required for creating the tunnel including the private key, RAP certificate with the chain of certificates and the trusted CA certificate. There is a limit of three supported intermediate CAs and the common name for the RAP certificate must be the MAC address of the RAP in the colon format.

NOTE

If you have an activated RAP that is using USB storage for the certificate, and you remove the USB storage, the RAP drops the tunnel. This is by design. However, for the RAP to re-establish the tunnel it has to be power cycled. It does not matter if you reinsert the USB storage before or after the power cycle as long as you power cycle it.

Marking the USB Device Connected as a storage device

If the AP provisioning parameter “usb-type” contains the value “storage,” this indicates that the RAP will retrieve certificates from the connected USB flash drive.

RAP Configuration Requirements

The RAP needs to have one additional provisioning parameter, the pkcs12_passphrase, which can be left untouched or can store an ACSII string. The string assigned to this parameter is used as the passphrase for decoding the private key stored.

NOTE

When placing certificates on USB storage, the naming of the file is important. For example, if the RAP’s MAC address is 00:0B:86:55:04:A2. The file name on the USB stick must be 000B865504A2.p12. You need to use capital letters for the first part of the filename, followed by lowercase.p12 extension. Without this exact format, the RAP does not activate.

When the RAP successfully extracts all the information including the CA certificate, the RAP certificate and the RAP private key using the passphrase from the provisioning parameter, it successfully establishes the tunnel.

Certificate Revocation Checking for SSH Pubkey Authentication

This feature allows the ssh-pubkey management user to be optionally configured with a Revocation Checkpoint (RCP). This meets the requirement for a two-factor authentication and integration of device management with PKI for SSH pubkey authentication. The ArubaOS implementation of SSH using Pubkey authentication is designed for integration with smart cards or other technologies that use X.509 certificates.

The RCP checks the revocation status of the SSH user’s client certificate before permitting access. If the revocation check fails, the user is denied access using the ssh-pubkey authentication method. However, the user can still authenticate through a username and password if configured to do so.

For information about configuring a revocation checkpoint, see the chapter titled, “Certificate Revocation,” in the *ArubaOS 6.3 User Guide.*

Firewall Reject Source Routing

Source routing options are used to obtain information of all routers through which a packet transits, however this could be used to bypass firewalls and cause a security threat. This feature permits the firewall, by default, to reject and log packets with the specified IP options loose source routing, strict source routing, and record route.

Note that network packets where the IPv6 source or destination address of the network packet is defined as an “link-local address (fe80::/64) are permitted.

Default Firewall Ruleset

New default firewall rules have been added to both the validuser and logon-control ACLs. To prevent malicious users from ip spoofing source addresses the default firewall rule in the validuser ACL causes the packet to be dropped.

A client with the correct source address can send traffic to the below networks as a destination IP address. To deny traffic, the default firewall rule added to logon-control ACL denies traffic to the reserved addresses from user with the logon role.

The following networks can be blocked by the default firewall rules in both the validuser and logon-control ACLs:

- Network packets where the source address of the network packet is defined as being on a broadcast network (source address == 255.255.255.255)
- Network packets where the source address of the network packet is defined as being on a multicast network (source address = 224.0.0.0 - 239.255.255.255)
- Network packets where the source address of the network packet is defined as being a loopback address (127.0.0.1 through 127.255.255.254)
- Network packets where the source or destination address of the network packet is a link-local address (169.254.0.0/16)
- Network packets where the source or destination address of the network packet is defined as being an address "reserved for future use" as specified in RFC 5735 for IPv4; (240.0.0.0/4)
- Network packets where the source or destination address of the network packet is defined as an "unspecified address"(::/128) or an address "reserved for future definition and use"(addresses other than 2000::/3) as specified in RFC 3513 for IPv6. The IPv6 "an unspecified address"(::/128) is currently being checked in datapath and the packet is dropped. This is the default behavior and you can view the logs by enabling **firewall enable-per-packet-logging** configuration.

Configuration of TCP/UDP Source Port in Firewall Rules

This feature allows you to configure a firewall rule, as part of an access list entry configuration, that is based on the TCP/UDP source port.

TLS 1.2 Support for HTTPS

The controller's embedded web server, that supports the management WebUI and captive portal, has been enhanced to support TLS 1.2. Previously, only TLS 1.0 was supported. When combined with the ArubaOS Advanced Cryptography License, support for Suite B ciphersuites in HTTPS sessions is allowed. Using TLS 1.2 also mitigates certain theoretical security vulnerabilities such as the BEAST attack.

Volume-Based SA Lifetime for IPsec

The IPsec security association (SA) lifetime is now supported in both seconds and kilobytes. Previously, only the seconds option was supported.

DH Group 14 Support for IKE Policy

This release now provides Diffie-Hellman (DH) Group 14 support for the IKE policy. This is the 2048-bit random DDH prime modulus group. DH is a specific method of exchanging cryptographic keys that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. You can configure this using the CLI.

Voice

This section describes voice features added in ArubaOS 6.3.

Lync Visibility and Granular QoS Prioritization

This release of ArubaOS provides a seamless user experience for Microsoft Lync users using voice or video calls, desktop sharing, and file transfer in a wireless environment. ArubaOS provides value added services such as Call Admission Control (CAC), call quality metrics, and call priority by implementing Lync Application Layer Gateway (ALG). This solution also provides a dedicated visibility and troubleshooting framework that allows network administrators to fine-tune and troubleshoot Lync traffic flow in the network. For more information, see the *ArubaOS 6.3 User Guide*.

WebUI

This section describes the features related to the WebUI.

Airwave Wizard

This release of ArubaOS introduces the Airwave wizard in the WebUI under **Configuration > Wizards > Airwave** to simplify the configuration process of the Airwave server.

Controller WebUI Dashboard Monitoring Enhancements

This release of ArubaOS provides enhancements to the following pages in Dashboard:

- Performace–You can now view the client health and channel quality details on the **Performance** page.
- Usage– You can view more information about the client and AP usage in addition to the details such as Air Group usage, WLAN usage, and applications usage from the **Usage** page.
- Access points–You can now view a summary of an AP along with the details such as WLANs, clients, charts and history related to the AP from the **Access Points** page.
- Clients–You can view the details such as firewall, Air Group, charts and an overall summary of an individual client on the **Clients** page. A Lync tab has also been added to view the details of the Lync usage on a client.
- WLANs–You can now click on a WLAN name to view the WLAN summary and the details of the clients, radios, charts, and firewalls related to the WLAN from the **WLANs** page.

NOTE

This release of ArubaOS provides the **Search** functionality to find the matched results for clients, APs, and WLANs. Click the count on the search results of clients, APs, and WLANs to navigate the related summary page with the filters applied.

Wireless

This section describes wireless features added in this release.

SSID Airtime Bandwidth Allocation Limit

Starting from ArubaOS 6.3, administrator can set a hard limit on Over the Air (OTA) bandwidth for a specific Service Set Identifier (SSID). Currently, the bandwidth allocation process is activated, when the bandwidth is completely saturated. The new enhancement allows you to limit an SSID to consume more bandwidth, when some unused bandwidth is available from other SSIDs. You can limit the bandwidth allocation to low priority SSIDs and allot the bandwidth to other high priority SSIDs.

Wireless Intrusion Prevention (WIP)

Enhanced Adhoc Network Containment

ArubaOS 6.3 includes a new Wireless Intrusion Protection (WIP) feature for enhanced containment of adhoc networks and clients, called **Protect From Adhoc Networks - Enhanced**.

This new feature introduces an enhanced adhoc network containment mechanism which can be used on adhoc networks operating without encryption. It is recommended that this feature be used in conjunction with Aruba’s current adhoc containment feature, as it can provide protection in certain cases where traditional containment mechanisms are not effective. For example, traditional adhoc network containment based on deauthentication is sometimes not effective because some clients in adhoc mode ignore deauthentication management frames.

You can enable and configure the Enhanced Adhoc Containment feature either by using the **Configuration > Advanced Services > All Profiles > DS > IDS Unauthorized Device** page in the WebUI or by using the **ids unauthorized-device-profile** commands in the command-line interface. This feature is disabled by default.

Detecting and Containing Wireless Hosted Networks

The Wireless Hosted Network feature available in Microsoft Windows 7 allows a wireless-enabled PC to share its network connection with other wireless users. Using this feature, the Windows 7 client can act as an access point to which other wireless clients can connect. If that client is connected to the wired or wireless network, it can share that connection with the connected clients, effectively becoming a Wi-Fi HotSpot. This creates a security issue for enterprises, because unauthorized users can use a hosted network to gain access to the corporate network, and valid users that connect to a hosted network are vulnerable to attack or security breaches.

ArubaOS 6.3 introduces a new feature that can detect the presence of a wireless hosted network, and contain the client hosting this network. When a wireless hosted network is detected this feature sends a “Wireless Hosted Network” warning level security log message and the wlsxWirelessHostedNetworkDetected SNMP trap. If there are clients associated to the hosted network, this feature will send a “Client Associated To Hosted Network” warning level security log message and the wlsxClientAssociatedToHostedNetworkDetected SNMP trap.

The existing feature that detects when valid clients associate to a non-valid AP has been enhanced to support wireless hosted network detection feature. When ArubaOS detects that a valid client has associated to a wireless hosted network, the log file for the event includes the message: Valid Client Misassociation to Hosted Network.

You can enable and configure the Enhanced Adhoc Containment feature either by using the **Configuration > Advanced Services > All Profiles > DS > IDS Unauthorized Device** page in the WebUI or by using the ids unauthorized-device-profile commands in the command-line interface.

Enhanced Containment of Suspected Layer-3 Rogue APs

The basic wired containment feature in the IDS general profile isolates layer-3 APs whose wired interface MAC addresses are either the same as (or one character off from) their BSSIDs. The enhanced wired containment feature introduced in this release can also identify and contain an AP with a preset wired MAC address that is completely different from the AP’s BSSID. In many off-the-shelf APs, especially those sold in Asia, the MAC address the AP provides to wireless clients as a ‘gateway MAC’ is offset by one character from its wired MAC address. This feature allows ArubaOS to check to see if a suspected Layer-3 rogue AP’s MAC address follows this common pattern.

You can enable and configure the Enhanced Adhoc Containment feature either by using the **Configuration > Advanced Services > All Profiles > DS > IDS General** page in the WebUI or by using the **ids general-profile** commands in the command-line interface.

MIB/Trap Enhancements

Aruba Products sysObject IDs

SNMP OIDs returned as sysObjectID for Aruba products defines the sysObjectIds for Aruba products added to this release:

Table 20: *SNMP OIDs returned as sysObjectID for Aruba products*

SNMP MIB	OID
AP-224	.1.3.6.1.4.1.674.10895.5033
AP-225	.1.3.6.1.4.1.674.10895.5034
RAP-155	.1.3.6.1.4.1.674.10895.5035
RAP-155P	.1.3.6.1.4.1.674.10895.5036

New WIP Module MIBs

- wlsxWirelessHostedNetworkDetected
- wlsxClientAssociatedToHostedNetworkDetected
- wlsxWirelessHostedNetworkContainment
- wlsxHostOfWirelessNetworkContainment
- wlsxEnhancedAdhocContainment
- wlsxAPWiredContainment

New Traps

The **wlsxNAccessPointIsUp** and **wlsxNAccessPointIsDown** are generated when an AP goes Up or Down

Deprecated MIBS/Traps

The following MIBS are now deprecated in this release:

wlsxMobilityHostTable

- mobilityHostHomeNetwork
- mobilityHostHomeMask
- mobilityHostDhcpInfo

wlsxMobilityProxyDHCPStatsGroup

- mobilityProxyDhcpBootpRx
- mobilityProxyDhcpPktProc
- mobilityProxyDhcpPktFwd
- mobilityProxyDhcpPktDrop
- mobilityProxyDHCPNak
- mobilityProxyBadDHCPPkt
- mobilityProxyNotDHCP
- mobilityProxyDHCPNoHomeVlan
- mobilityProxyDHCPUnexpFrame
- mobilityProxyDHCPUnexpRemote

wlsxMobilityHomeAgentTable

- mobilityHomeAgentSubnet
- mobilityHomeAgentMask
- mobilityHomeAgentVlan

aruba-switch.my

The traps **wlsxAccessPointIsUp** and **wlsxAccessPointIsDown** are now deprecated.

Changes to Regulatory Domains

The following regulatory domains have been enhanced in ArubaOS 6.3.

NOTE

Check with your local Aruba representative to confirm if device is approved and shipping in countries listed in the following table.

Table 21: *Regulatory Domain Changes*

Regulatory Domain	Change
Algeria, Australia, Bosnia & Herzegovina, Brazil, Colombia, Dominican Republic, Macedonia, New Zealand, Puerto Rico, South Korea,	Introduced support for the AP-104 access point.
Australia, Colombia, Dominican Republic, New Zealand, Puerto Rico, United States,	Added support for FCC DFS channels 52-64, and 100-140 on the AP-104 access point.
Algeria, Bolivia, Ecuador, El Salvador Guatemala, Nicaragua, Panama, Puerto Rico, Venezuela, Zambia	Introduced support for the AP-105 access point.
Mali	Introduced support for AP-134 and AP-135 access points.
Azerbaijan, Belarus, Bosnia & Herzegovina, Colombia, Croatia, Kazakhstan, Peru, Russia	Introduced support for the AP-135 access point.
Bermuda, Bosnia & Herzegovina, Colombia, Dominican Republic, Macedonia	Introduced support for the AP-175DC access point.
India	Introduced support for the 5 GHz radio band on the AP-175P access point.
Colombia, Algeria, Ukraine	Introduced support for AP-92 and AP-93 access points.
Colombia, Dominican Republic, Mexico, Puerto Rico, Singapore	Introduced support for the AP-93H access point.
Australia, Brazil, China, Egypt, Hong Kong, India, Malaysia, New Zealand, Qatar, Russia, Singapore, South Africa, Ukraine, United Arab Emirates	Introduced support for RAP-108 and RAP-109 access points.
Russia, South Africa, Ukraine	Introduced support for RAP-3WN and RAP-3WNP access points.

Limitations and Deprecated Features

- RF Plan has been deprecated from ArubaOS 6.3.
- On the AP-220 Series, AMSDU is supported in decrypt-tunnel and bridge forwarding modes. It is currently *not* supported in tunnel forwarding mode deployments.

The chapter describes the issues that have been fixed in ArubaOS 6.3.

Fixed in ArubaOS 6.3

The following issues have been resolved in ArubaOS 6.3:

Air Management-IDS

Table 22: *Air Management-IDS Fixed Issues*

Bug ID	Description
77174 81468	**Symptom**: The client classification in WLAN management system (WMS) was displayed as interfering for some time before being classified as valid. Until the client is classified as valid, the access point could not apply policies to protect those valid clients. To fix this issue, the access point locally marks clients as valid if they are detected to be associated to valid APs, and using encryption. **Scenario**: In large deployments, there can be a delay in classifying clients as valid. When WMS is very busy, this delay can become even longer. The issue was not specific to a controller model or a software version.
76808	**Symptom**: Some internal processes on the controller were unusually busy, while overall CPU utilization remained within expected levels. This release introduces changes that prevent APs from sending excessive containment event messages to the controller, so these internal processes do not become overloaded. **Scenario**: This issue was triggered when the wireless containment parameter in the IDS General profile was set to tarpit all-sta or tarpit-non-valid-sta, and one or more IDS Protection features are enabled such that active containment occurred.

AP–Platform

Table 23: *AP-Platform Fixed Issues*

Bug ID	Description
67276	**Symptom:** When a DHCP server sent multiple default gateway IP addresses and one of the addresses was not reachable, associated APs would appear to be up but not reachable. **Scenario**: This issue was resolved by removing the invalid default gateway (the unreachable IP) from the list of gateway IP addresses on the DHCP server.This issue was observed in all APs and controllers running ArubaOS 5.0.4.0 or later.
71978 75776	**Symptom**: AP model AP-68 unexpectedly rebooted due to a memory corruption. **Scenario**: This issue was observed in AP-68 running ArubaOS 6.2.0.0.
76021	**Symptom:** A core file from an AP with a special character in the AP name included the special character in the core file name, causing TFTP dump servers to reject that file. ArubaOS 6.2.1.0 resolves this issue by removing special characters from the core file name before it sends the file to the dump server. **Scenario:** This issue occurred when an internal process crashed on an AP, and a core file of troubleshooting data was sent to the dump server defined in the AP's system profile. This issue was seen on APs with one or more special characters in the AP name, and was not limited to a specific AP model.

Table 23: *AP-Platform Fixed Issues*

Bug ID	Description
77054	**Symptom:** An AP sent invalid deauthentication frames to the master controller. This issue is resolved by a change that prevents a station with a null MAC address from associating with the AP. **Scenario**: This issue occurred on a a 3600 or 3400 controller running 5.0.4.0, when a station with a null MAC address connected to the AP.
77183	**Symptom**: An AP-61 associated with a 7240 controller running ArubaOS 6.2.0.1 unexpectedly rebooted. The log files on the controller listed the reason for the AP reboot as “watchdog timeout.” Changes to channel reuse processing resolves this issue in ArubaOS 6.2.1.0. **Scenario**: This issue occurred when the RX Sensitivity Tuning Based Channel Reuse setting in the dot11x radio profile was set to dynamic.
77236	**Symptom**: An AP-125 configured to discover its master controller using DNS failed to connect to the controller after completing 802.1X authentication. Improvements to the master discovery process resolve this issue. **Scenario**: This issue would occur on any AP model running ArubaOS 6.1.3.2 with 802.1X authentication and dynamic master discovering, and was triggered because once the AP completed 802.1X authentication, the AP selected an IP address that could reach the master controller before the master was discovered.
79278	**Symptom:** The **show ap licence-usage** command displayed incorrect information about the available remote APs and campus APs. This command now displays the correct information. **Scenario:** This issue is not specific to any controller or AP model.
80412	**Symptom**: When a Remote AP (RAP) was replaced by RAP, the new RAP was unable to service the client requests. This issue is fixed by making internal changes to delete the stale entries. **Scenario**: The issue occurred when the first RAP was connected to the controller and after the connection was established it disconnected from the controller (due to issues related to IPsec connection to the controller was up but radio was dead). After connecting the second AP to the controller with same IP address, the new AP did not setup connection with the controller until the first AP timed out. This issue is not limited to a specific controller model or release version.

AP–Wireless

Table 24: *AP-Wireless Fixed Issues*

Bug ID	Description
82493	**Symptom:** An AP crashed when a virtual AP configuration changed during any downlink traffic to the clients. A few checks are added to the code to resolve this issue. **Scenario:** This issue is not specific to any AP model.

BaseOS Security

Table 25: *BaseOS Security Fixed Issues*

Bug ID	Description
52735 68792 77629 79839 80859 85453	**Symptom:** The process that handles DNS name resolution crashed when multiple instances of thread-unsafe API was executed. The API is now converted to single threaded API to resolve this issue. **Scenario:** This issue was observed when the configuration had too many unresolved DNS names. This issue is not specific to any controller model.

Table 25: *BaseOS Security Fixed Issues*

Bug ID	Description
68581	**Symptom:** When a mobile client roamed from a home agent (HA) controller to a foreign agent (FA) controller, issuing the CLI command **show user-table** from the FA controller incorrectly showed the client in an authenticated/derived role, whereas the output of the **show datapath user** command correctly showed the client in its dynamic role. The output of the **show user-table** command now shows correct information. **Scenario:** This issue was triggered when a mobile client roamed to a foreign agent controller running ArubaOS 6.2.x, and is not limited to any specific controller model.
77227	**Symptom:** An internal process that handles user authentication unexpectedly crashed in the controller due to incorrect memory allocation. The issue was fixed by making changes to the IP address pool. **Scenario:** When remote VPN users were deleted from the system, unexpected sequence of events pointed at stale memory entries. This resulted in an internal process failure. This issue is not limited to a specific controller model or release version.
78373 81390	**Symptom:** When some clients were connected using EAP-TLS authentication, the following error message was seen in the error logs: **<ERRS> |authmgr| user.c, derive_role2:5759: {04:f7:e4:26:c3:fb-??} Missing server in attribute list, auth=802.1x, utype=L2"** **Scenario:** This issue was observed when Common Name (CN) lookup was disabled in the client certificate. The issue was not specific to any ArubaOS version or controller model.
78728	**Symptom:** The authentication process on the controller crashed when the number of users reached the maximum limit. **Scenario:** This issue was observed on controllers running ArubaOS 6.1.3.5.
79564	**Symptom:** The **authmgr** (User Authentication) process crashed when a wireless client connected to captive portal with reauthentication configured as its user role. Improvements to the reauthentication timer fixed this issue. **Scenario:** The wireless client needed to have more than one IPv4/IPv6 addresses and have reauthentication configured. When the first IP address aged out before the reauthentication timer triggered, **authmgr** process crashed at the triggering time. This issue was observed in controllers running ArubaOS 6.x.
81426	**Symptom:** A memory leak was observed in wired clients with RADIUS accounting enabled. This issue is resolved by freeing the memory allocated for RADIUS context when a user was deleted. **Scenario:** This issue was observed when wired clients were connected to the APs with RADIUS accounting enabled on AAA profile. This issue was not specific to any controller model.
81547	**Symptom:** The **Monitoring>Network>All WLAN CLients** page in the WebUI failed to display client data, and instead displayed the error message “Controller <ip-addr> has not responded. The process is going to wait <number> minutes before displaying results.” This issue is resolved by changes that allow the master controller to better determine the role of a standby controller, preventing that master from polling the standby controller for user data. **Scenario:** This issue occurred in ArubaOS 6.1.3.7, in a master-standby controller topology.
84077	**Symptom:** A controller unexpectedly rebooted with a Crypto Post Failure message. This issue is resolved by enabling logs for the error message without automatically reloading the controller. **Scenario:** This issue is not specific to any controller model.
83620 84429	**Symptom:** Clients using Temporal Key Integrity Protocol (TKIP) or Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) suddenly stopped receiving traffic.This issue is resolved by improvements to how ArubaOS manages counters when new keys are installed. **Scenario:** This issue was observed on 7200 Series controllers running ArubaOS 6.2.1.1.

Command Line Interface

Table 26: *Command Line Interface Fixed Issues*

Bug ID	Description
62292	**Symptom**: The controller stopped responding and rebooted due to an internal process failure. Changes to the way the command **show hostname** handles filters fixed the issue. **Scenario**: When users executed the command **show hostname | include <filter>**, an internal process failed, causing the controller to crash. The issue was not specific to a controller model or a software version.

Control Plane Security

Table 27: *Control Plane Security Fixed Issues*

Bug ID	Description
66413 67875 68010	**Symptom**: Occasionally, the Control Plane Security (CPSec) whitelist database entries did not synchronize between the master and local controller. This issue is fixed by transmitting smaller sized CPsec records. **Scenario**: This issue was observed when the CPSec whitelist database size was large. The lossy network between the master and local controller caused some whitelist sync fragments to be lost. This issue is not limited to a specific controller model or release version.

Controller Datapath

Table 28: *Controller Datapath Fixed Issues*

Bug ID	Description
77247	**Symptom**: There was a discrepancy between configured per-user bandwidth contracts and the actual bandwidth allowed to those users. Changes to the internal credit process used to enforce bandwidth contracts, prevent users with low bandwidth contracts from having over credited contracts with a improperly increased contract rate. **Scenario**: This issue occurred when low contract rates (< 1Mbps) were applied to users, and is not limited to any specific controller model.
78312	**Symptom:** A client was losing connectivity and the ARP request from the client to its default gateway was redirected to a different place. Disabling the `firewall broadcast-filter arp` option fixed this issue. The same functionality is available with the `broadcast-filter arp` command on a per VAP-basis. **Scenario:** This issue was observed when a static IP configured to the client was matching the default gateway of the other clients and the `firewall broadcast-filter arp` option was enabled. This issue is not specific to any controller model.
78326	**Symptom:** A local M3 controller unexpectedly rebooted. The log files on the controller listed the reason for the reboot as “Datapath timeout.” Changes to unicast forwarding checks prevent this issue from occurring. **Scenario:** This issue was triggered when a controller that received GRE-type PPP packets had a user role that enabled source NAT.

Table 28: *Controller Datapath Fixed Issues*

Bug ID	Description
79553 77810 80138 80328 80717 80798 80799	**Symptom:** A datapath crash was observed in a Campus AP (CAP) configured behind Remote AP (RAP) configuration. Improvements to the encapsulation functionality fixed this issue. **Scenario:** This issue was observed in on M3 controllers running ArubaOS 6.2.0.2.
80326 80780 81399 81462 82385 82775	**Symptom:** A controller failed to respond and rebooted without saving SOS crash log tar files after upgrading to ArubaOS 6.1.3.7. The log files for the event listed the reason for the reboot as **Control Processor Kernel Panic**. Internal code changes fixed this issue. **Scenario:** This issue was first observed in ArubaOS 6.1.3.7.
83029	**Symptom**: A controller failed to respond when the **Firewall Visibility** option was enabled on the **Dashboard > Firewall** page of WebUI. **Scenario**: This issue was observed when high number of IPv6 sessions occurred with the **Firewall Visibility** option enabled. This issue was observed in 7200 Series and 3000 Series controllers running ArubaOS 6.2.1.0. and later.
83216	**Symptom**: A controller generated proxy ARP responses out of the same trusted port from where the controller learned the MAC address. Disabling the option **bcmc-optimization** in the VLAN interface resolved the issue. **Scenario**: The issue occurred when the trusted port was a port channel and the **bcmc-optimization** option was enabled on the VLAN interface. The issue was not specific to a controller model or a software version.

Controller Platform

Table 29: *Controller Platform Fixed Issues*

Bug ID	Description
59602	**Symptom:** When a controller running ArubaOS 2.4.1 FIPs version was upgraded to the 3.4 version, the system enforced the country code to change to US. **Scenario:** This issue occurred when the Electrically Erasable Programmable Read-Only Memory (EEPROM) of these controllers was corrupted on upgrading the controller to ArubaOS 3.4 version. This issue occurred on 5000 series controller models running 2.4.1 FIPs version.
80919	**Symptom:** A controller incorrectly identified the NTP_WRAP process restart as a crash. The improvements made to the NTP_WRAP restart process fixed this issue and the NTP_WRAP process restart is no longer identified as a crash. **Scenario:** This issue was observed in ArubaOS 6.2.0.2 and not specific to any controllers.

Table 29: *Controller Platform Fixed Issues*

Bug ID	Description
79719 81014 81086 81087 81181 81207 81368 81393 81479 81669 81853 82085 82232 82645 82708 82835	**Symptom:** A controller crashed and rebooted frequently after upgrading the software from ArubaOS 6.1.3.6 to ArubaOS 6.1.3.7. The improvements to packet processing fixed this issue in ArubaOS 6.3.0.1. **Scenario:** A high amount of control traffic triggered this issue, which is not specific to any controller model.
83738	**Symptom**: A crash was observed in all APs associated to the local controller followed by Access Control Lists (ACLs) configuration loss. The updates to the banner delimiter fixed this issue. **Scenario**: This issue was caused by banner message-of-the-day (motd) with **!** as a delimiter and the same character **!** was used to exit from a sub-mode command. The issue was observed in controllers running all versions of ArubaOS.

DHCP

Table 30: *DHCP Fixed Issues*

Bug ID	Description
77280	**Symptom**: Issuing the command **show running-config** from the command-line interface of a controller running ArubaOS 6.2.0.1 triggered the error **Module DHCP Daemon is busy. Please try later**. Improvements to how DHCP pool user options are generated resolves this issue. **Scenario**: This issue occurred when controllers configured with DHCP pools used non-alphanumeric characters in the pool name, resulting in bad syntax when DHCP user options were generated in the configuration file.

Dot1x

Table 31: *Dot1x Fixed Issues*

Bug ID	Description
77154	**Symptom**: If the **Use Server provided Reauthentication Interval** setting is enabled in an AP's 802.11X authentication profile, users associated to that AP do not reauthenticate when that client roams to a different AP. This issue is resolved by a change that allows the controller to store the session timeout reauthentication interval returned from the RADIUS server. **Scenario**: This issue occurred in ArubaOS 6.2.1.4, when clients authenticating using a RADIUS server roamed between APs.
83375	**Symptom:** Client failed to connect to Lightweight Extensible Authentication Protocol (LEAP) SSID when operation mode was set to Dynamic-WEP and Use Session Key was enabled on the client. The issue occurred when some of the clients failed to negotiate a separate session key. Enhancements in the security protocols fixed this issue in ArubaOS 6.3.0.1. **Scenario**: This issue was observed in controllers running ArubaOS 6.2.1.0 and was not specific to any controller model.

Enhanced Voice-Data Optimized

Table 32: *Enhanced Voice-Data Optimized (EVDO) Fixed Issues*

Bug ID	Description
78034	**Symptom**: A client connected to a 3G uplink port was unable to connect to the Internet when the option **firewall session-tunnel-fib** was enabled. The issue is fixed by changing a flag set in the route cache entry and adding the static ARP entry. **Scenario**: When an uplink port on the controller was connected via 3G link, a NAT client was not able to connect to the Internet. The issue was not specific to a controller model or a software version.

ESI

Table 33: *ESI Fixed Issues*

Bug ID	Description
73447	**Symptom:** External Services Interface (ESI) services had issues interpreting the new syslog message that comes from the customer's machine because of its new FireEye program. To fix this issue, users need to update their ESI regular expression pattern configuration to match the new output string from the newer FireEye log program. **Scenario:** The issue occurred after the user upgraded their FireEye log server and the newer version sends different log message. The issue is not specific to any controller or software version.

IPsec

Table 34: *IPsec Fixed Issues*

Bug ID	Description
68035 68956	**Symptom:** When site-to-site VPN was enabled between two controllers, static routes were not removed from the routing table when site-to-site VPN went down. **Scenario:** This issue occurs when site-to-site VPN was enabled and a static route was added to the remote subnet with an IPsec map. The issue is not specific to any controller or software version.
77201	**Symptom:** An internal module on a 6000 controller stopped responding, causing the controller to reboot. Improvements to the IKE rekey or IPsec rekey process resolved this issue. **Scenario:** This issue occurred on a standalone 6000 controller running ArubaOS 6.1.3.2 with control plane security enabled when that controller setup IKE/IPsec with a peer and enabled IKE or IPsec rekeys.
79452 77012	**Symptom**: IPv6 traffic from L3 mobility clients sent from a foreign agent (FA) to a home agent (HA) was double encrypted and sent through an IPsec tunnel instead of a Generic Routing Encapsulation (GRE) tunnel without encryption. This release updates the packets with tunnel flag so that data traffic does not get double encryption in an IPsec tunnel. **Scenario**: This issue was triggered by an internal flag that determines whether the packets parsed into the GRE tunnel should be encrypted. This issue was observed in ArubaOS 6.2.x.

IPv6

Table 35: *IPv6 Fixed Issues*

Bug ID	Description
74367	**Symptom:** Clients using temporary IPv6 addresses are not be able to communicate as traffic is getting dropped. The issue is been fixed by rotating the ipv6 addresses allocated to the client, and replacing the old IP address by new IP addresses. **Scenario:** A client can support up to four IPv6 addresses. The usage of temporary IPv6 addresses on the clients replaced old IPv6 addresses allocated in user-table and sent traffic using these addresses. This issue occurred on the controllers that support IPv6 clients.
76426 78962	**Symptom**: An increase in CPU utilization by the user authentication process was observed on the controller. Creating a rule in the validuser Access Control List (ACL) to deny packets from the host source IPv6 address fe80::/128 fixed this issue. **Scenario**: This issue was triggered when an HTC One X smartphone running Android version 4.1.1 generated a link-local IPv6 address fe80::/128, resulting in an increased CPU utilization on the controller. This issue was not limited to any specific version of ArubaOS.

MAC-Based Authentication

Table 36: *MAC-Based Authentication Fixed Issues*

Bug ID	Description
77491	**Symptom:** The Session-Timeout attribute returned from the Radius Server during MAC authentication was not honored in re-authentications and the user did not roll back to the initial-role when the MAC authentication/re-authentication failed. This issue has been fixed by adding Session-timeout support for MAC authentication. **Scenario:** This issue was not specific to any controller model.

Management Auth

Table 37: *Management Auth Fixed Issues*

Bug ID	Description
73779	**Symptom:** The station and user tables on local controllers showed stale entries for users that aged out. The issue is been fixed by introducing a new message that notifies the STM module that non-permanent user-entries are cleared. **Scenario:** Stale entries for wireless users associated to a remote AP in bridge mode appeared on local controllers running ArubaOS 5.0.4.1 with control plane security disabled. This issue was primarily triggered by a remote AP rebootstrapping.

Master-Redundancy

Table 38: *Master-Redundancy Fixed Issues*

Bug ID	Description
70343	**Symptom:** Custom captive portal pages were not synced between master and standby when set up to do so. **Scenario:** For all software versions, when the standby becomes the master, the custom captive portal page did not show up during CP authentication. The database synchronize command only copied database files and rf plan floor plan backgrounds.

Mesh

Table 39: *Mesh Fixed Issues*

Bug ID	Description
71371	**Symptom:** An AP-85 configured as a mesh portal unexpectedly rebooted. The log files for the event listed the reason for the reboot as **kernel page fault**. This issue was caused by memory corruption, and is resolved in ArubaOS 6.2.1.0 by changes to how internal controller modules restart. **Scenario:** This issue occurred in an AP-85 mesh portal associated to an M3 controller in a master-local topology.

Mobility

Table 40: *Mobility Fixed Issues*

Bug ID	Description
75093 81716	**Symptom**: The **show ip mobile host** command displayed the roaming status of a client as **No state** as opposed to **Home Switch/Home VLAN** and did not free the host entry. Changes in the mobile IP process code to free up host entry state of a client fixed this issue in ArubaOS 6.3.0.1. **Scenario**: This issue was observed when L3-mobility was enabled in the controller. This issue was observed in all controllers running any version of ArubaOS.
78111	**Symptom:** Loss of traffic was observed on roaming clients, when L3 mobility was enabled on the controller. **Scenario:** This issue occurred because duplicate ARP responses were sent from both home agent and foreign agent for the roamed client. Due to this issue, the bridge entry for the roamed client on the upstream switch was flipped. This issue was observed when the controllers were upgraded from ArubaOS 5.x to 6.1.x.
82673	**Symptom:** DHCP packets from the clients at foreign agent were getting redirected through IPIP tunnel due to wrong order of the ACL. This caused a delay in allocating a valid IP address to the clients. This issue is resolved by correcting the order of the ACL. **Scenario:** This issue was observed when L3 mobility was enabled on controllers running ArubaOS 6.1.x.

Online Certificate Status Protocol (OCSP)

Table 41: *OCSP Fixed Issues*

Bug ID	Description
79704	**Symptom:** The process that handles the OCSP verification requests from the internal user authentication module was not responding. This issue is resolved by making the OCSP server communication asynchronous. **Scenario:** This issue was observed when OCSP server was configured as revocation check point and an incoming certificate was validated against the OCSP, with rapid similar incoming requests. This issue is not specific to any controller model.

OSPF

Table 42: *OSPF Fixed Issues*

Bug ID	Description
82730	**Symptom:** A controller failed to add the default route when it was advertized by the neighboring router. This issue is resolved by ensuring that the default route is not skipped while adding the route information. **Scenario:** This issue was observed on controllers running ArubaOS 6.2.1.0.

RADIUS

Table 43: *RADIUS Fixed Issues*

Bug ID	Description
76336	**Symptom:** Clients no longer get a DHCP IP when DHCP is denied in the user role. **Scenario:** When the AAA profile was configured with MAC authentication, and if the 802.1X authentication profile was configured without a server group, the default-role (logon) was applied to the user-traffic upon failure of MAC authentication. As the default role allows DHCP, the users end up getting a DHCP IP. This issue was observed in all APs running ArubaOS 6.1.3.4.
76484	**Symptom:** RADIUS authentication failed in networks that had different Maximum Transmission Values (MTUs). **Scenario:** The RADIUS authentication failed when the MTU value in the network between the controller and RADIUS server was different.This issue was observed in controllers running ArubaOS 6.2.1.2 or earlier and was not specific to any controller model.

Remote AP

Table 44: *Remote AP Fixed Issues*

Bug ID	Description
64778 84004	**Symptom:** Users were unable to make calls to IP phones. This issue was fixed by increasing the maximum acceptable frame size to 1518 bytes in RAP3's Ethernet driver. **Scenario:** This issue occurred when the IP phone was connected to the enet interface of RAP3 and was observed in ArubaOS 6.2.1.1.
75817	**Symptom:** The Captive Portal login screen is now correctly displayed for the client after the client switches between bridge SSID and tunnel SSID multiple times. **Scenario:** This issue occurred when the client changed its connection from tunnel SSID to bridge SSID on the same RAP repeatedly. This issue was observed in ArubaOS 6.1.3.5.
83976	**Symptom:** An unprovisioned remote AP was detected as a Campus AP causing a license issue even though there is bandwidth to connect more RAPs. This issue is resolved by improvements to how the controller adds and deletes licenses, as well as enhancements how the controller updates the unused AP licenses count. **Scenario:** This issue was observed when the RAP is unprovisioned and there was no bandwidth to connect a campus AP.

Role/VLAN Derivation

Table 45: *Role/VLAN Derivation Fixed Issues*

Bug ID	Description
78322	**Symptom:** Bridge clients were deriving incorrect roles when the AP was connected to a Cisco bridge VLAN. **Scenario:** This issue was observed when an AP was connected to a Cisco bridge VLAN, the AP was receiving its own broadcast message over uplink and started deleting L2 and L3 entries. This issue was not specific to a controller model.

Station Management

Table 46: *Station Management Fixed Issues*

Bug ID	Description
72194 74720	**Symptom**: When the preserve VLAN feature was enabled on the controller, the user VLAN still changed when the client roamed from one AP to another. Changes to the internal process that handles the AP management and client association fixed this issue. **Scenario**: When the VLAN mobility or the preserves VLAN feature was enabled on the controller, the controller's bridge table kept the user VLAN entries for 12 hours. This issue was observed when a user switched to a different ESSID with different VLAN configured. The bridge table lookup returned the VLAN which was created when the user was associated with the original ESSID. This behavior was observed during every roaming. This issue is not limited to a specific controller model or release version.
75872 78805	**Symptom:** The Station Management process was terminated and restarted erratically on the controller. This issue was fixed by blocking certain entries and events that are created during an image-mismatch. **Scenario:** This issue was observed in M3 controllers running ArubaOS 6.1.3.6 with Mesh Portals and Points in the setup. When the image version on Mesh Portals and Points was different from the image version stored on the controller, the initialization sequence for these APs was not accurate. This created some incomplete entries that caused a crash.
83091 83547	**Symptom:** Active APs of a local controller were not displayed on the master controller when the local controller showed the APs were active on the master controller. Introducing a new action to handle the race condition fixed this issue. **Scenario:** This issue was triggered by a race condition which resulted in creating session entries before IPSec tunnel and Network Address Translation (NAT) rules were created. The session removal mechanism could not remove the session entries without NAT flags. This issue was observed in controllers running ArubaOS 6.2.1.0.

SNMP

Table 47: *SNMP Fixed Issues*

Bug ID	Description
81499	**Symptom**: An SNMP get request to poll *sysExtCardStatus* for the operational status of any installed cards could return the message **No such instance currently exists at this OID** and trigger an alert. Improvements to SNMP polling allow a get request to *sysExtCardStatus* to display a cached information from the previous poll status instead of an error message. **Scenario**: This issue was identified in ArubaOS 6.1.2.5, and occurred when the SNMP request was issued while the internal controller hardware monitor polled for hardware status. The SNMP request would time out, but the controller would return the error message instead of a timeout message.

Switch-Datapath

Table 48: *Controller Datapath Fixed Issues*

Bug ID	Description
80625	**Symptom:** A controller unexpectedly rebooted. Log files for the event listed the reason for the reboot as a Datapath timeout due to change in the tunnel MTU while processing a frame. This issue is resolved by ensuring that the same tunnel MTU is used for processing a given frame. **Scenario:** This issue was observed when tunnels were used on controllers running ArubaOS 6.1.3.x or later.
83409	**Symptom:** A controller rebooted due to missing heartbeats, and log files for the event listed the reason for the reboot as **watchdog timeout**. This issue is resolved by improvements to the communication infrastructure. **Scenario:** This issue was observed when a huge traffic hit the control plane causing loss of acknowledgements in the communication infrastructure. This is not specific to any controller model.

UI-Configuration

Table 49: *UI-Configuration Fixed Issues*

Bug ID	Description
85051 77933	**Symptom:** The firewall rule count was not displayed correctly in the **Configuration > Security > User Roles > Edit Role <role_name>** page of the WebUI. The modifications to the parsing and calculation logic fixed this issue and now the WebUI displays the accurate firewall rule count. **Scenario:** The incorrect rule count was triggered by an issue in the parsing logic and calculation. This issue was observed in M3 controllers in a master-local topology running ArubaOS 6.1.3.5 and 6.2.1.1.

Voice

Table 50: *Voice Fixed Issues*

Bug ID	Description
76750	**Symptom**: The Real-time Transport Protocol Analysis (RTPA) process crashed in the controller. This release introduces changes to the software code to ensure that RTPA feature (**voice real-time-config** command) can be enabled only for those Virtual APs (VAP) that are in decrypt-tunnel forwarding mode. **Scenario**: This issued was observed when RTPA was enabled for a VAP profile in split-tunnel or bridge forwarding mode. This issue was observed in all controllers running any version of ArubaOS.
81487 83707 83757 84631	**Symptom:** Voice clients registered as SIP clients were overridden with the application-level gateway (ALG) value as Vocera or New Office Environment (NOE). This issue is resolved by improvements that prevent subsequent updates to the initially configured ALG value. **Scenario:** This issue was observed in 7200 Series controllers running ArubaOS 6.1.3.3 or later.

Virtual Router Redundancy Protocol (VRRP)

Table 51: *VRRP Fixed Issues*

Bug ID	Description
77114	**Symptom:** When system clock was set backwards through Network Time Protocol (NTP), Virtual Router Redundancy Protocol (VRRP) went to a weird state with two masters in the network. This issue is fixed by removing the VRRP dependency on the system clock. **Scenario:** This issue was observed when an NTP server update with large negative offset happened in the network. This issue is not specific to any controller model.

Web UI

Table 52: *Web UI Fixed Issues*

Bug ID	Description
66521	**Symptom**: Two **Apply** buttons displayed in the controller's WebUI when adding users to the internal database. This issue is fixed by renaming the top **Apply** button to **Add**. **Scenario**: Adding a new user from the WebUI displayed two **Apply** buttons in the **Configuration > Security > Authentication > Internal DB** page due to incorrect labeling of the buttons. This issue is not limited to a specific controller model and was observed in ArubaOS 6.1.3.1 or later.
74227	**Symptom:** The **Monitoring** tab of the WebUI and the output from the `show ap database` command do not match. The WebUI showed more APs than are actually up and the output of show ap database displays the correct number. The issue is fixed by making changes to the internal process due to which both the process memory and the database are updated to show the correct AP count. **Scenario:** This occurred on any controller model acting as a master and running ArubaOS 6.1.3.2 or later if the bootstrap threshold in the ap system profile is set to more than 40 minutes. In this instance, these APs were powered off when the controller attempted to send a configuration update. The APs failed to receive the update, and the controller marked the APs as down but did not update the AP database as well.
74890 76149 76493 79257 82660	**Symptom**: The client name, IP Address, and role details of some clients were not displayed in the **Dashboard > Client** page of the WebUI. This issue is fixed by ensuring the client information is available till the client is disconnected. **Scenario**: This issue was triggered when a client roamed and associated to another AP without completing the authentication cycle. This issue was observed in controllers running ArubaOS 6.2.X for L3 users.
76451	**Symptom:** When guest users were imported using a .CSV file in the **Configuration > Security > Authentication > Internal DB > Guest User** page of the WebUI, the sponsor's email address was not imported. **Scenario**: The issue was observed in ArubaOS controllers running 6.1.3.4 and 6.2.x and was not specific to any controller model.
75873 78387 80198	**Symptom:** An error message was displayed in the WebUI after enabling or disabling the user debug option. To fix this issue, a new **stop debug** button is introduced and by clicking on this button the alert message is disabled. **Scenario:** After enabling or disabling user debug in the **Monitoring > Clients > Debug** page of the WebUI and even though the user debug was successful an error message `Error enabling debugging for user error` was displayed. This issue was observed in ArubaOS 6.1.3.4 and higher and is not limited to any specific controller model.

Table 52: *Web UI Fixed Issues*

Bug ID	Description
76335	**Symptom:** In the ArubaOS 6.2.0.x **Dashboard** tab the WebUI, the y-scale of the **Noise Floor** graph was inverted compared to previous versions of ArubaOS. This has been changed in ArubaOS 6.2.1.0, so -110 dBm is now shown at the bottom of the y-scale instead of the top. **Scenario:** This issue occurred on controllers running ArubaOS 6.2.0.x, and was not limited to a specific controller model.
80269	**Symptom:** The GigabitEthernet interface 10 option was missing in the VRRP tracking Interface drop-down under **Advanced Services > Redundancy > Add virtual Router > Tracking Interface table** of the WebUI. ArubaOS 6.2.1.2 now includes the GigabitEthernet interface 10 option in the VRRP tracking Interface. **Scenario:** This issue was observed in M3 controller models running ArubaOS 6.1.3.1.
81664	**Symptom:** When the controller clock changed from 11:59 a.m. to 12:00 p.m., the last updated time value displayed in the Dashboard tab incorrectly displayed times with a p.m. suffix instead of an a.m. suffix. **Scenario:** This issue occurred on a 3000 Series controller running ArubaOS 6.1.3.1 and using an NTP server to synchronize its system clock.
82959	**Symptom:** User was not able to navigate to the fields properly using the tab key in the **Configuration > Security > Authentication > Internal DB > Guest User** page of the WebUI and use the options: **create New**, **import**, **delete**, **print**, and **cancel**. Adding code to the guest provisioning page to create an appropriate tab index for new, import, and edit windows fixed this issue in ArubaOS 6.3.0.1. **Scenario:** This issue was observed in ArubaOS 6.2.x and is not specific to any controller model.

This chapter describes the known issues and limitations observed in previous 6.3.0.x versions of ArubaOS.

Known Issues and Limitations

The following are the known issues and limitations found in ArubaOS 6.3. Applicable Bug IDs and workarounds are included.

Air Management -IDS

Table 53: *Air Management- IDS Known Issues*

Bug ID	Description
79913	**Symptom**: When configuring an AP in Air Monitor (AM) mode, a user has the option to select the **rare** scan-mode, causing the AP to scan most frequencies in the spectrum, even if they are non-standard channels. Currently some AP-220 Series APs configured to use the **rare** scan mode cannot scan non-standard channels that do not belong to some country's regulatory domain. **Scenario**: This issue occurs on AP-220 Series access points running ArubaOS 6.3. **Workaround**: None.

AP Wireless

Table 54: *AP Wireless Known Issues*

Bug ID	Description
74984	**Symptom**: Blackberry devices experience severe ping losses when connected to a high throughput SSID. **Scenario**: This issue occurs on AP-135 access points configured to use a high-throughput SSID and running ArubaOS 6.1.3.4. **Workaround**: None.
84329	**Symptom**: AP-175 access points experienced significant ping losses, causing clients to disconnect. **Scenario**: This issue occurred on AP-175 associated to a standalone 6000 controller running ArubaOS 6.2.1.0. **Workaround**: None.

AP Platform

Table 55: *AP Platform Known Issues*

Bug ID	Description
82015 84757	**Symptom**: An AP associated with a controller does not age out as expected when you change the heartbeat threshold and interval parameters. **Scenario**: This issue occurs when you change the heartbeat threshold and interval parameters in the AP's system profile while the AP's status is UP in the controller. This issue is not specific to a controller, AP model, or ArubaOS release version. **Workaround**: Reboot the AP after changing the heartbeat threshold and interval parameters. Alternatively, configure the heartbeat threshold and interval parameters before associating the AP with the controller.
82388	**Symptom:** The iperf throughput test fails to start on 650 and 7200 Series controllers. **Scenario:** Although the iperf server commands can be successfully executed and no warning messages are displayed, the iperf throughput test fails to begin on 650 and 7200 Series controllers running ArubaOS 6.3.0.0. **Workaround:** None.

Base OS Security

Table 56: *Base OS Security Known Issues*

Bug ID	Description
50206	**Symptom:** Secure Shell (SSH) access to a controller fails to authenticate local database when the RADIUS server is not responsive. **Scenario:** This issue occurs when multiple authentication servers are configured with local authentication enabled. This issue is not specific to any controller model and release version. **Workaround:** None.
75565	**Symptom**: A wired user is incorrectly assigned to an initial user role instead of a user role derived from DHCP fingerprinting. **Scenario**: This issue is observed in ArubaOS 6.1.3.4, and is not specific to any controller platform. **Workaround**: Delete the user from the user table, and verify that the corresponding bridge entry is removed from the datapath before reconnecting the user.

Controller Datapath

Table 57: *Controller Datapath Known Issues*

Bug ID	Description
74428	**Symptom:** On the RJ45 ports 0/0/0 and 0/0/1, if the port speed is forced from 1Gbps to10/100Mbps when traffic is flowing, traffic forwarding on the port can stop in an unintended manner. **Scenario:** This issue has been observed in controller models 7210, 7220, and 7240 running ArubaOS 6.2 in configurations or topologies where traffic is flowing. The trigger is unknown. **Workaround:** Change the speed on the port following these steps: 1. Shut the port. 2. Change the speed on the port. 3. Open the port.

Table 57: *Controller Datapath Known Issues*

Bug ID	Description
82824	**Symptom**: In some cases, when the number of users is high (more than16k), a user may be flagged as IP spoofed user with the **Enforce DHCP** parameter is enabled in the AP group's AAA profile. **Scenario**: This issue is observed in controllers running ArubaOS 6.3. **Workaround**: Disable the **enforce_dhcp** parameter in the AP group's AAA profile.
84494	**Symptom**: A controller unexpectedly rebooted. The log files for the event listed the reason for the reboot as “Nanny rebooted machine - udbserver process died.” **Scenario**: This issue occurred on a standalone master 7210 controller with one associated AP-135 access point. **Workaround**: None.
85368	**Symptom:** After booting up and logging into the controller, the configured message of the day banner does not display. Instead, a portion of the configuration displays. **Scenario:** This issue is observed in controllers running ArubaOS 6.2 and 6.3,after upgrading a controller with a “banner motd” config that has more than 255 characters in one line. This issue occurs in old versions such as ArubaOS 6.1.X-FIPS that do not validate the length per line. **Workaround:** Change the banner to comply with new the character limit per line. You can have more than1 line of 255 characters. Run the write-mem command afterwards to fix this issue.

Local Database

Table 58: *Local Database Known Issues*

Bug ID	Description
84494	**Symptom:** An internal process (udbserver) crashes and the controller is getting rebooted. **Scenario:** This issue occurred due to an error in the internal code and is observed in 7210 controllers running ArubaOS 6.2.1.1. **Workaround:** None.

Master-Redundancy

Table 59: *Master-Redundancy Known Issues*

Bug ID	Description
75367	**Symptom**: Enabling web-server debug logging using the CLI command **logging level debugging system subcat webserver** does not take effect until you restart the HTTPD process. **Scenario**: This happens on all controller models running ArubaOS 3.x, 5.x and 6.x software versions when web-server debug logging mode is enabled. **Workaround**: Restart the HTTPD process in order to enable debug logging.

Mobility

Table 60: *Mobility Known Issues*

Bug ID	Description
63163	**Symptom:** There is an increase in datapath CPU utilization in the controller. **Scenario:** This issue occurs in a Layer-3 IP mobility enabled network, where a wired 802.1X client is connected to an untrusted port and the IP address of the client changes rapidly. The Layer-3 IP mobility edits the bridge table entries for such clients. This results in an increased CPU utilization. This issue is found in controllers running ArubaOS 6.2 or earlier. **Workaround:** Do not change the IP address of the wired client at a rapid rate.

RAP+BOAP

Table 61: *RAP+BOAP Known Issues*

Bug ID	Description
85053	**Symptom:** A controller crashes frequently for split tunnel wired user in a configuration with the RADIUS accounting enabled. This issue occurs in 6000M3 controllers running ArubaOS 6.2.1.1. **Scenario:** The user authentication process is not able to find the user entry for the accounting statistics message received for a user from Remote AP (RAP). This is because the message contains incorrect forward mode value which is used to obtained the user entry. **Workaround:** None.
85249	**Symptom:** A degradation of Transmission Control Protocol (TCP) throughput by 9 to 11 Mbps is observed on a RAP. **Scenario:** This issue occurs in RAPs with any forwarding mode and not specific to any AP model. **Workaround:** None.

Remote AP

Table 62: *Remote AP Known Issues*

Bug ID	Description
81245	**Symptom**: The controller/AP displays details of the users who are no longer connected to an AP or the network. **Scenario**: This issue occurs when users associated to a AP in split-tunnel forwarding mode and using captive portal authentication roam to multiple APs exhibiting the same ESSID. **Workaround**: Periodically delete the users who are no longer connected to an AP or the network, from the user table.
83002	**Symptom**: A wireless client connected to a backup virtual AP configured in bridge forwarding mode is unable to get an IP address from an assigned VLAN. **Scenario**: This issue occurred when the controller upgraded to ArubaOS 6.2. **Workaround**: Once the AP connects to the controller, remove the virtual AP profile from the ap-group/ap-name configuration, then return the virtual AP profile to the ap-group/ap-name settings.
82427	**Symptom**: A RAP-5WN AP in split-tunnel forwarding mode using a Sierra Wireless AirCard modem can stop responding when an associated client sends traffic, **Scenario:** This issue only occurs when the RAP-5WN AP's cellular network preference settings is configured to use 3G-only mode. **Workaround:** Configure the cellular network preference settings in the RAP-5WN to use 4G mode.

Station Management

Table 63: *Station Management Known Issues*

Bug ID	Description
82012	**Symptom**: An internal controller process kept restarting, preventing the controller from servicing clients. **Scenario**: This issue was identified when the controller upgraded its image, and was triggered when the controller expected IKEv2 information that was missing from the mysql global AP database. **Workaround**: None.

VLAN

Table 64: *VLAN Known Issues*

Bug ID	Description
85630	**Symptom**: Auto downgrade from ArubaOS 6.3 to 6.2 is not supported for VLAN pooling. **Scenario**: When auto downgrade is used from ArubaOS 6.3 to 6.2, VLAN pool configuration is lost. **Workaround**: To maintain your VLAN pool configuration, use a 6.2 configuration file for downgrade.

WebUI

Table 65: *WebUI Known Issues*

Bug ID	Description
55981	**Symptom:** When a user views the Spectrum UI with saved preferences from a newer version of ArubaOS, the UI will display charts incorrectly. **Scenario:** After downgrading from a newer version of ArubaOS, such as from 6.2.x to 6.1.x with saved Spectrum preferences, will cause the Spectrum UI to display charts incorrectly. This is due to the difference between the Spectrum UI in 6.2 and previous versions. **Workaround:** Use the command **ap spectrum clear-webui-view-settings** on the controller to delete the saved preferences.
77542	**Symptom:** Upgrading from a local file does not work on the 600 Series controller. **Scenario**: For the local file upgrade to be successful, the controller must have at least 75 MB of free memory. When upgraded to ArubaOS 6.2, the 600 Series controller has only 77 MB of free memory remaining. And when the browser UI is launched, the free memory is decreased to 75 MB. In this case, the local file upgrade will fail. It is recommended that you do not use the local file upgrade function in the controller has less than 80 MB of free memory. **Workaround:** None. Use the USB, TFTP, SCP, or CLI option to upgrade instead.
77548 80604	**Symptom**: Accessing any page of the controller's WebUI generates a **Null** error message. **Scenario**: This issue occurs due to an internal error in a process that affects how commands are executed in a WebUI session. This issue is not limited to any controller model or version of ArubaOS. **Workaround**: None.

Table 65: *WebUI Known Issues*

Bug ID	Description
80233 82724	**Symptom**: The **Monitoring > Access Points** and **Monitoring > Network > All Access Points** pages of the controller WebUI show APs as down, even they are shown as up in the command-line interface. **Scenario**: This issue occurs on a master/local topology with one 6000 master controller and two local controllers running ArubaOS 6.2.1.0. **Workaround**: None.
82611	**Symptom**: The **Dashboard > Access Points** page of the WebUI of a controller running ArubaOS 6.2.0.3 does not correctly display AP information. **Scenario**: Accessing the **Dashboard > Access Points** page can trigger the following error in the controller log files: **An internal system error has occurred at file mon_mgr.c function mon_mgr_proc_trend_query line 4142 error PAPI_Send failed: Cannot allocate memory**. This issue was not related to a memory allocation error. **Workaround**: None.

Issues Under Investigation

The following issues have been reported in ArubaOS but not confirmed. The issues have not been able to be reproduced and the root cause has not been isolated. They are included here because they have been reported to Aruba and are being investigated. In the tables below, similar issues have been grouped together.

AP Wireless

Table 66: *AP Wireless Issues Under Investigation*

Bug ID	Description
84779	**Symptom:** Alcatel-Lucent OmniTouch 8118 WLAN handsets are unable to associate to an access points running ArubaOS 6.2 or later releases. Investigations into this issue indicate that the AP transmits beacons, but the client device does not send probe requests.

Controller Datapath

Table 67: *Controller Datapath Issues Under Investigation*

Bug ID	Description
84071	**Symptom:** A 3600 controller running ArubaOS 6.2.1.1 stopped responding and rebooted. The cause for this issue has not been identified.

Controller Platform

Table 68: *Controller Platform Issues Under Investigation*

Bug ID	Description
82402	**Symptom**: A controller unexpectedly reboots with the reason **httpd_wrap process died**. This issue occurs in 3400 controllers running ArubaOS 6.2.1.0 and later and is under investigation.

Startup Wizard

Table 69: *Startup Wizard Issues Under Investigation*

Bug ID	Description
85533	**Symptom**: The **Configuration > WIZARDS > Campus WLAN** page of a controller's WebUI, creating a new WLAN SSID with only "$" text as the name of the SSID does not allow you to go to the next step after the **Captive Portal** page. This issue is under investigation and not specific to any controller model or release version. **Workaround**: Do not create a WLAN SSID with name "$" text only.

Upgrade Procedures

This chapter details software upgrade procedures. Aruba best practices recommend that you schedule a maintenance window for upgrading your controllers.

CAUTION

Read all the information in this chapter before upgrading your controller.

Topics in this chapter include:

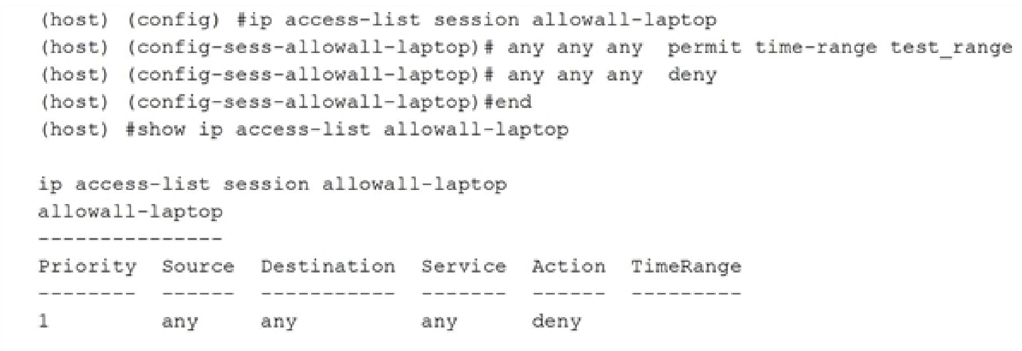
Upgrade Caveats

Before upgrading to any version of ArubaOS 6.3, take note of these known upgrade caveats.

- The local file upgrade option in the 7200 Series controller WebUI does not work when upgrading from ArubaOS 6.2. When this option is used, the controller displays the error message “Content Length exceed limit” and the upgrade fails. All other upgrade options work as expected.
- AirGroup
  - Starting from ArubaOS 6.3, AirGroup is enabled by default. Upgrading the access controller from any version of ArubaOS to ArubaOS 6.3 converts the access controller to integrated mode controller. To continue to be in overlay mode, you must disable AirGroup on the access controller running ArubaOS 6.3.
  - If you migrate from an overlay mode to an integrated mode, you must remove the already configured redirect ACLs from the user roles and remove the L2 GRE tunnel from the access controller. Aruba recommends to remove the overlay controller from the network or disable AirGroup on it.
- ArubaOS 6.3 does not allow you to create redundant firewall rules in a single ACL. ArubaOS will consider a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
  - source IP/alias
  - destination IP/alias
  - proto-port/service

  If you are upgrading from ArubaOS 6.1 or earlier and your configuration contains an ACL with redundant firewall rules, upon upgrading, only the last rule will remain.

  For example, in the below ACL, both ACE entries could not be configured in ArubaOS 6.3. Once the second ACE entry is added, the first would be over written.



```
(host) (config) #ip access-list session allowall-laptop
(host) (config-sess-allowall-laptop)# any any any  permit time-range test_range
(host) (config-sess-allowall-laptop)# any any any  deny
(host) (config-sess-allowall-laptop)#end
(host) #show ip access-list allowall-laptop

ip access-list session allowall-laptop
allowall-laptop
---------------
Priority  Source  Destination  Service  Action  TimeRange
--------  ------  -----------  -------  ------  ---------
1         any     any          any      deny
```

- When upgrading the software in a multi-controller network (one that uses two or more Aruba controllers), special care must be taken to upgrade all the controllers in the network and to upgrade them in the proper sequence.(See Upgrading in a Multi-Controller Network on page 67.)
- The local file upgrade option in the WebUI may not work when upgrading the 7200 Series controller. When this option is used, the controller may display the error message “Content Length exceed limit” and the upgrade fails. All other upgrade options work as expected.
- Upgrading from a local file does not work on the 600 Series controller. Use other upgrade options. See bug ID 77542 in Table 65 for details.
- Upon upgrading to ArubaOS 6.3, the internal AP of the 651 controller will be disabled. The 651 will appear as 650 in ArubaOS and function as 650.
- 3200 controllers with 1 GB of memory (Serial Number DG000XXXX) can be upgraded to ArubaOS 6.3. The 3200 controller with 512 MB of memory (Serial Number DK000XXXX) is not supported by ArubaOS 6.3. To upgrade to the 1 GB version of 3200 controller, please contact Aruba Support and arrange for a replacement.

Installing the FIPS Version of ArubaOS 6.3.0.1

Before you install a FIPS version of software on a controller that is currently running a non-FIPS version of the software, you must reset the configuration to the factory default or you will not be able to login to the CLI or WebUI. Do this by running the **write erase** command just prior to rebooting the controller. This is the only supported method of moving from non-FIPS software to FIPS software.

Important Points to Remember and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions listed below. You should save this list for future use.

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any other changes to your network during the upgrade, such as configuration changes, hardware upgrades, or changes to the rest of the network. This simplifies troubleshooting.
- Know your network and verify the state of your network by answering the following questions.
  - How many APs are assigned to each controller? Verify this information by navigating to the **Monitoring > Network All Access Points** section of the WebUI, or by issuing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the controller (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS is currently on the controller?
  - Are all controllers in a master-local cluster running the same version of software?
  - Which services are used on the controllers (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.

- If possible, use FTP to load software images to the controller. FTP is faster then TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to ArubaOS 6.3.0.1, assess your software license requirements and load any new or expanded licenses you require. For a detailed description of these new license modules, refer to the “Software Licenses” chapter in the *ArubaOS 6.3 User Guide*.

Memory Requirements

All Aruba controllers store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the controller. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. To maintain the reliability of your WLAN network, Aruba recommends the following compact memory best practices:

- Issue the **show memory** command to confirm that there is at least 40 MB of free memory available for an upgrade using the CLI, or at least 60 MB of free memory available for an upgrade using the WebUI. Do not proceed unless this much free memory is available. To recover memory, reboot the controller. After the controller comes up, upgrade immediately.
- Issue the **show storage** command to confirm that there is at least 60 MB of flash available for an upgrade using the CLI, or at least 75 MB of flash available for an upgrade using the WebUI.

CAUTION

In certain situations, a reboot or a shutdown could cause the controller to lose the information stored in its compact flash card. To avoid such issues, it is recommended that you issue the **halt** command before power cycling.

If the output of the **show storage** command indicates that insufficient flash memory space is available, you must free up additional memory. Any controller logs. crash data or and flash backups should be copied to a location off the controller, then deleted from the controller to free up flash space. You can delete the following files from the controller to free memory before upgrading:

- **Crash Data:** Issue the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 66 to copy the **crash.tar** file to an external server, then issue the command **tar clean crash** to delete the file from the controller.
- **Flash Backups:** Use the procedures described in Backing up Critical Data on page 66 to back up the flash directory to a file named **flash.tar.gz**, then issue the command **tar clean flash** to delete the file from the controller.
- **Log files:** Issue the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 66 to copy the **logs.tar** file to an external server, then issue the command **tar clean logs** to delete the file from the controller.

Backing up Critical Data

It is important to frequently back up all critical configuration data and files on the compact flash file system to an external server or mass storage device. At the very least, you should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database

- Floor plan JPEGs
- Custom captive portal pages
- x.509 certificates
- Controller Logs

Back Up and Restore Compact Flash in the WebUI

The WebUI provides the easiest way to back up and restore the entire compact flash file system. The following steps describe how to back up and restore the compact flash file system using the WebUI on the controller:

1. Click on the **Configuration** tab.
2. Click the **Save Configuration** button at the top of the page.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to back up the contents of the compact flash file system to the flashbackup.tar.gz file.
5. Click **Copy Backup** to copy the file to an external server.

   You can later copy the backup file from the external server to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.
6. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page. Click **Restore**.

Back Up and Restore Compact Flash in the CLI

The following steps describe the back up and restore procedure for the entire compact flash file system using the controller's command line:

1. Enter **enable** mode in the CLI on the controller, and enter the following command:
   ```
   (host) # write memory
   ```
2. Use the backup command to back up the contents of the Compact Flash file system to the flashbackup.tar.gz file.
   ```
   (host) # backup flash
   Please wait while we tar relevant files from flash...
   Please wait while we compress the tar file...
   Checking for free space on flash...
   Copying file to flash...
   File flashbackup.tar.gz created successfully on flash.
   ```
3. Use the copy command to transfer the backup flash file to an external server or storage device:
   ```
   (host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword> <remot
   e directory>
   (host) copy flash: flashbackup.tar.gz usb: partition <partition-number>
   ```
   You can later transfer the backup flash file from the external server or storage device to the Compact Flash file system with the copy command:
   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   (host) # copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
   ```
4. Use the restore command to untar and extract the flashbackup.tar.gz file to the compact flash file system:
   ```
   (host) # restore flash
   ```

Upgrading in a Multi-Controller Network

In a multi-controller network (a network with two or more Aruba controllers), special care must be taken to upgrade all controllers based on the controller type (master or local). Be sure to back up all controllers being upgraded, as described in Backing up Critical Data on page 66.

NOTE

For proper operation, all controllers in the network must be upgraded with the same version of ArubaOS software. For redundant (VRRP) environments, the controllers should be the same model.

To upgrade an existing multi-controller system to ArubaOS 6.3.0.1:

1. Load the software image onto all controllers (including redundant master controllers).
2. If all the controllers cannot be upgraded with the same software image and reloaded simultaneously, use the following guidelines:
   a. Remove the link between the master and local mobility controllers.
   b. Upgrade the software image, then reload the master and local controllers one by one.
   c. Verify that the master and all local controllers are upgraded properly.
   d. Connect the link between the master and local controllers.

Upgrading to 6.3.x

Install using the WebUI

CAUTION

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash available for an upgrade using the WebUI. For details, see Memory Requirements on page 66

Upgrading From an Older version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. If you are running one of the following versions of ArubaOS, you must download and upgrade to an interim version of ArubaOS before upgrading to ArubaOS 6.3.

- For ArubaOS 5.0.x versions earlier than ArubaOS 5.0.3.1, download the latest version of ArubaOS 5.0.4.x.
- For ArubaOS versions 6.0.0.0 or 6.0.0.1, download the latest version of ArubaOS 6.0.1.x.

Follow step 2 to step 11 of the procedure described in Upgrading From a Recent version of ArubaOS to install the interim version of ArubaOS, then repeat step 1 to step 11 of the procedure to download and install ArubaOS 6.3.

Upgrading From a Recent version of ArubaOS

The following steps describe the procedure to upgrade from one of the following recent versions of ArubaOS:

- 6.0.1.x or later
- 5.0.3.1 or later

Install the ArubaOS software image from a PC or workstation using the Web User Interface (WebUI) on the controller. You can also install the software image from a TFTP or FTP server using the same WebUI page.

1. Download ArubaOS 6.3.0.1 from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Log in to the ArubaOS WebUI from the PC or workstation.
4. Navigate to the **Maintenance > Controller > Image Management** page. Select the **Upload Local File** option, then click **Browse** to navigate to the saved image file on your PC or workstation.
5. Select the downloaded image file.
6. In the **partition to upgrade** field, select the non-boot partition.
7. In the **Reboot Controller After Upgrade** option field, best practices is to select **Yes** to automatically reboot after upgrading. If you do not want the controller to reboot immediately, select **No**. Note however, that the upgrade will not take effect until you reboot the controller.

8. In Save **Current Configuration Before Reboot** field, select **Yes**.
9. Click **Upgrade**.
10. When the software image is uploaded to the controller, a popup window displays the message **Changes were written to flash successfully**.Click **OK**. If you chose to automatically reboot the controller in step 7, the reboot process starts automatically within a few seconds (unless you cancel it).
11. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > Controller > Controller Summary** page to verify the upgrade.

Once your upgrade is complete, perform the following steps to verify that the controller is behaving as expected.

1. Log in into the WebUI to verify all your controllers are up after the reboot.
2. Navigate to **Monitoring > Network Summary** to determine if your APs are up and ready to accept clients.
3. Verify that the number of access points and clients are what you would expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a back up of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 66 for information on creating a backup.

Install using the CLI

CAUTION

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash available for an upgrade using the CLI. For details, see Memory Requirements on page 66

Upgrading From an Older version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. If you are running one of the following versions of ArubaOS, you must download and upgrade to an interim version of ArubaOS before upgrading to ArubaOS 6.3.0.1.

- For ArubaOS 5.0.x versions earlier than ArubaOS 5.0.3.1, download the latest version of ArubaOS 5.0.4.x.
- For ArubaOS versions 6.0.0.0 or 6.0.0.1, download the latest version of ArubaOS 6.0.1.x.

Follow step 2 - step 7 of the procedure described in Upgrading From a Recent version of ArubaOS to install the interim version of ArubaOS, then repeat step 1 to step 7 of the procedure to download and install ArubaOS 6.3.

Upgrading From a Recent version of ArubaOS

The following steps describe the procedure to upgrade from one of the following recent versions of ArubaOS:

- 6.0.1.x or later
- 5.0.3.1 or later.

To install the ArubaOS software image from a PC or workstation using the Command-Line Interface (CLI) on the controller:

1. Download ArubaOS 6.3 from the customer support site.
2. Open a Secure Shell session (SSH) on your master (and local) controller(s).
3. Execute the **ping** command to verify the network connection from the target controller to the SCP/FTP/TFTP server:

   ```
   (hostname)# ping <ftphost>
   ```

   or

   ```
   (hostname)# ping <tftphost>
   ```

   or

   ```
   (hostname)# ping <scphost>
   ```

4. Use the **show image version** command to check the ArubaOS images loaded on the controller's flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

```
(hostname) #show image version
----------------------------------
Partition               : 0:0 (/dev/ha1)
Software Version        : ArubaOS 6.1.1.0 (Digitally Signed - Production Build)
Build number            : 28288
Label                   : 28288
Built on                : Thu Apr 21 12:09:15 PDT 2012
----------------------------------
Partition               : 0:1 (/dev/ha1)**Default boot**
Software Version        : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)
Build number            : 33796
Label                   : 33796
Built on                : Fri May 25 10:04:28 PDT 2012
```

5. Use the **copy** command to load the new image onto the non-boot partition:

```
(hostname)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
```

or

```
(hostname)# copy tftp: <tftphost> <image filename> system: partition <0|1>
```

or

```
(hostname)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
```

or

```
(hostname)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
```

NOTE

The USB option is only available on the 7200 Series controllers.

6. Execute the **show image version** command to verify the new image is loaded:

```
(hostname)# show image version

----------------------------------
Partition               : 0:1 (/dev/ha1) **Default boot**
Software Version        : ArubaOS 6.3.0.1 (Digitally Signed - Production Build)
Build number            : 38319
Label                   : 38319
Built on                : Fri June 07 00:03:14 PDT 2013
----------------------------------
Partition               : 0:1 (/dev/ha1)
Software Version        : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)
Build number            : 33796
Label                   : 33796
Built on                : Fri May 25 10:04:28 PDT 2012
```

7. Reboot the controller:

```
(hostname)# reload
```

8. Execute the **show version** command to verify the upgrade is complete.

```
(hostname)# show version
```

Once your upgrade is complete, perform the following steps to verify that the controller is behaving as expected.

1. Log in into the command-line interface to verify all your controllers are up after the reboot.
2. Issue the command **show ap active** to determine if your APs are up and ready to accept clients.

3. Issue the command **show ap database** to verify that the number of access points and clients are what you would expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 66 for information on creating a backup.

Downgrading

If necessary, you can return to your previous version of ArubaOS.

WARNING

If you upgraded from 3.3.x to 5.0, the upgrade script encrypts the internal database. New entries created in ArubaOS 6.3.0.1 are lost after the downgrade (this warning does not apply to upgrades from 3.4.x to 6.1).

CAUTION

If you do not downgrade to a previously-saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from ArubaOS 6.3.0.1 to 5.0.3.2, changes made to WIPS in 6.x prevents the new predefined IDS profile assigned to an AP group from being recognized by the older version of ArubaOS. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.

These new IDS profiles begin with ids-transitional while older IDS profiles do not include transitional. If you think you have encountered this issue, use the `show profile-errors` and `show ap-group commands` to view the IDS profile associated with AP Group.

CAUTION

When reverting the controller software, whenever possible, use the previous version of software known to be used on the system. Loading a release not previously confirmed to operate in your environment could result in an improper configuration.

Before you Begin

Before you reboot the controller with the pre-upgrade software version, you must perform the following steps:

1. Back up your controller. For details, see Backing up Critical Data on page 66.
2. Verify that control plane security is disabled.
3. Set the controller to boot with the previously-saved pre-6.3 configuration file.
4. Set the controller to boot from the system partition that contains the previously running ArubaOS image.

   When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next controller reload. An error message displays if system boot parameters are set for incompatible image and configuration files.
5. After downgrading the software on the controller:
   - Restore pre-6.3 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.3.0.1 flash backup file.
   - You do not need to re-import the WMS database or RF Plan data. However, if you have added changes to RF Plan in ArubaOS 6.3.0.1, the changes do not appear in RF Plan in the downgraded ArubaOS version.
   - If you installed any certificates while running ArubaOS 6.3.0.1, you need to reinstall the certificates in the downgraded ArubaOS version.

Downgrading using the WebUI

The following sections describe how to use the WebUI to downgrade the software on the controller.

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the controller by navigating to the **Maintenance > File > Copy Files** page.

   a. For **Source Selection**, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the pre-upgrade configuration file.
   b. For **Destination Selection**, enter a filename (other than default.cfg) for Flash File System.
2. Set the controller to boot with your pre-upgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved pre-upgrade configuration file from the Configuration File menu.
   b. Click **Apply**.
3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition):
   a. Enter the FTP/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
4. Navigate to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the system partition that contains the pre-upgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The controller reboots after the countdown period.
6. When the boot process is complete, verify that the controller is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

Downgrading using the CLI

The following sections describe how to use the CLI to downgrade the software on the controller.

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the controller:

```
(host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
or
(host) # copy tftp: <tftphost> <image filename> system: partition 1
```

2. Set the controller to boot with your pre-upgrade configuration file.

```
# boot config-file <backup configuration filename>
```

3. Execute the **show image version** command to view the partition on which your previous software image is stored. You cannot load a new image into the active system partition (the default boot).

   In the following example, partition 0, the backup system partition, contains the backup release 6.1.3.2. Partition 1, the default boot partition, contains the ArubaOS 6.3.0.1 image:

```
#show image version
----------------------------------
Partition               : 0:1 (/dev/ha1)
Software Version        : ArubaOS 6.3.0.1(Digitally Signed - Production Build)
Build number            : 33796
Label                   : 33796
Built on                : Fri May 25 10:04:28 PDT 2012
----------------------------------
Partition               : 0:1 (/dev/hda2) **Default boot**
Software Version        : ArubaOS 6.3.0.1(Digitally Signed - Production Build)
Build number            : 38319
Label            : 38319
Built on                : Fri June 07 00:03:14 2013
```

4. Set the backup system partition as the new boot partition:

```
# boot system partition 0
```

5. Reboot the controller:

```
# reload
```

6. When the boot process is complete, verify that the controller is using the correct software:

```
# show image version
```

Before You Call Technical Support

Before you place a call to Technical Support, follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the Aruba controller with IP addresses and Interface numbers if possible).
2. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless NIC make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
3. Provide the controller logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
4. Provide the syslog file of the controller at the time of the problem. Aruba strongly recommends that you consider adding a syslog server if you do not already have one to capture logs from the controller.
5. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have an outage in a network that worked in the past, a network configuration that has never worked, or a brand new installation.
6. Let the support person know if there are any recent changes in your network (external to the Aruba controller) or any recent changes to your controller and/or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) when the problem first occurred.If the problem is reproducible, list the exact steps taken to recreate the problem.
8. Provide any wired or wireless sniffer traces taken during the time of the problem.
9. Provide the controller site access information, if possible.