ArubaOS 6.3.1.2

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 for 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 vendor's 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 an Aruba warranty. For details, see the Aruba Networks standard warranty terms and conditions

Chapter 1
Release Overview

ArubaOS 6.3.1.2 is a software patch release that introduces fixes to the issues identified in the previous ArubaOS releases. For details on the features described in the following sections, see the *ArubaOS 6.3.1 User Guide* and *ArubaOS 6.3.1 CLI Reference Guide*.

NOTE

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

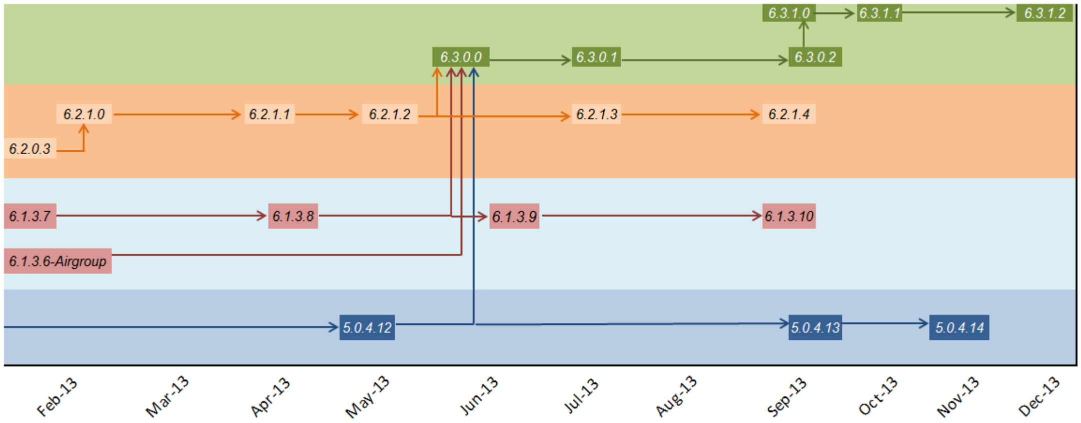
Contents Overview

- What's New in this Release describes the new fixes, known issues, and enhancements introduced in this release.
- Features Added in Previous Releases provides description of features and enhancements added in previous releases of ArubaOS 6.3.1.x.
- Issues Resolved in Previous Releases provides a description of issues resolved in ArubaOS 6.3.1.x.
- Known Issues and Limitations in Previous Releases provides a description and workaround for the issues identified in previous releases of ArubaOS 6.3.1.x.
- Upgrade Procedures describes the procedures for upgrading a controller to ArubaOS 6.3.1.x.

Release Mapping

The following illustration shows the patch and maintenance releases that are included in their entirety in ArubaOS 6.3.1.2.

Figure 1 *ArubaOS Releases and Code Stream Integration*



Supported Browsers

The following browsers are officially supported to use with ArubaOS 6.3.1.2 WebUI:

- Microsoft Internet Explorer 10.x, and 11.0, on Windows XP, Windows Vista, Windows 7, and Windows 8
- Mozilla Firefox 23 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*

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/aruba-support-program/contact-support/
Software Licensing Site	licensing.arubanetworks.com/login.php
End of Support Information	www.arubanetwroks.com/support-services/end-of-life-products/end-of-life-policy
Wireless Security Incident Response Team (WSIRT)	arubanetworks.com/support/wsirt.php
Support Email Addresses	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
Wireless Security Incident Response Team (WSIRT)	wsirt@arubanetworks.com

This chapter describes regulatory changes and lists bugs fixed in the ArubaOS 6.3.1.2 release. In addition, it lists bugs discovered since the prior release but not resolved yet, and lists customer issues currently under investigation.

Regulatory Updates

The following table describes regulatory enhancements introduced in 6.3.1.2.

Table 2: *Regulatory Domain Updates*

Regulatory Domain	Change
Australia, Saudi Arabia, New Zealand, Singapore, Taiwan, Qatar, UAE, Columbia, Thailand, Chile, Hong Kong, Malaysia, Hong Kong	Added support for AP-114 and AP-115.
Thailand	Added support for AP-109.
Taiwan	Added support for AP-108 and AP-109.
China	Added support for AP-115.

Resolved Issues

The following issues are resolved in ArubaOS 6.3.1.2.

802.1X

Table 3: *802.1X Fixed Issues*

Bug ID	Description
89106	**Symptom**: When previously idle clients reconnected to the network, a configured CLASS attribute was missing from the accounting messages sent from the RADIUS server. This issue is resolved with the introduction of the **delete-keycache** parameter in the 802.1X authentication profile. When this parameter is enabled, it deletes the user keycache when the client's user entries get deleted. This forces the client to complete a full 802.1X authentication process when the client reconnects after an idle timeout, so the CLASS attributes will again be sent by the RADIUS servers. **Scenario**: This issue occurred in a deployment using RADIUS accounting, where the RADIUS server pushed CLASS attributes in the access-accept messages for 802.1X authentication. When an idle user timed out from the network, ArubaOS deleted the CLASS attribute for the user along with rest of the user data.
92564	**Symptom**: Clients experienced authentication failure when they used 802.1 x authentication. This issue is resolved by increasing the stack size. **Scenario**: The issue occurred due to stack overflow which caused memory corruption. This issue was observed in 600 Series controllers and 3000 Series controllers running ArubaOS 6.1 and 6.2.

AirGroup

Table 4: *AirGroup Fixed Issues*

Bug ID	Description
88522 92368	**Symptom:** The multicast Domain Name System (mDNS) process of AirGroup crashed and restarted in a controller. This issue is resolved by blocking the memory leak to ensure that the controller is not crashing when the maximum number of servers and users supported on each platform is exceeded. **Scenario:** This issue was triggered when the number of AirGroup users exceeded the limit set for the platform. This issue was observed in controllers running ArubaOS 6.3 or earlier versions.

Air Management- IDS

Table 5: *Air Management- IDS Fixed Issues*

Bug ID	Description
90330	**Symptom**: An adhoc AP marked to be manually contained would not be contained unless the protect from adhoc feature was enabled. This issue is resolved by allowing traditional adhoc containment whenever enhanced adhoc protection is enabled, even if the protect from adhoc feature is not enabled. **Scenario:** This issue was observed in controllers running ArubaOS 6.2.x.

AP-Datapath

Table 6: *AP-Datapath Fixed Issues*

Bug ID	Description
90645	**Symptom:** The **show datapath session ap-name** command output did not display **ap-name** option. The command output is now displayed correctly even if the **ap-name** parameter is used. **Scenario:** This issue was observed in controllers running ArubaOS 6.2.1.3 and was not limited to any specific controller model.
94067	**Symptom:** The VLAN in the wired AP is different from the AP's native VLAN. **Scenario:** This issue occurred on the AP-93H device connected to controllers running any ArubaOS version. This issue occurred because the wired driver did not support the extra two bytes used by the internal switch chip.

AP-Platform

Table 7: *AP-Platform Fixed Issues*

Bug ID	Description
86096	**Symptom:** When multiple DNS servers were configured in a local RAP DHCP pool, only the first server in the DNS server list was available to the DHCP client. **Scenario**: This issue was observed in RAPs that were configured to use a local DHCP server and were running ArubaOS 6.2 or 6.3. This issue occurred due to incorrect handling of the DNS servers configured by SAPD.

Table 7: *AP-Platform Fixed Issues*

Bug ID	Description
88389 89882 90175 90332	**Symptom:** 802.11n-capable access points unexpectedly rebooted. The log files for the event listed the reason for the reboot as **kernel page fault**. Improvements in the wireless driver of the AP resolved this issue. **Scenario:** This issue was observed when an 802.11n-capable campus AP was in bridge forwarding mode and there was a connectivity issue between the AP and the controller. This issue was observed in 802.11n-capable access points running any version of ArubaOS.
89041	**Symptom:** A 802.11n-capable access point unexpectedly rebooted or failed to respond. This issue was resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario**: This issue was observed when a client disconnected from the network. The issue occurred on 802.11n access points running ArubaOS 6.3.0.1.
89016	**Symptom**: The SNMP OID **wlanStaAccessPointESSID** had no value when a client roamed from a down AP to an active AP. Improvements to internal processes that managed Layer-2 roaming resolved this issue. **Scenario**: This issue was observed in controllers running ArubaOS 6.2, when clients roamed between APs.
89691 94047	**Symptom**: APs stopped responding and rebooted. The log files for the event listed the reason for the crash as **kernel page fault**. A change in the route cache has fixed this issue. **Scenario**: This issue occurred when the deletion of the route cache was interrupted. This issue was not limited to any specific controller model or release version.
91803	**Symptom**: The AP-120 failed due to insufficient memory caused by heavy traffic. Improvements to the wireless drivers resolved this issue. **Scenario**: This issue was observed in AP-120 connected to controllers running ArubaOS 6.3.1.0
91820	**Symptom:** An AP crashed and rebooted frequently and the log file for the event listed the reason for the reboot as **Kernel Panic**. Updates to the wireless driver fixed this issue. **Scenario:** This issue occurred while receiving and freeing the buffer memory. This issue was observed in AP-135 access points running ArubaOS 6.3.1.0.
91937	**Symptom:** AP-92 and AP-93 access points were unable to come up with ArubaOS 6.3.x.x-FIPS. ArubaOS 6.3.x.x-FIPS now supports AP-92 and AP-93 access points. **Scenario:** When upgrading to ArubaOS 6.3.x.x.-FIPS, the image size was too big to fit into AP-92's or AP-93's 8MB flash, and hence was rejecting these access points to come up although these access points required to be supported with 16MB flash. **NOTE:** Due to the infrastructure limitation, to support 16MB flash, the code block for 8MB flash had to be removed as well. So, AP-92 and AP-93 access points with 8MB flash will also come up with ArubaOS 6.3.x.x-FIPS but it is not supported. Only AP-92 and AP-93 access points with 16MB flash is supported with ArubaOS 6.3.x.x-FIPS.
91963	**Symptom:** An AP rebootstrapped with the **Wrong cookie in request** error after a failover from one controller to other. This issue is fixed by enhancements to drop the error message if an AP detected a cookie mismatch when the error message came from a different controller than the current LMS. **Scenario:** This issue occurred after a failover of an AP from one controller to other and when the AP received the messages from old controller and incorrectly identified as a cookie mismatch. This issue was observed in controllers in a master-local topology with a primary and backup Local Management Switch (LMS) configured.
89514 92163 93504	**Symptom:** An AP-220 Series access point rebooted repeatedly when connected to a Power over Ethernet (PoE) switch, without storing a reboot reason code in the flash memory of the AP. Design changes to the AP-220 Series code fixed this issue. **Scenario:** This issue was observed in AP-220 Series running ArubaOS 6.3.x and later versions.

Table 7: *AP-Platform Fixed Issues*

Bug ID	Description
92245	**Symptom:** An AP does not respond and displays an error message - **aruba_valid_rx_sig: Freed packet on list at ath_rx_tasklet+0x138/0x2880…**…. A manual power cycle was required to restore the AP to the normal status. This issue is resolved by adding an assertion. **Scenario:** This issue was observed in AP-125 access points connected to controllers running ArubaOS 6.3.1.
92572	**Symptom:** APs stopped responding and crashed due to a higher utilization of memory caused by the client traffic. A change in the AP memory management has resolved this issue. **Scenario:** This issue was observed in ArubaOS 6.2 and later versions, but was not limited to any specific controller model.
93067	**Symptom:** The authorization for users was unexpectedly revoked and the **show ap client trail-info** CLI command displayed the reason as **Ptk Challenge Failed**. Sending the Extensible Authentication Protocol over LAN (EAPoL) packets as best effort traffic instead of voice traffic resolved this issue. **Scenario:** This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.1 when virtual AP is configured with WPA-802.1X-AES encryption.

AP-Regulatory

Table 8: *AP-Regulatory Fixed Issues*

Bug ID	Description
86764	**Symptom**: The output of the **show ap allowed channels** command incorrectly indicated that AP-68 and AP-68P supported 5 GHZ channels. This issue is resolved by modifying the output displayed for the allowed channel list for AP-68 and AP-68P APs. **Scenario:** This issue was observed in AP-68 and AP-68P running ArubaOS 6.1.x.x and 6.2.x.x.

AP-Wireless

Table 9: *AP-Wireless Fixed Issues*

Bug ID	Description
67847 69062 69346 71530 74352 74687 74792 75212 75792 75944 76142 76217 76715 77273 77275 78118 80735 82147 83242 83243 83244 83624 83833 84170 84339 84511 85015 85054 85086 85367 85959 88515 89136 89253 89256 89816 90603 91084 92871 92877 92878 92879 93923	**Symptom:** APs unexpectedly rebooted and the log files listed the reason for reboot as **Data BUS error**. A change in the exception handling module has fixed this issue. **Scenario:** This issue was observed in the AP-120 Series and AP-68P connected to controllers running ArubaOS 6.3.1.2.

Table 9: *AP-Wireless Fixed Issues*

Bug ID	Description
69424 75874 78978 78981 79891 80054 87250 88619 88620 88989 89537 91689 93455 93811	**Symptom:** When upgraded to ArubaOS 6.2, AP-125 crashed and rebooted. Reallocating the ArubaOS loading address in memory fixed the issue. **Scenario:** This issue was observed when controllers were upgraded to ArubaOS 6.2 from ArubaOS 6.1.3.2 and later in any deployment with an AP-125.
88741	**Symptom:** The degradation in performance occurred due to settings made in the preferred-access. **Scenario:** This issue was caused by an internal ArubaOS malfunction and was observed only in AP-225.
88328 89623	**Symptom:** Wireless clients experienced packet loss when connected to remote APs in bridge mode. The fix ensures that some buffer is reserved for transmitting unicast traffic. **Scenario:** This issue was observed in AP-105 access points connected to controllers running ArubaOS 6.1.3.8 when there was a heavy multicast or broadcast traffic in the network.
89442	**Symptom:** The AP-220 Series devices crashed frequently. **Scenario:** This issue occurred when the radio mode was altered between Monitor and Infrastructure. This issue was observed only in AP-220 Series devices running ArubaOS 6.3.1.2.
89460	**Symptom:** When APs used adjacent DFS channels, the AP-135 falsely detected RADAR and exhausted all DFS channels. If no non-DFS were enabled, the AP stopped responding to clients. **Scenario:** This issue was observed in an AP-135 running ArubaOS6.3.x and 6.2.x. It was caused when APs used adjacent DFS channels.
89735 89970 90572 91140 91560 91620 92017 92428 93373	**Symptom:** The Ethernet interface of an 802.11ac capable AP restarted frequently. Changes in the internal code fixed this issue. **Scenario:** This issue was observed in AP-220 Series connected to controllers running ArubaOS 6.3.1.0 and later version.
90065	**Symptom:** AP-125 rebooted unexpectedly. Improvements to the wireless driver has resolved this issue. **Scenario:** This issue was observed in AP-125 access points connected to controllers running ArubaOS 6.1.3.9.
90960	**Symptom**: Microsoft® Surface Pro and Surface RT clients were unable to acquire an IP address or correctly populate the ARP table with a MAC address when connecting to an AP using 20 MHz channels on 2.4 GHz or 5 GHz radios. This issue is resolved by channel scanning improvements to APs in 20 Mhz mode. **Scenario**: This issue was triggered when Microsoft Surface clients running Windows 8 or Windows 8.1 connected to 20 MHz APs running ArubaOS 6.1.3.8.

Table 9: *AP-Wireless Fixed Issues*

Bug ID	Description
91379	**Symptom:** AP-220 Series access points unexpectedly crashed. Using the correct structure to fill the information in the outgoing response frame resolved this issue. **Scenario:** The 802.11k enabled client that sent a Neighbor Report Request frame caused the AP-220 Series to crash when the packet was freed. This issue was observed in AP-220 Series running ArubaOS 6.3.x.
91856	**Symptom:** Certain 802.11b clients did not communicate with Aruba 802.11n-capable access points. Improvements to the wireless driver of 802.11n-capable access points resolved the issue. **Scenario:** This issue was observed when Denso® 802.11b handy terminals communicated with Aruba 802.11n-capable access points on channel 7. This issue was not limited to a specific controller model or release version.
91946 92052 92550 92552 92554 92555 92557 92559 92561 92562 92788 92976 92977	**Symptom:** AP-135 stopped responding and rebooted. Improvements to the wireless driver in ArubaOS 6.1.3.2 resolved the issue. **Scenario:** This issue occurred when the buffer was corrupted in the wireless driver. This issue was observed in AP-135 access points connected to controllers running ArubaOS 6.3.1.0.
92346	**Symptom:** When the 80MHz option in the rf arm-profile was enabled or disabled, HT Capabilities in the beacon showed only 20MHz Support. This issue was resolved by ensuring that the profile enable and disable function operates properly. **Scenario:** This issue was observed in AP-225 access points connected to controllers running ArubaOS 6.3.1.0.
92626	**Symptom:** An AP crashed and the log files for the event listed the reason for the crash as **kernel panic**. This issue was fixed by referencing the valid memory. **Scenario:** This issue occurred when an invalid memory was referenced. This issue occurred in AP-220 Series access points running ArubaOS 6.3.1.1.
93710	**Symptom:** Vocera clients associated to an AP were unable to communicate with the Vocera server. This issue was resolved by limiting the multicast transmission rate so that the unicast transmission is not affected. **Scenario:** This issue occurred when multicast traffic blocked hardware and software queues resulting in unicast packets being dropped. This issue is observed in AP-225 connected to controllers running ArubaOS 6.3.1.1.
94059	**Symptom:** An AP rebooted unexpectedly. This issue was resolved by MAC address bit manipulation. **Scenario:** This issue was observed in AP-120 Series when the controllers were upgraded from ArubaOS 6.1.3.7 to 6.1.3.9, but was not limited to a controller model.
94155	**Symptom:** An AP-225 device rebooted unexpectedly when connected to a PoE. This issue was resolved by making code level changes in the index table. **Scenario:** This issue occurred due to the drastic peak in power when AP-225 is connected to 3af PoE (Power over Ethernet) and operates in low-power mode. This issue was observed in AP-225 connected to controllers running ArubaOS.

Base OS Security

Table 10: *Base OS Security Fixed Issues*

Bug ID	Description
86141 93351 93726	**Symptom:** Issuing the **show global-user-table list** command displayed duplicate client information. Ignoring the master controller IP query in LMS list fixed the issue. **Scenario:** This issue was observed in a VRRP or master-local deployment whereby the master controller queried itself and the LMS list resulting in duplicate client information. This issue was observed in controllers running ArubaOS 6.3.X.0.
89453	**Symptom**: The show rights command did not display all the user roles configured in the controller. This issue is resolved by a change that ensures that the output of this command displays all the user roles configured on the controller. **Scenario**: This issue was observed when more than 50 user roles were configured in a controller running ArubaOS 6.2.1.3.
89676	**Symptom:** Users could not authenticate to the TACACS server as TCP handshake failed and the aaa-test-server with TACAS displayed two different messages - **auth module busy** and **authentication is successful** for the same controller running a similar image version. **Scenario**: This issue was observed in controllers running ArubaOS 6.1.3.7 or 6.4, but is not limited to a specific hardware model.
90180	**Symptom:** Re-authentication of the management users was not triggered upon password change. The users are now getting **Password changed, please re-authenticate** message on the console, forcing the user to login again with the new password. **Scenario**: The issue was observed when users were already connected, and password for these users was changed. The re-authentication message for these users was not shown. This issue was not limited to any specific controller model or ArubaOS version.
90209	**Symptom:** A controller rebooted unexpectedly due to an internal process (datapath) timeout. **Scenario:** The timeout occurred due to a VIA client sending an SSL fallback packet, where the third SSL record encapsulating the IPSec packet had an invalid IP header. was limited to a specific controller model and was observed in ArubaOS 6.2.1.2.
90233	**Symptom:** Clients with a logon user role did not age out from the user-table after the logon-lifetime AAA timer expired. This issue was resolved by changing the aged out users to logon users if User Derivation Rule (UDR) is configured in the AAA profile. **Scenario:** This issue was observed when UDR was configured in the AAA profile with logon defined as the default user role. This issue was observed in controllers running ArubaOS 6.2.1.x.
90454	**Symptom**: A remote AP unexpectedly rebooted, because it failed to receive heartbeat responses from the controller. Changes to the order in which new IPsec Security Associations (SAs) are added and older IPsec SAs are removed resolved this issue. **Scenario**: This issue occurred after a random IPsec rekey was triggered and when the outbound IPsec SA was deleted before the inbound IPsec SA was added. This removed the route cache for the inner IP, causing the session entry to incorrectly point to the default gateway, and prevent heartbeat responses from reaching the AP.
92674	**Symptom:** The CLASS attribute was missing in Accounting STOP packet. This issue is resolved by not resetting the counters when an IPv6 user entry is deleted. **Scenario:** This issue occurred when the counters were reset during an IPv6 user entry aged out. This issue was not limited to a specific controller or ArubaOS version.
92817	**Symptom:** Wireless clients were blacklisted even when the rate of the IP Session did not exceed the threshold value set. This issue is resolved by increasing the storage of the threshold to16 bits. **Scenario:** This issue was observed when the threshold of the IP Session rate was set to a value greater than 255. This issue was observed in controllers running ArubaOS 6.x.

Captive Portal

Table 11: *Captive Portal Fixed Issues*

Bug ID	Description
87294 87589 92575	**Symptom:** Captive Portal (CP) whitelist that was mapped to the user-role was not synchronized with the standby controller. Checks in the CP whitelist database fixed this issue. **Scenario:** This issue was observed when a net-destination was created and added to the CP profile whitelist that mapped to the user-role in the master controller. This issue was observed in ArubaOS 6.2.1.2 and not limited to a specific controller model.
91442	**Symptom:** In the **Login** page using the master controller's command line interface, the question mark symbol was neither getting pushed nor getting added to the local controller. This issue is resolved by ensuring that the master controller's command line interface accepts the question mark symbol. **Scenario:** This issue was observed while synchronizing the configuration from the master controller to the local controller.

Controller-Datapath

Table 12: *Controller-Datapath Fixed Issues*

Bug ID	Description
88469	**Symptom:** A controller denied any FTP download that used Extended Passive mode over IPv4. Modifying the FTP ALG to handle Extended Passive mode correctly resolved this issue. **Scenario:** This issue was observed when an IPv4 FTP client used Extended Passive mode. In such a case, the FTP ALG on the controller detected it as a Bounce Attack and denied the session. This issue was not limited to a specific controller model or release version.
93423	**Symptom:** A controller unexpectedly rebooted and the log file listed the reason for the reboot as **Datapath timeout**. This issue is fixed by increasing the stack memory size in the data plane. **Scenario:** This issue was observed when clients using SSL VPN connected to RAP and the controller tried to decompress these packets. This issue was not limited to a specific controller model or a release version.

Controller-Platform

Table 13: *Controller Platform Fixed Issues*

Bug ID	Description
82736 82875 83329 83502 83762 84022 85355 85370 85628 86005 86029 86031 86572 86589 87410 87505 87587 88005 88332 88351 88434 88921 89636 89818 90909 91269 91308 91370 91517 92823 93294 93770	**Symptom:** A controller rebooted unexpectedly. Changes in the watchdog implementation on the controller resolved the issue. **Scenario:** Log files for the event indicated the reasons for the reboot as **soft watchdog reset** or **user pushed reset**. This issue was identified in ArubaOS 6.1.3.x, and is not limited to a specific controller model.

Table 13: *Controller Platform Fixed Issues*

Bug ID	Description
86216 85566 87090 87635 88321 88387 88699 89436 89727 89839 89911 90162 90338 90481 91193 91387 91941 92139 92187 92516 92808 93630 93693 93931 94308	**Symptom:** During a kernel panic or crash, the panic dump generated by the controller was empty. New infrastructure has been added to improve the collection of crash dumps. **Scenario:** This issue impacts 3000 Series, 600 Series, and M3 controllers and was observed on ArubaOS 6.1.3.7.
89155	**Symptom**: 600 Series controllers experienced high level of CPU usage during bootup, which triggered a warning message - **Resource 'Controlpath CPU' has exceeded 30% threshold.** This issue is resolved by changes to the internal CPU threshold that reflects the expected CPU usage levels. **Scenario**: This issue was observed in controllers running ArubaOS 6.1.2.3.
90619 92250	**Symptom:** The controller WebUI stopped responding indefinitely. The fix ensures that the AirWave query fails if there is no firewall visibility. **Scenario:** This issue occurred when AirWave queried for firewall visibility details from a controller on which the firewall visibility feature was disabled. This issue was observed in controllers running ArubaOS 6.2 or later.
91383	**Symptom**: Executing a **show** command causes the controller command-line interface to display an error: **Module Configuration Manager is busy. Please try later**. Improvements to how the controller manages HTTP session keys resolved this issue. **Scenario**: This issue occurred when issuing **show** commands from the command-line interface of a 3000 Series standby controller, and is triggered when the database synchronization process attempts to simultaneously replace and add an HTTP session key in the user database.

DHCP

Table 14: *DHCP Fixed Issues*

Bug ID	Description
90611	**Symptom:** The Dynamic Host Configuration Protocol (DHCP) module crashed on a controller and users were not able to perform a new DHCP configuration. The updates to the DHCP wrapper fixed this issue in ArubaOS 6.3.1.2. **Scenario:** This issue was triggered by a race condition that caused the DHCP wrapper process to crash with continuous restarts. This issue was not specific to a controller model or release version.

GRE

Table 15: *GRE Fixed Issues*

Bug ID	Description
89832	**Symptom:** Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel between L2 connected controllers dropped because of keepalive failures. This issue is fixed by bridging the packets before routing to the forwarding pipeline. **Scenario:** This issue occurred when the GRE tunnel keepalives were enabled and the **Configuration > Network > IP > IP Interface > Edit VLAN (1) > Enable Inter-VLAN Routing** option was disabled. This issue was observed in controllers running ArubaOS 6.3 configured with L2 GRE tunnel between L2 connected switches.

GSM

Table 16: *GSM Fixed Issues*

Bug ID	Description
91870	**Symptom:** The output of the **show ap database** command indicated that a RAP-5 was inactive and that the RAP-5 would not come up. This issue is resolved by increasing the allocation for AP wired ports to 16x. **Scenario:** This issue was observed with RAP-5 APs when all four wired AP ports were enabled in ArubaOS 6.3. ArubaOS 6.3 introduced GSM where space was pre-allocated for the AP wired ports based on the maximum number of APs times the maximum number of wired ports, because RAP-5 has four wired ports and the controller allowed four times the campus APs. As a result, the number of GSM slots was insufficient.

Hardware-Management

Table 17: *Hardware-Management Fixed Issues*

Bug ID	Description
87481	**Symptom:** The 7200 Series controllers failed to generate the controller's internal temperature. Setting the SNMP attribute for temperature in 7200 Series controllers fixed this issue. **Scenario:** This issue was observed when an SNMP walk was performed using the OID.1.3.6.1.4.1.14823.2.2.1.2.1.10. This issue was observed in 7200 Series controllers running ArubaOS 6.3 or later.

IPv6

Table 18: *IPv6 Fixed Issues*

Bug ID	Description
88814	**Symptom:** When clients connected to a controller, they received IPV6 router advertisements from VLANs that they were not associated with. This issue is resolved by updating the datapath with router advertisements conversion flag, so that datapath converts multicast router advertisements to unicast. **Scenario:** This issue was observed in IPv6 networks with derived VLANs and was not limited to a specific controller model or release version.

Licensing

Table 19: *Licensing Fixed Issues*

Bug ID	Description
89294	**Symptom:** RAPs were unable to come up on a standby controller if the AP licenses were installed only on the master controller. **Scenario:** This issue occurred when centralized licensing was enabled and all AP licenses were installed on the master controller and the RAP feature was disabled on the standby controller. This issue was observed in controllers running ArubaOS 6.3.

Local Database

Table 20: *Local Database Fixed Issues*

Bug ID	Description
88019	**Symptom:** A warning message **WARNING: This controller has RAP whitelist data stored in pre-6.3 format, which is consuming ……………..running the command 'local-userdb-ap del all** appeared, when a user logged in to the controller. This issue is fixed by deleting the warning file, when all the old entries are deleted. **Scenario:** This issue occurred when a controller was upgraded from a previous version of ArubaOS to 6.3 or later versions. This issue was not specific to a controller model or release version.

Master-Redundancy

Table 21: *Master-Redundancy Fixed Issues*

Bug ID	Description
80041	**Symptom:** Master-Backup database fails to synchronize with the reason **Last failure cause: Standby switch did not respond to the start request or is not ready**. This issue was resolved by ignoring any aborted database synchronization sequence number on the master controller, so that the subsequent database synchronization can proceed without waiting for a response from the standby controller for the previous aborted database sync. **Scenario:** The standby controller database was out-of-sync with the master controller and any switchover during out-of-sync state caused the controller to be in an inconsistent state. This issue was observed in controllers in a master-standby configuration and was not specific to a release version.

Mobility

Table 22: *Mobility Fixed Issues*

Bug ID	Description
88281	**Symptom:** IP mobility entries were not cleared even when the client leaves the controller and user entries aged out. Additionally, the command **clear ip mobile host <mac-address>** did not clear the stale entry. **Scenario:** This issue was caused by a message loss between the controller's Mobile IP and authentication internal processes. Due to the message loss, the affected clients were blocked. This issue was observed in controllers running ArubaOS 6.3.x, 6.2.x, and 6.1.x.

Mesh

Table 23: *Mobility Fixed Issues*

Bug ID	Description
92614	**Symptom:** A Mesh Point rebooted frequently as it could not connect to a Mesh Portal. This issue was resolved by allowing Mesh Point to use the configured power for transmitting probe requests instead of reduced power. **Scenario:** This issue occurred when the transmission power on the Mesh Point was very low compared to the configured power. This issue was observed in AP-105 and AP-175 connected to controllers running ArubaOS 6.1.x or later versions.

RAP+BOAP

Table 24: *RAP+BOAP Fixed Issues*

Bug ID	Description
86650	**Symptom:** A controller sent continuous RADIUS requests for the clients connected behind wired port of a remote AP (RAP). This issue is resolved by enhancing the code for memory corruption. **Scenario:** This issue was observed when the RAP used PPPoE uplink and wired AP was operating in split-tunnel or bridge mode. This issue occurred in controllers running ArubaOS 6.1.3.6 or later and was not limited to a specific controller model.
91106	**Symptom:** When a Remote Access Point (RAP) was rebooted from the controller using the **apboot** command, the system did not generate a log message. Changes to the internal code for handling log messages fixed this issue. **Scenario:** This issue was observed in RAPs running ArubaOS 6.1 and later versions.

Station Management

Table 25: *Station Management Fixed Issues*

Bug ID	Description
86357	**Symptom:** Station Down messages were not logged in the syslog. Changes to the syslog messaging resolved this issue. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.x.
66261	**Symptom**: A client moving from one virtual AP (VAP) to another could not connect to the new virtual AP. Changes to how ArubaOS allocates VLANs resolve this issue. **Scenario**: This issue occurred when the **even VLAN** and **preserve VLAN** features were enabled in both VAPs, and if the client VLAN defined in the previous VAP did not exist in the new VAP.This issue was first observed in ArubaOS 6.1.3.x, and was not limited to any specific controller model.

SNMP

Table 26: *SNMP Fixed Issues*

Bug ID	Description
83948	**Symptom:** The Simple Network Management Protocol (SNMP) module crashed when the management interface was deactivated while an SNMP query was running. A build option was modified to avoid generating code that may access invalid memory. **Scenario:** This issue was observed when SNMP was enabled and AirWave was used to monitor 620 and 3600 controllers running ArubaOS 6.3.0.0.

WebUI

Table 27: *WebUI Fixed Issues*

Bug ID	Description
88398	**Symptom:** Network administrators were unable to manually contain or reclassify a group of detected rogue APs in the **Dashboard** > **Security** page of the WebUI. This issue is fixed by adding support to classify multiple rouge APs. **Scenario:** This issue occurred when multiple rogue APs were selected in the **Dashboard** > **Security** page. This issue was observed in controllers running ArubaOS 6.2.1.3.
88802 91141	**Symptom:** When the client tried to access the **Air Group** option from the Web UI, the system did not respond. To resolve this issue, the **Air Group** option is now removed from the WebUI for 600 Series controllers. **Scenario:** This issue was observed in 600 Series controllers running ArubaOS 6.3.x.
90110	**Symptom:** The ArubaOS Campus WLAN Wizard was not accessible. This issue is resolved by changing the LDAP server filter to include an ampersand. **Scenario:** The Campus WLAN wizard was not accessible due to the presence of an ampersand (&) in the LDAP server filter. This issue was observed in a 650 controller running ArubaOS 6.2.1.3, but could impact any controller model.
92340 92649	**Symptom:** WebUI of the controller failed to load in Microsoft® Internet Explorer 11 with the error message **can't create XMLHttpRequest object: Object doesn't support property or method 'creatXMLHttpRequest'**. The ArubaOS WebUI is updated to be compatible with Microsoft® Internet Explorer 11. **Scenario:** This issue was not limited to a specific controller model or ArubaOS release version.
93606 93718	**Symptom:** Clients were not displayed in the **Monitoring** > **Controller** > **Clients** page of the WebUI when filtered with AP Name. This issue is fixed by changing the **show user-table location <ap-name>** command to **show user-table ap-name <ap-name>**. **Scenario:** This issue was triggered by changes to CLI commands. This issue was observed in controllers running ArubaOS 6.2 and 6.3.

Voice

Table 28: *Voice Fixed Issues*

Bug ID	Description
77716 88996 90000	**Symptom:** Incompatibility issues were observed between an Aruba 3600 controller and a Cisco CUCM using SCCP version 20. Users were able to make and receive calls using a Cisco phone but there was no audio. This issue is resolved by changes that allow the Aruba controller to handle Open Receive Channel Acknowledge (ORCA) messages for SCCP Version 20. **Scenario:** The Cisco CUCM was compatible with the Skinny Client Control Protocol (SCCP) version 20, while the 3600 controller supported only up to version 17 of the SCCP. This incompatibility issue resulted in media traffic not passing through the 3600 controller as the controller was not able to parse the SCCP signaling packets. This issue was observed in a 3600 controller running ArubaOS 6.0 or later.
86135 87296 88314 88891 89170 89893 90613 91073 91625 92159	**Symptom:** The Station Management (STM) module on a 7240 local controller configured with voice ALGs stopped responding and restarted after idle voice clients aged out. This caused network disruption. This issue is resolved by making code level changes to avoid creation of voice clients with invalid MAC addresses. **Scenario:** This issue occurred in controllers running ArubaOS 6.3.1.0 where AP entries were created as voice clients with invalid MAC address.

Table 28: *Voice Fixed Issues*

Bug ID	Description
86683	**Symptom:** The **show voice call-cdrs** and **show voice client-status** command outputs did not display the call details for Lync wired clients with media classification configured on session ACL. This issue is resolved by handling the message appropriately for wired clients. **Scenario**: This issue was observed when Lync clients were identified as voice clients using media classification. This issue occurred in ArubaOS 6.2 and 6.3 versions, and was not limited to any specific controller version.
88998 90912	**Symptom:** Controllers stopped responding and rebooted due to lack of memory resulting in network disruptions. Enhancements to memory allocation resolved this issue. **Scenario:** The issue occurred when an internal module (STM) crashed due to memory corruption. This issue was observed in controllers running ArubaOS 6.1 and later.
93517	**Symptom:** Access points rebooted unexpectedly resulting in wireless clients to lose network connectivity. Releasing CDR events for AP statistics and AP event in the CDR buffer resolved the issue. **Scenario:** This issue was observed in a VoIP deployment when the Station Management (STM) process that handles AP management and user association crashed on the controller. This issue was observed in controllers running ArubaOS 6.1 and later versions.

Known Issues and Limitations

The following known issues and limitations are observed in ArubaOS 6.3.1.2. The applicable workarounds are also included.

AirWave Monitoring

Table 29: *Air Wave Monitoring Known Issues*

Bug ID	Description
94104	**Symptom:** A M3 controller module stops responding and reboots. Log files for the event indicate that the internal controller module, which manages firewall visibility triggers the error. **Scenario:** This issue is observed in a local M3 controller module running ArubaOS 6.3.1.1 in a master-local topology. **Workaround**: None.

AP-Platform

Table 30: *AP- Platform Known Issues*

Bug ID	Description
93344	**Symptom**: Clients are unable to connect to some APs. **Scenario**: This issue is observed in AP-220 Series connected to controllers running ArubaOS 6.3.1.1. **Workaround**: None

AP-Wireless

Table 31: *AP- Wireless Known Issues*

Bug ID	Description
93342	**Symptom:** There is no traffic from all clients on 802.11g capable access points. **Scenario**: This issue is observed in AP-220 Series connected to controllers running ArubaOS 6.3.1.1. **Workaround**: None.
93380 93494 93687 93744	**Symptom:** Occasionally, an AP stops responding and reboots. **Scenario:** This issue is observed because of Ethernet connectivity problem leading to loss of connectivity between the AP and controller. This issue occurs on AP-224 and AP-225 models and not limited to a specific ArubaOS version. **Workaround**: Ensure that the Ethernet connection issues does not lead to loss of connectivity between the AP and the controller.
93813	**Symptom:** The AP rebooted unexpectedly. **Scenario:** This issue occurs when an internal process fails. This issue is observed in AP-125 connected to controllers running ArubaOS 6.3.1.0. **Workaround:** None.
94117	**Symptom**: Clients are unable to connect to a SSID when the **Local Probe Request Threshold** setting in the SSID profile (which defines the SNR threshold below which incoming probe requests will get ignored) is set to a value of 25 dB. **Scenario:** This issue is triggered in ArubaOS 6.3.1.x, because the threshold value is set to 25 dB and the AP does not respond to probe requests with SNR higher than 35 dB. As a result, APs did not respond to authentication requests from the clients, preventing them from associating to the AP. **Workaround**: Disable the **Local Probe Request Threshold** parameter in the SSID profile, or use a less aggressive setting (such as 15-20 dB).
93996	**Symptom:** The AP-120 Series access point rebooted unexpectedly. **Scenario:** This issue occurs on AP-120 Series connected to controllers running ArubaOS 6.3.1.0. **Workaround:** None.
94164	**Symptom:** Wireless clients are unable to connect to an AP through the G band when the WPA2 authentication scheme is used. **Scenario:** This issue is observed in AP-225 connected to controllers running ArubaOS 6.3.1.1. **Workaround:** None.

Configuration

Table 32: *Configuration Known Issues*

Bug ID	Description
93922	**Symptom:** A custom banner with the **#** delimiter gets added as part of the **show running-config** command output. **Scenario:** The issue is observed when an administrator configures the banner using the **banner motd** command in the controller with the **#** delimiter. This issue is not limited to a specific controller model and is observed in ArubaOS 6.3.1.1. **Workaround:** None.

Controller-Datapath

Table 33: *Controller-Datapath Known Issues*

Bug ID	Description
87417 87846 87949 88039 88226 88445 89433 89539 89641 90024 90458 90469 90746 90896 91853 92284 92464 92466 92827 92828 92829 92830 92832 94007	**Symptom:** A master controller reboots unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. **Scenario:** This issue is observed in Aruba7240 controller running ArubaOS 6.3.1.1 in a master-local topology. **Workaround:** None.
93466	**Symptom:** The 7200 Series controllers reboots and the log files for the event displays the reason for the reboot as **Datapath Timeout**. **Scenario:** This issue is observed when port monitor is enabled or Small Form-factor Pluggable(SFP) is plugged or speed of the port is changed in the controller. This issue occurs in 7200 Series controllers and is not limited to a specific ArubaOS version. **Workaround:** None.
93582	**Symptom**: A 7210 controller crashes. The logs for this error listed the reason for the crash as **Datapath Timeout**. **Scenario**: This issue is observed in 7210 controllers running ArubaOS 6.3.1.0. **Workaround**: None.
94267	**Symptom**: After an upgrade to ArubaOS 6.3.1.x, clients are unexpectedly disconnected from the network, or are unable to pass traffic for 2-3 minutes after roaming between APs. **Scenario**: This issue is observed in Psion Omni handled scanners roaming between AP-175 and AP-120 series running ArubaOS 6.3.1.1. **Workaround**: None.

Controller-Platform

Table 34: *Controller-Platform Known Issues*

Bug ID	Description
92968	**Symptom:** Generating the **tech-support.log** file from the WebUI of the controller gets truncated at times. **Scenario:** This issue is not limited to a specific controller model and is observed in ArubaOS 6.2.1.3 and ArubaOS 6.3.1.0. **Workaround:** Using the CLI, execute the **tar logs tech-support** command to download the **tech-support.log** file.

RADIUS

Table 35: *RADIUS Known Issues*

Bug ID	Description
94081	**Symptom:** Multiple authentication failures are observed in the controllers. **Scenario:** This issue is observed when external LDAP server is used for authentication. This issue is not limited to a specific controller models and occurs in ArubaOS running 6.3.x versions. **Workaround:** Reduce LDAP timeout parameter value to 3 seconds for LDAP servers.

SNMP

Table 36: *SNMP Known Issues*

Bug ID	Description
94205	**Symptom:** The MIB "sysExtFanSTatus" cannot be queried. **Scenario**: This issue occurs on 7200 Series controllers running ArubaOS 6.3.1.1. This occurs because the hwMonprocess does not return the proper values for fanStatus SNMP queries. **Workaround:** None.

Station Management

Table 37: *Station Management Known Issues*

Bug ID	Description
91758	**Symptom**: Stationary Macbook laptops unexpectedly disassociates from APs, and are temporarily unable to pass traffic for 3-5 minutes during a period when many users on the network roam between APs. **Scenario**: This issue occurs in a network with a 3600 controllers running ArubaOS 6.3.1.1 with ARM channel assignment and scanning features enabled. **Workaround**: Disable ARM channel assignment and scanning features.

WebUI

Table 38: *WebUI Known Issues*

Bug ID	Description
93993	**Symptom:** The **Security** page under the **Dashboard** tab of the controller's WebUI does not display any statistics. **Scenario:** This issue occurs when there is a large number of entries in the WLAN Management System (WMS) database table. This issue is observed when a 3600 master controller is upgraded to ArubaOS 6.3.1.1 in a master-local topology. **Workaround:** None.

Issues Under Investigation

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

AP-Wireless

Table 39: *AP-Wireless Known Issues Under Investigation*

Bug ID	Description
93113	**Symptom:** Windows 7 clients using Intel 4965 NIC intermittently stops passing traffic when connected to AP-225. **Scenario:** This issue occurs on AP-225 running ArubaOS 6.3.1.1 version, and is under investigation. **Workaround:** None.

Controller-Datapath

Table 40: *Controller-Datapath Known Issues Under Investigation*

Bug ID	Description
94143	**Symptom:** A 3200XM controller rebooted unexpectedly. **Scenario:** An unexpected reboot caused by a internal process (datapath) timeout is observed on a 3200XM controller running ArubaOS 6.3.1.1. **Workaround:** None.
94200	**Symptom:** A local controller reboots unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. **Scenario:** This issue is observed in Aruba 7220 controller running ArubaOS 6.3.1.1 in a master-local topology. **Workaround:** None.

Controller-Platform

Table 41: *Controller-Platform Known Issues Under Investigation*

Bug ID	Description
93465	**Symptom:** A local controller reboots unexpectedly. The log files for the event listed the reason for the reboot as **Control Processor Kernel Panic**. **Scenario:** This issue occurs when the controller releases the memory of corrupted data packets. This issue is observed in 3000 Series and M3 controllers running ArubaOS 6.3.1.1 in a master-local topology. **Workaround:** None.

Features Introduced in ArubaOS 6.3.1.0

This chapter describes the features introduced in ArubaOS 6.3.1.0.

6.3.0.0 Feature Support

All features that were considered "beta quality" in ArubaOS 6.3.0.0 are now fully supported in ArubaOS 6.3.1.0.

Feature Support by Controller Platform

The table below lists the ArubaOS 6.3 features supported by hardware platform.

Table 42: *6.3 Feature Support by Platform*

Features	Controller			
	7200 Series	3600/M3	3400/3200XM	650/620
AirGroup	Yes	Yes	Yes	No
AppRF 1.0/Firewall Visibility	Yes	Yes	Yes	No
IF-MAP	Yes	Yes	Yes	No
AP Image Preload	Yes	Yes	No	No
Centralized Image Upgrade	Yes	Yes	Yes	No
IAP-VPN	Yes	Yes	Yes	No
RF Planning (Controller)	No	No	No	No
Access Points	All Access Points Supported			

AP Support

ArubaOS 6.3.x.x will be the last release to support the a/b/g only APs as well as the RAP-5 and AP-120 Series. ArubaOS 6.3 will be supported at least through October 31st 2018. Individual AP support dates will vary based on their end of sale date. Please see the Aruba end of support page http://www.arubanetworks.com/support-services/end-of-life-products/ for additional details.

Table 43: *AP Support*

AP Model	End of Sale Dates (Standard Variants)	Last ArubaOS Version Supported
AP-60, AP-61, AP-65, AP-65WB, AP-70 (All Variants)	31-May-2011	ArubaOS 6.3
AP-85 (All Variants)	30-Apr-2013	ArubaOS 6.3

Table 43: *AP Support*

AP Model	End of Sale Dates (Standard Variants)	Last ArubaOS Version Supported
AP-124, AP-125 (All Variants)	31-Jul-2013	ArubaOS 6.3
AP-120, AP-121 (All Variants)	31-Jan-2012	ArubaOS 6.3
RAP-2WG	31-Oct-2013	ArubaOS 6.3
RAP-5WN	31-Oct-2013	ArubaOS 6.3
RAP-5	31-Jan-2012	ArubaOS 6.3

Changes to Controller Communication with AirWave/ALE

This release of ArubaOS provides support for profile-based AMON message filtering for the configured management servers such as AirWave and Analytics Location Engine (ALE). Using this feature, you can filter the AMON messages sent to a configured destination server (AirWave or ALE) based on the message types enabled in the profile.

It is now mandatory to include the filtering profile while configuring the management server. The management server type **XC** in ArubaOS 6.3 is now updated to ALE. In addition, the ArubaOS 6.3.1 upgrade script automatically applies the pre-defined profile (default-amp and default-ale) for both AirWave and XC servers. For more information on configuring the management server and applying message filtering, see the *ArubaOS 6.3.x CLI Reference Guide*.

NOTE

If you delete a management server profile that is applied to a destination server, you must re-apply a different profile to the server or re-create the same profile for the message filtering process to continue.

Adaptive Radio Management

Dynamic Scanning Enhancements

The Adaptive Radio Management (ARM) feature is improved with an enhanced scanning technique to better identify the best channels for AP channel assignments. In previous releases, when ARM performed a 40 MHz or 80 MHz scan of a channel with a high level of noise or interference (such as that caused by a video bridge), ARM also reported a high noise floor for the entire 40 MHz or 80 MHz channel set. This could prevent ARM from assigning an AP to a secondary channel.

Starting with ArubaOS 6.3.1, if ARM reports a high noise floor on a channel within a 40 MHz channel pair or 80 MHz channel set, ARM performs an additional 20 MHz scan on each channel within that channel pair or set, to determine the actual noise floor of each affected channel. This allows ARM to avoid assigning the over utilized channel, while still allowing channel assignments to the other unaffected channels in that channel pair or set.

Enhanced Client Health Metric

An AP’s client health is the efficiency at which that AP transmits downstream traffic to a particular client. This value is determined by comparing the amount of time the AP spends transmitting data to a client to the amount of time that would be required under ideal conditions, that is, at the maximum Rx rate supported by client, with no data retries. Starting with ArubaOS 6.3.1, AP-220 Series access points support the client health metric introduced in ArubaOS 6.3.

A client health metric of 100% means the actual airtime the AP spends transmitting data is equal to the ideal amount of time required to send data to the client. A client health metric of 50% means the AP is taking twice as long as is ideal, or is sending one extra transmission to that client for every packet. A metric of 25% means the AP is taking four times longer than the ideal transmission time, or sending 3 extra transmissions to that client for every packet.

The client health metric appears on the **Dashboard > Performance** page of the controller WebUI, or in the output of the CLI command **show ap debug client-health**.

Cellular Handoff Assist

When both the client match and cellular handoff assist features are enabled, the cellular handoff assist feature can help a dual-mode, 3G/4G-capable Wi-Fi device such as an iPhone, iPad, or Android client at the edge of Wi-Fi network coverage switch from Wi-Fi to an alternate 3G/4G radio that provides better network access.

This feature is disabled by default, and is recommended only for Wi-Fi hotspot deployments. Enable this feature using the ARM profile in the WebUI, or through the following command in the command-line interface:

```
rf arm <profile> cellular-handoff-assist
```

AP Platform

Support for the AP-110 Series

Aruba AP-114 and AP-115 wireless access points support the IEEE 802.11n standard for high-performance WLAN. These dual radio access points use 3x3 MIMO (Multiple-in, Multiple-out) technology and other high-throughput mode techniques to deliver high-performance, 802.11n 2.4 GHz and 5 GHz functionality, while simultaneously supporting existing 802.11a/b/g wireless services.

NOTE

The Aruba AP-114 and AP-115 wireless access points are not available for sale at this time. Please check with your local sales contact.

Link Aggregation Support on AP-220 Series

AP-220 Series access points support link aggregation using either standard port-channel (configuration based) or Link Aggregation Control Protocol (protocol signaling based). AP-220 Series access points can optionally be deployed with LACP configuration to benefit from the higher (greater than 1 Gbps) aggregate throughput capabilities of the two radios.

To enable and configure LACP on AP-220 Series access points, configure the **LMS IP** parameter and the **GRE Striping IP** parameter in the **AP System profile**. The **GRE Striping IP** value must be an IPv4 address owned by the controller that has the specified **LMS IP**. The **GRE Striping IP** does not belong to any physical or virtual interface on the controller, but the controller can transmit or receive packets using this IP. For more information on Link Aggregation Support on AP-220 Series, see the *ArubaOS 6.3.x User Guide*.

NOTE

LACP configuration is not applicable to the other AP models.

AP-220 Series Functionality Improvements when Powered Over 802.3af (POE)

Internal AP power optimization allows for increased functionality in the AP-220 Series when powered over 802.3af power. Starting in ArubaOS 6.3.1, the AP-220 Series will have full 802.11ac functionality when powered over 802.3af power. On standard 802.3af power, the USB port and second Ethernet port will be disabled. The 2.4 GHz radio runs with a single stream. The 5 GHz 11ac radio runs with full functionality. All features of the AP-220 Series functions on 802.3at or POE+ power.

RAP Mode Support on AP-220 Series

This release of ArubaOS allows AP-220 Series access points to be deployed as remote APs (RAPs).

Netgear Cellular Modem Support

ArubaOS 6.3.1 introduces support for the Netgear 313U, 320U, and 330U 4G USB cellular modems on RAP-155.

Franklin Wireless U770 4G Modem Support

ArubaOS 6.3.1 introduces support of the Franklin Wireless U770 4G USB cellular modem for the Sprint LTE service on the RAP-3WN, RAP-5WN, RAP-108, and RAP-109.

AP-220 Series Legacy Feature Support

The following legacy features have been added to the AP-220 Series:

- **max-tx-fail:** The number of consecutive unacknowledged transmit frames from a client, that when reached, the AP internally clears up the client state under the assumption that the client is not reachable.
- **probe response threshold:** Indicates the signal strength of the incoming probe request packet, below which the AP will not respond and send probe responses.

AP-220 Series access points running ArubaOS 6.3.1.x have the following limitations:

- AP-220 Series access points cannot be configured as mesh nodes.
- AP-220 Series access points do not support:
  - ArubaOS 6.3.x.x-FIPs software images
  - The **Reduce Cell Size (Rx Sensitivity)** feature configurable in the 802.11a and 802.11g radio profiles.
  - 3G/4G USB Modems
  - Call admission control (CAC) and TSPEC handling features configurable in the VoIP Call Admission Control profile.

Dashboard Monitoring

AirGroup Enhancements

The **Dashboard** tab of the controller WebUI contains an **AirGroup** link that displays the information about AirGroup clients and servers. In previous releases that supported the AirGroup feature, this information was not available in the WebUI, and could only be displayed using the **show airgroupusers** and **show airgroup servers** commands in the command-line interface,

Lync interoperation with Microsoft Lync Server SDN API

ArubaOS 6.3.1.0 supports Microsoft® Lync SDN API 1.2. This Microsoft® plug-in works with Microsoft® Lync server to export details about voice or video calls, desktop sharing, and file transfer to the controller's web server. ArubaOS 6.3.1.0 also includes the following enhancements:

- Microsoft® Lync supports mobile devices running Windows, Android and iOS operating systems.
- The Lync SDN API 1.2 can communicate with the web server over HTTP and HTTPS protocols.
- The **web-server web-lync-listen-port** command now includes the **http** and **https** configuration parameters.

Regulatory Updates

The following table describes regulatory enhancements introduced in ArubaOS 6.3.1.

Table 44: *Regulatory Domain Updates*

Regulatory Domain	Change
FCC DFS Support	Added support for AP-224, AP-225, RAP-108, and RAP-109.

Table 44: *Regulatory Domain Updates*

Regulatory Domain	Change
United States, Japan, Canada, all European countries	Added support for AP-114 and AP-115 access points.
Chad, Mali	ArubaOS 6.3.1 introduces support for the Chad (TD) and Mali (ML) country domains. These domains follow the EU country domain settings.
Brazil, Mexico, South Africa, Algeria, Bosnia and Herzegovina, Dominican Republic, Ukraine, South Korea, Macedonia, Malaysia, Puerto Rico	Added support for the AP-104 access point.
Algeria, Colombia, Bolivia, Ecuador, El Salvador, Colombia, Guatemala, Nicaragua, Panama, Puerto Rico, Venezuela, Zambia	Added support for the AP-105 access point.
Algeria, Colombia, Russia	Added support for AP-92 and AP-93 access points.
Columbia, Dominican Republic, Mexico, Puerto Rico, Singapore	Added support for the AP-93H access point.
India	Added support for the 5 GHz band on AP-175P access point.
Russia, Indonesia, Bolivia, Bosnia, Columbia, Croatia, Dominican Republic, El Salvador, Guatemala, Macedonia, Panama, Puerto Rico, Ukraine, Bermuda, Venezuela, Trinidad and Tobago	Added support for the AP-175P access point.
Bermuda, Bosnia and Herzegovina, Colombia, Croatia, Dominican Republic, Macedonia, Russia	Added support for the AP-175DC access point.
Malaysia, Brazil, Venezuela, Bermuda, Bosnia and Herzegovina, Colombia, Croatia, Dominican Republic, Uganda, Macedonia, Russia	Added support for the AP-175AC access point.
Azerbaijan, Belarus, Bosnia and Herzegovina, Colombia, Croatia, Kazakhstan, Peru, Russia, Trinidad and Tobago	Added support for the AP-135 access point.
Argentina	Added support for the RAP-5WN access point.

Table 44: *Regulatory Domain Updates*

Regulatory Domain	Change
Macau	Added support for the following access points: - AP-92 - AP-93 - AP-104 - AP-105 - AP-134 - AP-135 - AP-68 (2.4 GHz only) - AP-175 - AP-175AC - AP-175DC - RAP-2WG (2.4 GHz only) - RAP-3WN (2.4 GHz only) - RAP-3WNP (2.4 GHz only) - RAP-5WN (5 GHz only)
Thailand	Added support for the following access points: - AP-92 - AP-93 - AP-93H - AP-104 - AP-105 - AP-134 - AP-135 - AP-175P - AP-175AC - AP-175DC - RAP-3WN - RAP-3WNP
South Korea, Saudi Arabia, UAE, India, Puerto Rico, Columbia, Dominican Republic, Macau, Pakistan, Qatar	Added support for RAP-108 and RAP-109 access points.
Canada	Channel 165 is no longer supported on AP-105 access points. DFS channels are enabled for the following access points: - AP-175P - AP-175AC - AP-175DC
Egypt	Removed support for DFS channels on the AP-125 access point.
Cyprus	Added support for DFS channels on the AP-125 access point.
Bolivia, Sri Lanka	Removed support for the AP-135 access point.

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the controller command-line interface and issue the command **show ap allowed-channels country-code <country-code> ap-type <ap-model>**.

The following example shows indoor, outdoor and DFS channels supported by an AP-105 in the **United States** domain.

```
(host) #show ap allowed-channels country-code us ap-type 105
Allowed Channels for AP Type 105 Country Code "US" Country "United States"
```

```
--------------------------------------------------------------------------
PHY Type                 Allowed Channels
--------                 ----------------
802.11g (indoor)         1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)         36 40 44 48 52 56 60 64 100 104 108 112 116 132 136 140 149 153 157 1
61 165
802.11g (outdoor)        1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)        52 56 60 64 100 104 108 112 116 132 136 140 149 153 157 161 165
802.11g 40MHz (indoor)   1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (indoor)   36-40 44-48 52-56 60-64 100-104 108-112 132-136 149-153 157-161
802.11g 40MHz (outdoor)  1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor)  52-56 60-64 100-104 108-112 132-136 149-153 157-161
802.11a (DFS)            52 56 60 64 100 104 108 112 116 132 136 140
```

Security

Support for RADIUS Framed-IP-Address for VPN Clients

IP addresses are usually assigned to VPN clients from configured local address pools. This feature provides another way to do this by using the Framed-IP-Address attribute that is returned from a RADIUS server to assign the address.

VPN clients use different mechanisms to establish VPN connections with the controller such as IKEv1, IKEv2, EAP or a user certificate. Regardless of how the RADIUS server is contacted for authentication, the Framed-IP-Address attribute is assigned the IP address as long as the RADIUS server returns the attribute. The Framed-IP-Address value always has a higher priority than the local address pool.

Advertisement of VPN Client Host Routes through OSPF

This feature allows VPN client addresses to be exported to OSPF, and to be advertised as host routes (/32). Exporting applies to any VPN client address regardless of how it is assigned.

Use this command to export the VPN client's assigned address to OSPF using IPC.ai

```
(host) (config) #aaa authentication vpn default
(host) (VPN Authentication Profile "default") #
(host) (VPN Authentication Profile "default") # export-route
```

Use the **show ip ospf database** command to show LSA types that are generated.

Off-Loading a Controller RAP Whitelist to CPPM

This feature allows a global whitelist to be maintained on ClearPass Policy Manager (CPPM) instead of on an individual controller. When a RAP or an IAP attempts to authenticate, the controller constructs a radius access request message for CPPM to validate. On a successful authentication, CPPM sends back a radius accept message along with the appropriate Vendor Specific Attributes (VSA).

For RAPs, the appropriate VSAs are **Aruba-AP-Group** and **Aruba-Location-Id**.

This feature allows whitelist entries to be maintained externally in CPPM for RAPs. The controller, if configured to use an external server, can send a RADIUS access request to a CPPM server. The RAP MAC address is used as a username and password to construct the access request packet and the CPPM validates the RADIUS message and returns the relevant parameters for the authorized RAPs.

If the RAP was initially an Instant AP (IAP), then the RADIUS access request is sent to the CPPM server with the IAP Ethernet address as the username. CPPM verifies if the corresponding entry exists in its local database. Depending on the configured policy, CPPM sends an access reject or accept with attributes that are applicable to the controller.

Serviceability

AP-220 Series Serviceability Enhancements

The following enhancements have been added to the AP-220 Series to improve AP troubleshooting, and used under the supervision Aruba Technical Support.

- **Packet Capture Raw Mode:** Raw packet capture mode is now supported on the AP-220 Series. To enable raw packet capture, use the ap packet-capture raw-start.
- **Crash Dump Improvements:** The number of associated clients at the time of the crash has been added to the AP kernel crash information. This enhancement is seen in the output of the command show ap debug crash-info.
- **Driver Log Improvements:** The log buffer and show command buffer length has been increased from 4k to 16k. This will prevent the logs from rolling over and causing a loss of information. This enhancement is seen in the output of the **show ap debug driver-log** command.

Spectrum Analysis

Enhanced Support for Spectrum Monitor and Hybrid AP Modes

AP-220 Series and AP-110 Series access points can now be configured as spectrum monitors (AP radios that gather spectrum data but do not service clients), or as hybrid APs (APs that serve clients as access points while analyzing spectrum analysis data for the channel the radio uses to serve clients).

Features Introduced in ArubaOS 6.3.0.0

This section lists the major features introduced in ArubaOS 6.3.0.0.

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 one (1).

NOTE

In ArubaOS 6.3, the MPDU Aggregation option under the HT SSID Profile does not affect the AP-220 Series. 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 45: *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

Table 45: *WLAN HT-SSID Profile Settings for VHT*

Parameter	Description
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 46: *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 47: *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 parameter was added to the regulatory domain profile:

Table 48: *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

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 acts 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 a 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 **licensingprofile** 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 disregards the built-in licenses used, and reports 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, and 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 a 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.

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*.

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.

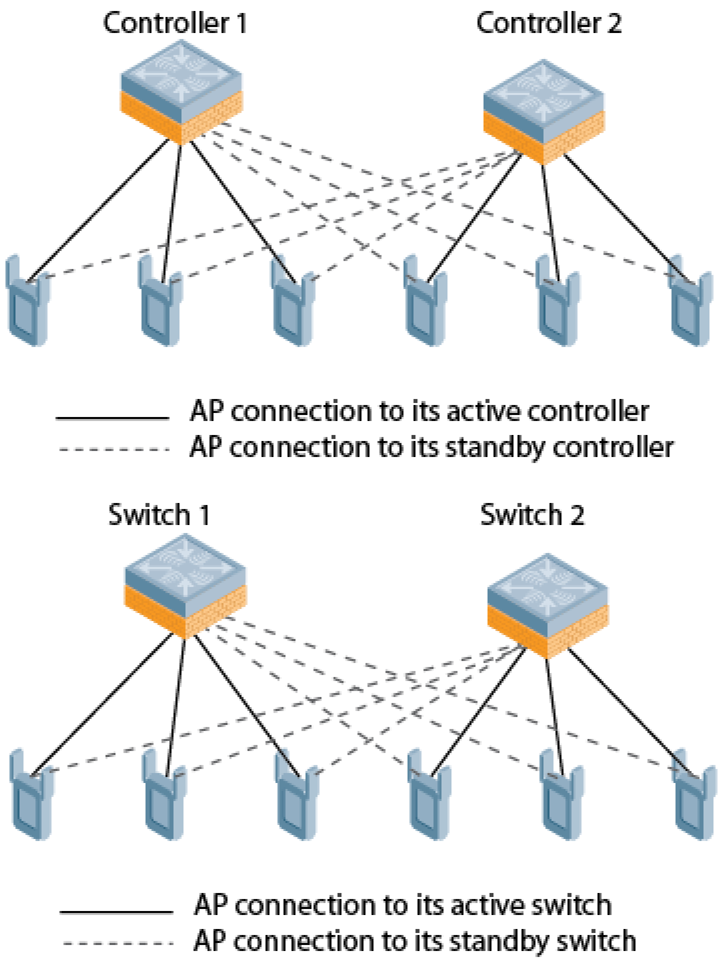
High Availability groups support the following deployment modes.

- Active/Active Deployment model on page 41
- 1:1 Active/Standby Deployment model on page 42
- N:1 Active/Standby Deployment model on page 43

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.

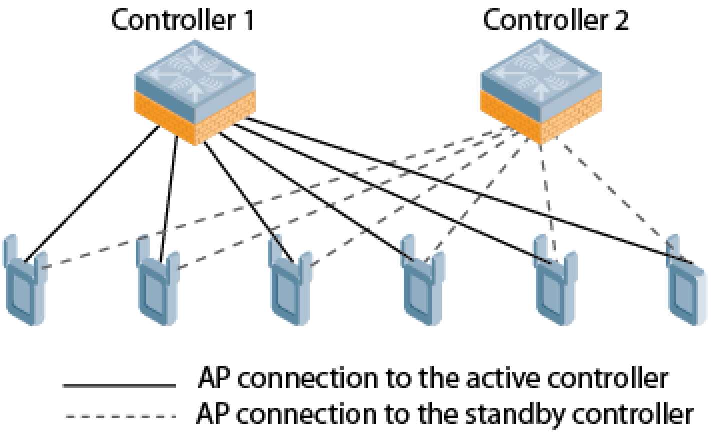
Figure 2 *Active-Active HA Deployment*

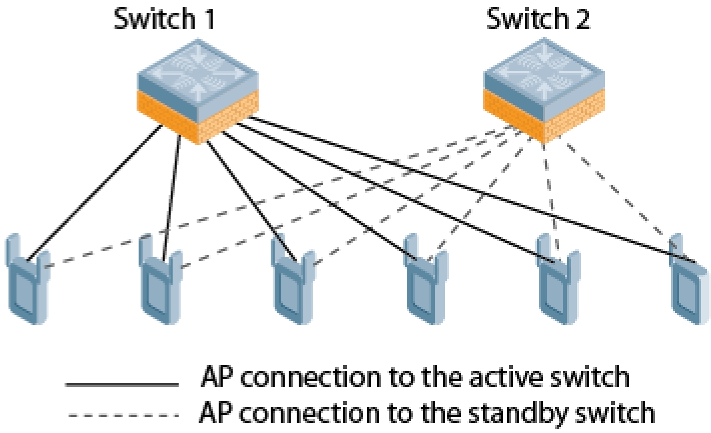

Controller 1
Controller 2
AP connection to its active controller
AP connection to its standby controller
Switch 1
Switch 2
AP connection to its active switch
AP connection to its standby switch

1:1 Active/Standby Deployment model

In this model, the active controller supports up to 100% of its rated AP capacity, 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

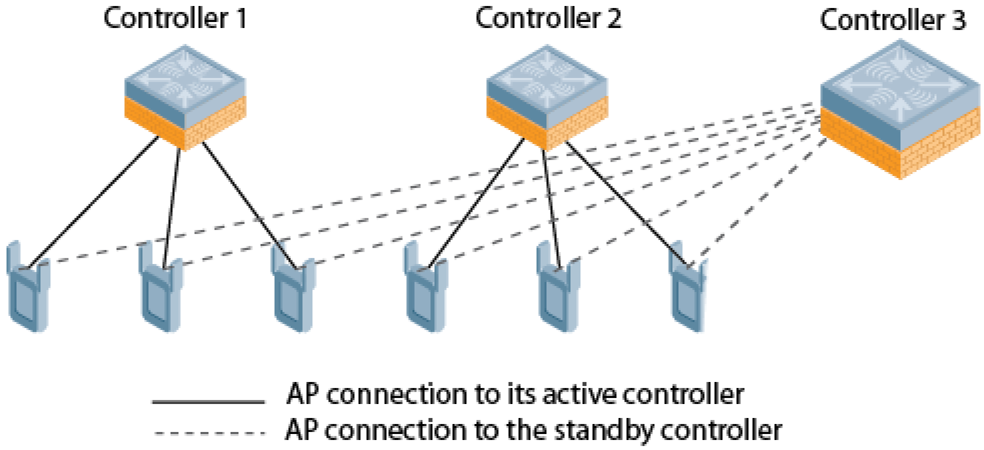
In this model, the active controller supports up to 100% of its rated AP capacity, while the other controller in standby mode is idle. If an active controller fails, all APs served by the active controller would failover to the standby controller.

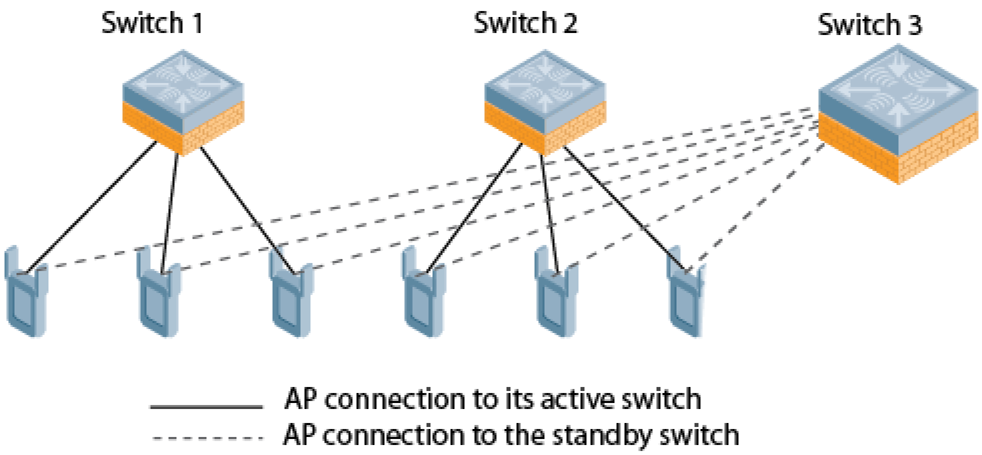
NOTE

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, the standby controller has enough AP capacity to support the total number of APs terminating on the active controllers. (Controller 1 and Controller 2)

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.

When the AP first connects to its active controller, the active controller provides the IP address of a standby controller, and the AP attempts to establish a tunnel to the standby controller. If an AP fails to connect to the first standby controller, the active controller selects a new standby controller for that AP, and the AP will attempts to connect to that 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** command in the command-line interface.

The following issues were resolved in ArubaOS 6.3.1.x release.

Resolved Issues in ArubaOS 6.3.1.1

The following issues were resolved in ArubaOS 6.3.1.1:

AP-Platform

Table 49: *AP-Platform Fixed Issues*

Bug ID	Description
89041	**Symptom:** 802.11n capable access points unexpectedly rebooted or failed to respond. This issue was resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario:** This issue was observed when a client disconnected from the network. The issue occurred on 802.11n access points running ArubaOS 6.3.0.1.
89042	**Symptom**: An access point crashed and rebooted frequently, and the log files for the event listed the reason for the crash as **kernel panic**. This issue was resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario:** This issue was observed in 802.11n access points running ArubaOS 6.3.0.1.
89043 89054 89045	**Symptom:** 802.11n capable access points unexpectedly rebooted or failed to respond. This issue was resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario:** This issue was observed on 802.11n-capable access points running ArubaOS 6.3.0.1.
89717	**Symptom:** The 802.11 APs had been malfunctioning. **Scenario:** This issue was observed on 802.11n APs and ArubaOS 6.3.1.2. This issue no longer occurs as the wireless driver has been upgraded.
89898	**Symptom:** The AP-120 Series APs malfunctioned due to low memory. **Scenario:** This issue was observed on AP-120 Series APs. This issue no longer occurs as the wireless driver has been upgraded.
90934 89137 90021 90495 90604 91016 91392 91393	**Symptom**: Access points unexpectedly stopped responding and rebooted. Log files for the event listed the reason for the crash as **kernel panic** or **kernel page fault**. This issue was resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario**: This issue was observed in 802.11n access points such as AP-125, AP-134, and AP-105 running ArubaOS 6.3.0.1.

AP-Wireless

Table 50: *AP-Wireless Fixed Issues*

Bug ID	Description
88631 88044 88569 88843 89044 89046 89053 89058 89325 89326 89811 89901 90890	**Symptom:** An access point continuously stopped responding and rebooted. This issue was resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario:** This issue was observed in AP-220 Series running ArubaOS 6.3.0.1 when the clients disconnected from the network.
88771 88772 91086	**Symptom:** 802.11n capable access points stopped responding and rebooted. The log files for the event listed the reason for the crash as **kernel page fault**. This issue was resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario**: This issue was observed only in 802.11n capable access points running ArubaOS 6.3.0.1.
91163 91315 91380 91468 91492 91516 91557	**Symptom:** An access point continuously rebooted. This issue was resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario:** This issue occurred when the clients disconnected from the network. This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.0.
91373	**Symptom**: MacBook clients were unable to pass traffic on the network. This issue was resolved by changes to ArubaOS that require APs to send data frames to all connected clients. **Scenario**: This issue was observed in AP-220 Series access points that were upgraded to ArubaOS 6.3.1.0, and was triggered by virtual APs being enabled or disabled, either manually (by network administrators) or automatically, as a part of the regular AP startup process.
91374	**Symptom:** Wireless clients observed high latency when associated to 802.11ac capable access points. Enhancements to the Broadcom driver of the access point fixed this issue. **Scenario:** This issue was observed in AP-225 running ArubaOS 6.3.0.1. This issue occurred when the wireless client went into power-save mode.

Controller-Platform

Table 51: *Controller-Platform Fixed Issues*

Bug ID	Description
90751 90633 90863 91154 91138 91474 91656	**Symptom:** Controllers continuously stopped responding and rebooted. Enhancements to memory allocation resolved this issue. **Scenario:** The issue occurred when an internal module (FPCLI) crashed due to memory corruption. This issue was observed in M3 controllers and is not limited to a specific ArubaOS version.

Resolved Issues in ArubaOS 6.3.1.0

The following issues were resolved in ArubaOS 6.3.1.0:

802.1X

Table 52: *802.1X Fixed Issues*

Bug ID	Description
86162	**Symptom**: Users experienced authentication failures with WPA2-PEAP. **Scenario**: This issue was triggered by some 2k server certificates. This issue was observed on 6000 Series controllers platforms with XLR/XLS processors, 3000 Series, and 600 Series controllers running ArubaOS 6.x.

AirGroup

Table 53: *AirGroup Fixed Issues*

Bug ID	Description
88239	**Symptom:** The command-line interface and the WebUI was not accessible on a controller when a large number of users supported multicast Domain Name System (mDNS) on the network and advertised different mDNS service IDs. This issue has not affected the client connectivity. This issue is fixed by upgrading to ArubaOS 6.3.1.0. **Scenario:** This issue occurred only when the **AirGroup Status** parameter was enabled in the **Configuration > Advanced Services > AirGroup > AirGroup Settings** tab of the WebUI with a large number (above 400) of AirGroup service IDs listed under **allowall** service. This issue was observed in controllers running ArubaOS 6.3.

Air Management - IDS

Table 54: *Air Management-IDS Fixed Issues*

Bug ID	Description
75039 77380	**Symptom**: AP-224 and AP-225 access points generated frequent false Intrusion Detection System (IDS) alarm **Beacon Frame With Incorrect Channel**. Changes to the internal code of AP-224 and AP-225 access points fixed the issue. **Scenario**: Due to the way AP-224 and AP-225 access points scan a channel, it received frames from an alternate channel in the 80 MHz channel set. This triggered a false IDS alarm. This issue was observed in AP-224 and AP-225 access points running ArubaOS 6.3.

AP–Datapath

Table 55: *AP–Datapath Fixed Issues*

Bug ID	Description
85279	**Symptom:** In a Master-local setup, all the users connected in bridge or split tunnel mode experienced a low throughput when no bandwidth contracts were configured. **Scenario:** This issue occurred on controllers running ArubaOS 6.2 or later due to incorrect mapping of the role to bandwidth contract when the ACL IDs in the master and local controllers were different for the same role. It was also observed during an authentication process restart.

AP–Platform

Table 56: *AP–Platform Fixed Issues*

Bug ID	Description
78289	**Symptom:** Crashes observed in the kernel in the node leave path, when the STA is disconnected. This issue is fixed by using appropriate reference counter protection. **Scenario:** This issue was triggered by aggressive STATION roams and power saves. This issue is not specific to any AP model and release version.
87359	**Symptom:** Users were unable to connect to the AP-225 every few hours. **Scenario:** Enabling the 802.11k feature caused this issue. The action frame was not freed up in the driver sent by the AP. This caused outstanding data frames in the driver to be dropped if the count exceeded a threshold. This issue was observed on the AP-225 and release version ArubaOS 6.3.

AP–Wireless

Table 57: *AP-Wireless Fixed Issues*

Bug ID	Description
88227 88286 88449 88509 88510 88561 88765 88767 88768 88770 88773 89133	**Symptom:** AP-125 stopped responding and rebooted due to lack of memory when the traffic was heavy. This issue is resolved by removing lldp support on AP-125, thereby reducing the memory consumed. **Scenario:** This issue was observed only on AP-125.
88282	**Symptom:** AP-225 running ArubaOS 6.3.0.1 stopped responding and rebooted. The log files for the event listed the reason for the crash as **kernel panic: Fatal exception**. Changes to the internal code fixed this issue. **Scenario:** This issue occurred in a master-local 7200 Series controller topology where the AP-225 terminated on both the controllers in a campus mode.
86063	**Symptom:** The Max Tx Fail feature was not supported on the AP-220 Series in ArubaOS 6.3. **Scenario:** When a user attempted to enable Max Tx Fail, the feature did not work on the AP-220 Series in ArubaOS 6.3. This feature has now been implemented.
87890	**Symptom:** The Service Set Identifier (SSID) was not hidden even after the **Hide-SSID** and the **deny-bcast** parameters were enabled. This issue is fixed by limiting the broadcast probe response if the **Hide-SSID** parameter is enabled. **Scenario:** This issue was observed in AP-225 associated with 7200 Series controllers.
88288	**Symptom:** An AP-134 crashed with a **Fatal exception in interrupt** error. **Scenario:** This issue was observed on 11n APs running ArubaOS 6.3 upon client disassociation.
88512	**Symptom**: An AP-225 access point transmitting A-MPDU aggregate traffic can perform excessive retries. **Scenario**: This issue occurred on an AP-225 in a network environment with a busy channel and a large number of intel clients. **Workaround**: None.

Bug ID	Description
80426 77834 81672 85186 85381 85396 85400 85658 85713 80426 85186 80426 86821	**Symptom:** An 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 APs (RAPs) or campus APs (CAPs) 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.

ARM

Table 58: *ARM–Datapath Fixed Issues*

Bug ID	Description
86084	**Symptom:** A wireless client remained associated to an AP-220 Series even though the signal strength was weak. **Scenario:** This issue occurred on AP-220 Series running ArubaOS 6.3. When the hand off assist feature was enabled on AP-220 Series, packets were not sent over the air to the client.

Authentication

Table 59: *Authentication–Datapath Fixed Issues*

Bug ID	Description
81035	**Symptom:** When roaming, the offered PMKID from the client is ignored and full authentication occurred.If no user credentials are stored on the machine (or saved), the PMKID is ignored. The username and password need to be provided at each roam. **Scenario:** This issue occured on no specific controller and was caused by a Wi-Fi client. In this case, the client was Ahteros-based NICs.This issue is not caused by an ArubaOS controller or AP. A client driver upgrade resolved the issue.

Base OS Security

Table 60: *Base OS Security Fixed Issues*

Bug ID	Description
83776	**Symptom:** Atheros based client devices were unable to connect to WPA-TKIP networks after 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 the Atheros clients did not support multiple relay counters.
84456	**Symptom:** Remote APs (RAPs) kept rebooting and did not come up on the controller. **Scenario:** This issue occurred as two RAPs using a static IP address tried to establish sessions using the same RAP credentials. This issue was not limited to any specific controller or RAP model.

Table 60: *Base OS Security Fixed Issues*

Bug ID	Description
84628 86814 87497 88406 88571	**Symptom:** An M3 controller module in a 6000 controller unexpectedly rebooted. Log files for the event listed the reason for the reboot as **Datapath timeout**. This issue is fixed by validating the bridge entries for VoIP clients. **Scenario:** This issue occurred when an invalid bridge value was computed and stored in an internal module (datapath). This issue was observed in an M3 controller module running ArubaOS 6.2.0.0.
85519	**Symptom:** One or more SSH (Secure Shell) sessions to a controller failed when multiple simultaneous SSH sessions occurred. The updates are made to sshd (SSH Daemon) process in ArubaOS 6.3.1.0 to avoid this issue . **Scenario:** This issue was observed in ArubaOS 6.1, 6.2, and 6.3.
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 changes to the code that maintain the state of radius exchange. **Scenario:** This issue was observed in ArubaOS 6.3.0.0 while performing VIA-VPN authentication with an RSA server using RSA SecureID.
86687	**Symptom:** The controller's SSH configuration has been modified to reduce a potential vulnerability to DOS attacks. **Scenario:** This issue was identified on controllers running ArubaOS 6.3.0.0.
86867	**Symptom:** When a user-role and the ACL configured as the ip access-group on the interface for APs/RAPs have the same name, the AP/RAP traffic is hitting the user-role ACL instead of the ip access-group ACL. **Scenario:** This issue was observed on a controller running ArubaOS 6.2.1.2. **Workaround:** Do not create an ACL for the IP access-group that has a name matching that of any user-role in the configuration.
88165	**Symptom** Clients using a wired connection are assigned an incorrect user role **Scenario**: This bug is applicable for wired clients, and is not specific to a controller type of software version. This issue occurs when information about an AP wired connection gets overwritten by similar information from another AP, resulting in a loss of wired information on the first AP, and preventing users associated with that AP from falling into their user role.
88386	**Symptom:** User roles disappeared randomly after a controller reloaded. Internal code changes fixed this issue. **Scenario:** The issue occurred when many user roles were added, or roles with heavy configurations exceeded the buffer space on the controller. This issue was not specific to any ArubaOS version or controller model.

Controller - Datapath

Table 61: *Controller Datapath Fixed Issues*

Bug ID	Description
84071	**Symptom:** A controller stopped responding and unexpectedly rebooted. The log files for the event listed the reason for the reboot as **Datapath exception**. This issue occurred on 7200 Series controller running ArubaOS 6.2.1.0. **Scenario:** This issue occurred when an SSL encapsulated invalid ESP frame was received and processed by the controller.

High Availability

Table 62: *High Availability Fixed Issues*

Bug ID	Description
86798	**Symptom:** When APs were connected to controllers using the high availability: fast failover feature in a master\master topology, AirWave could not see information about rogue APs from the active master controller. Improvements to the way master IP information for each controller is saved resolves this issue. **Scenario:** When the high availability fast failover feature was enabled between two master controllers acting as HA-Active and HA-Standby controllers, the active controller's master IP address stored in the AP was overwritten by the master IP address from the standby controller. This caused WLAN Management System (WMS) information to be sent to the standby controller instead of the active controller.

Local Database

Table 63: *Local Database Fixed Issues*

Bug ID	Description
84494	**Symptom:** A controller unexpectedly rebooted, with the log files for the event listing 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, and was resolved by internal code changes.
88019	**Symptom:** A warning message **WARNING: This controller has RAP whitelist data stored in pre-6.3 format, which is consuming ………………..running the command 'local-userdb-ap del all** appeared, when a user logged into a controller. This issue is fixed by deleting the warning file, when all the old entries are deleted. **Scenario:** This issue occurred when a controller was upgraded from a previous version of ArubaOS to 6.3 or later. This issue was not specific to any controller model or release version.

Multicast

Table 64: *Multicast Fixed Issues*

Bug ID	Description
88138	**Symptom:** One of the proxy group entries aged out after issuing the **show ip igmp proxy-group** command. This crashed the multicast module in the controller. Changes to the internal code of the multicast module fixed the issue. **Scenario:** This issue was not limited to a specific controller model and was observed in ArubaOS 6.3.0.1.

Platform

Table 65: *Platform Fixed Issues*

Bug ID	Description
76447	**Symptom:** An M3 controller stopped responding and rebooted. The controller listed the reason for the crash as a controller processor kernel panic. This issue was resolved by internal improvements to hardware register access. **Scenario:** This issue was observed in local M3 controllers running ArubaOS 6.1.3.5.

Bug ID	Description
81555	**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 a 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. This issue was not specific to any controller model.

RADIUS

Table 66: *RADIUS Fixed Issues*

Bug ID	Description
85848	**Symptom:** The **Calling_Station_Id** was sent an IP address instead of MAC address even though the option "Use IP address for calling station ID" was not selected in the AAA server. This issue is fixed in 6.3.1.0, by adding a new check box for the MAC address. **Scenario:** This issue was observed when the user executed the **aaa authentication-server radius x** command, and was not specific to any controller model.
87814	**Symptom:** On client disconnection, the RADIUS accounting STOP record packet counter reset to zero. Changes to the internal code fixed the issue. **Scenario:** This issue occurred when an AP was provisioned in decrypt-tunnel mode with RADIUS accounting enabled. This issue was not limited to a specific controller model and was observed in ArubaOS 6.3.0.0 or later.

Remote AP

Table 67: *Remote AP Fixed Issues*

Bug ID	Description
85473	**Symptom:** A RAP-3WN AP using a USB modem was unable to come up until it rebooted. Changes to how the RAP-3WN determines the modem product ID has resolved this issue. **Scenario:** This issue occurred on a RAP-3WN AP running ArubaOS 6.2.1.2 connected to a Huawei E156 modem.
86082	**Symptom:** An AP-225 failed to respond. Enhancements in the internal code fixed this issue. **Scenario:** This issue was observed on when Point-to-point protocol over Ethernet (PPPoE) was enabled on AP-220 Series access points.
86934	**Symptom:** The AP failed during boot up when the Huawei modem E1371 was used. An internal code error when using this modem caused the issue. **Scenario:** This issue was observed on a RAP-108 and RAP-109 running ArubaOS 6.3.
87105	**Symptom:** Printers connected to the wired port of a remote AP (RAP) in tunnel mode intermittently fall into the wrong VLAN. This issue is resolved by improvements that ensure that the remote AP configuration state is properly cleared when its connection is reset. **Scenario:** This issue occurred on a RAP-5 remote AP running ArubaOS 6.2.1.2, when configuration settings were not properly cleared on a remote AP that reset its connection to the controller. As a result, the RAP's ethernet interface was brought up in bridge mode first, then changed to tunnel mode. This caused a configuration conflict between the controller and the RAP, as the controller managed the RAP as a remote bridge user, and the RAP operated as a user in tunnel mode.

Startup Wizard

Table 68: *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 high-throughput or very-high-throughput settings in the 802.11a or 802.11g radio profiles before enabling 40MHz and 80MHz, and disabling 80MHz and 40MHz, before disabling the throughput setting. **Scenario:** This error occurred when a WLAN is configured with a, a+n, b/g, or b/g+n radio types.

UI Monitoring

Table 69: *UI Monitoring Fixed Issues*

Bug ID	Description
80233	**Symptom:** The **Monitoring > Access Points and Monitoring > Network > All Access Points** page of the controller WebUI showed APs as down, even if they are showed as up in the command-line interface. This issue is fixed by improvements to the local management switch (LMS) IP on the master controller and now the status of APs is displayed accurately on the WebUI. **Scenario:** This issue was observed on a 6000 master controller with two local controllers running ArubaOS 6.2.0.2 in a master/local topology.
83820	**Symptom:** Dashboard page was not getting loaded in the WebUI. This issue was fixed by disabling the compatibility mode on the IE. **Scenario:** The issue occurred when the user tried to access the WebUI in IE8 in compatibility mode (This mode is used to support websites that were developed for older versions of IE browser). The issue was not specific to a controller model or a software version.
84151 85229 85569 86554	**Symptom:** The **Security Summary** page in the WebUI timed out if the event table in the WMS database became very large. This issue was resolved by enabling a periodic clean-up of the WMS event table entries. **Scenario:** This issue was observed when too many APs where terminating on a controller. This issue was not limited to any specific controller model.

Voice

Table 70: *Voice Fixed Issues*

Bug ID	Description
83403 86180 86369	**Symptom:** The clients were disconnected from the network due to an internal module crash. This issue was resolved by not prioritizing the subsequent RTP sessions for the SCCP calls for the clients. **Scenario:** This issue was observed while handling SCCP state transition, hence an internal module (STM) crashed. This issue occurred on controllers running ArubaOS 6.1 and 6.2 versions, and was not limited to a specific controller model.
86224	**Symptom:** Calls dropped after 30 seconds when performing a blindly transferred SIP call. **Scenario:** This issue was observed on the M3 controller module running ArubaOS version 6.2.1. It occurred when Ascom phones sent a DELTS request upon receiving either an "invite" message from the SIP server or after sending a "180 Ringing" message back to the server.

WMM

Table 71: *WMM Fixed Issues*

Bug ID	Description
68503	**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 earlier in tunnel and decrypt-tunnel forwarding modes.

Known Issues and Limitations

The following are the known issues and limitations observed in ArubaOS 6.3.1.x.

Advanced Monitoring

Table 72: *Advanced Monitoring Known Issues*

Bug ID	Description
88392	**Symptom:** The **Reference count** column in the output of the **show mgmt-server profile <profile-name>** command displays an incorrect reference count value due to an architectural limitation. **Scenario:** This issue is not limited to any specific controller model. **Workaround:** None.
88752 87809	**Symptom:** A crash is observed in the firewall visibility due to DNS cache corruption. **Scenario:** The trigger of this issue is not known and this issue is not limited to any specific controller model or release version. **Workaround:** None.

Air Management

Table 73: *Air Management Known Issues*

Bug ID	Description
86804	**Symptom:** The master controller reboots periodically and displays the message "Nanny rebooted machine - low on free memory." **Scenario:** This issue is observed on the 3200XM controllers running ArubaOS version 6.3. It occurs when the 3200XM controller is near its memory limit and the customer upgrades to a newer version of ArubaOS software that requires more memory than the 3200XM controller is capable of handling. **Workaround:** Tune or disable some features in order to use less memory.

Air Management-IDS

Table 74: *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-Platform

Table 75: *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.
87138	**Symptom:** The **show running-config** command output does not display the default rf ht-radio profiles (default-a and default-g). **Scenario:** This issue is observed on 3000 Series controllers running ArubaOS 6.3 in an all master deployment. **Workaround:** Make any minor configuration change to the default rf ht-radio profiles (default-a and default-g) and revert it.

AP-Wireless

Table 76: *AP-Wireless Known Issues*

Bug ID	Description
84884	**Symptom:** Fragmented EAP frames are not sent with the same data rate as a non-fragmented EAP frames. **Scenario:** This issue occurs on 802.11ac access points running ArubaOS 6.3.0.0 or later. **Workaround:** None.
87231	**Symptom:** A high CPU utilization is noticed on AP-105 after upgrading to 6.3. However, the client performance is not impacted. **Scenario:** This issue is observed on AP-105 running ArubaOS 6.3 deployed in a high Wi-Fi or non-Wi-Fi interference environment. **Workaround:** None

88124	**Symptom**: 802.11ac MacOS clients are unable to pass traffic to APs in tunnel forwarding mode.
	Scenario: This issue may be triggered by issues in the client Broadcom drivers, when there are three MPDUs in an AMSDU packet.
	Workaround: Change the **Maximum number of MSDUs in an A-MSDU** parameters in the high-throughput SSID profile to a value of 2.
	`wlan ht-ssid-profile <profile>`
	`max-tx-a-msdu-count-be 2`
	`max-tx-a-msdu-count-bk 2`
	`max-tx-a-msdu-count-vi 2`

88512	**Symptom**: An AP-225 access point transmitting A-MPDU aggregate traffic can perform excessive retries. **Scenario**: This issue occurs on an AP-225 in a network environment with a busy channel and a large number of Intel clients. **Workaround**: None.
88631	**Symptom:** AP-125 access points unexpectedly reboot. Log files for the event indicate that the APs reboot because they are out of memory. **Scenario:** This issue is observed on AP-125 access points associated with a controller running ArubaOS 6.3.0.1. **Workaround:** None.

Base OS Security

Table 77: *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.
86867	**Symptom:** When a user-role and the ACL configured as the ip access-group on the interface for APs/RAPs have the same name, the AP/RAP traffic is hitting the user-role ACL instead of the ip access-group ACL. **Scenario:** This issue was observed on a controller running ArubaOS 6.2.1.2. **Workaround:** Do not create an ACL for the IP access-group that has a name matching that of any user-role in the configuration.
88271	**Symptom:** It is not possible to configure a deny any any protocol ACL that overrides a statically configured permit any any protocol ACL. **Scenario:** This issue is observed on a controller running ArubaOS 6.3.0.1. This action is expected behavior and is prevented by ArubaOS so the user cannot disrupt controller functions. **Workaround:** None. However, it is possible to configure user defined ACLs on the subnet to override static ACLs.

Captive Portal

Table 78: *Captive Portal Known Issues*

Bug ID	Description
87294	**Symptom:** Captive Portal (CP) whitelist mapped to the user-role does not get synchronized with the standby controller. **Scenario:** The administrator creates a net-destination and adds it to the CP profile whitelist mapped to the user-role in the master controller. This configuration does not get synchronized with the standby controller. This issue is observed in ArubaOS 6.2.1.2 and is not limited to a specific controller model. **Workaround:** None
88405	**Symptom**: After successfully authenticating a client using Captive Portal, the browser does not automatically redirect the client to the original URL. **Scenario**: This issue is observed in the 7200 Series controller running ArubaOS 6.3.0.0. **Workaround**: Set the **welcome-page** parameter to the desired URL under **aaa authentication captive-portal** profile.

Controller-Datapath

Table 79: *Controller-Datapath Known Issues*

Bug ID	Description
74428 88758	**Symptom:** On the RJ45 ports 0/0/0 and 0/0/1, if the port speed is forced from 1 Gbps to 10/100 Mbps when traffic is flowing, traffic forwarding on the port can stop in an unintended manner. **Scenario:** This issue has been observed on 7200 Series controllers 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.
82824	**Symptom**: In some cases, when the number of users is high (more than 16k), 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.
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 the new character limit per line. You can have more than 1 line of 255 characters. Run the **write-mem** command afterward to fix this issue.

Controller-Platform

Table 80: *Controller-Platform Known Issues*

Bug ID	Description
82736 84022 86005 86572 86589 87410 87587 85628 82875 88434 88921 88332 88351 89818	**Symptom:** A controller rebooted unexpectedly. **Scenario:** This reboot is caused by a soft watchdog reset. This was observed on ArubaOS 6.1.3.x, 6.2.1.x, and 6.3.x, and is not limited to specific controller model. **Workaround:** None.
82402 84212 86636 87552 89437 90466 91280	**Symptom:** A controller unexpectedly stops responding and reboots. The log files for the event lists the reason for the crash as **httpd_wrap process died**. **Scenario**: This issue occurs in 3400 series controllers running ArubaOS 6.2.1.0 and later, and triggered by limits to the size of the data packets used by the internal controller library that manages communication between controller processes. **Workaround**: None.
88321	**Symptom:** A local controller crashes and reboots, and log files for the event lists the reason for the crash as **watchdog timeout**. **Scenario:** The trigger of this issue is not known. This issue occurs in M3 controllers running ArubaOS 6.3.0.1 in a master-local topology. **Workaround:** None.

ESI

Table 81: *ESI Known Issues*

Bug ID	Description
88042	**Symptom:** The http traffic from a user is not redirected to the ESI server, even when the ESI server is reachable and the http traffic redirection for the corresponding user role is enabled. **Scenario:** The trigger of this issue is not known. This issue is observed on 7240-US controllers running ArubaOS 6.3 in a master-local topology. **Workaround:** None

High Availability

Table 82: *High Availability Known Issues*

Bug ID	Description
80206	**Symptom:** The high availability:fast failover feature introduced in ArubaOS 6.3 does not support a deployment model where a VRRP-based redundant master pair (a master controller and standby-master controller) is also configured as high availability active-standby pair. **Scenario:** This topology is not supported because the high availability: fast failover feature does not allow the APs to form standby tunnels to the standby master. **Workaround:** None

IPSec

Table 83: *IPSec Known Issues*

Bug ID	Description
80460	**Symptom:** Remote client and Site-to-Site VPN performance is low and does not scale to the controller's limit when IKEv2 with GCM256-EC384 encryption algorithm is configured. **Scenario:** This issue impacts the 651, 3600, and 7200 Series controllers, and occurs when the IKE session is established to a standby unit in a failover deployment. **Workaround:** None.

Licensing

Table 84: *Licensing Known Issues*

Bug ID	Description
87424	**Symptom:** The licenses are lost on a standby master causing the configuration on the local controller to be lost. **Scenario:** This issue occurs when the standby comes up before the master after a reboot. This may also occur in an all master scenario when running ArubaOS 6.3. **Workaround:** None.

Master-Local

Table 85: *Master-Local Known Issues*

Bug ID	Description
88430	**Symptom:** User-role configuration is lost after upgrading master, standby, and local controllers to ArubaOS 6.3.1. **Scenario:** This issue is observed on a 7200 Series controller running ArubaOS 6.3.1. **Workaround:** Disabling the configuration snapshot by executing the **cfgm set sync-type complete** command on master and standby controllers prevents partial configuration loss. Wait at least five (5) minutes after the upgraded master and standby have rebooted before reloading the upgraded local controller.

Master-Redundancy

Table 86: *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.
80041 87946 87032 88067	**Symptom:** The `show database synchronize` command from the CLI displays the **FAILED** message. The standby controller database is out-of-sync with the master controller, and any switchover during the out-of-sync state causes the controller to be in an inconsistent state. **Scenario:** This issue occurs in controllers running ArubaOS 6.3.0.0, in a master-standby configuration. **Workaround:** None

Remote AP

Table 87: *Remote AP Known Issues*

Bug ID	Description
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 occurs 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.
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.
89861	**Symptom**: If a RAP-108/ RAP-109 with a USB modem is powered with a Power over Ethernet (PoE) injector, the remote AP might not have sufficient power to activate the USB port, preventing the AP from detecting the USB modem. **Scenario**: This issue is identified on RAP-108/ RAP-109 remote APs powered only by PoE, without an external power source. **Workaround**: Connect a RAP-108/ RAP-109 remote AP with a USB modem to an external power source.

Table 87: *Remote AP Known Issues*

Bug ID	Description
88497	**Symptom:** A RAP-5WN AP using a Sierra Wireless AirCard 313U modem can stop responding when an associated client sends traffic. **Scenario:** This issue only occurs in a 3G network when the AP's cellular network preference setting is configured to use **auto** mode. **Workaround:** Configure the cellular network preference settings in the RAP-5WN AP to use **4G-only** mode to connect to the network.

Station Management

Table 88: *Station Management Known Issues*

Bug ID	Description
82012	**Symptom**: An internal controller process stops responding and restarts, preventing the controller from servicing clients. **Scenario**: This issue is identified when the controller upgrades its image, and is triggered when the controller expects IKEv2 information that is missing from the mysql global AP database. **Workaround**: None.
86620	**Symptom**: The **show ap association client-mac** command shows client MAC addresses for clients that aged out beyond the idle timeout value. **Scenario**: This issue is not limited to a specific controller or ArubaOS release version. **Workaround**: Issue **aaa user fast-age** command to age out the inactive clients.

Voice

Table 89: *Voice Known Issues*

Bug ID	Description
89258	**Symptom:** Lync SDN API-based ALG does not work when clients are behind NAT. **Scenario:** When the user VLANs to which Lync clients are connected have IP NAT inside, or the Lync users are behind a NAT, the Lync SDN API based Lync ALG is not be able to prioritize the Lync traffic. Apart from this, it does not provide the visibility information to these calls through either CLI or dashboard. This issue is observed on a controller running ArubaOS 6.3.1. **Workaround:** None.

WebUI

Table 90: *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 displays 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, the Spectrum UI displays 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.

Table 90: *WebUI Known Issues*

Bug ID	Description
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.
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.
89225	**Symptom:** Configuration of a mgmt-server (ALE or AirWave) using the WebUI is not supported. **Workaround:** Use the CLI to configure mgmt-servers.

Issues Under Investigation

The following issues have been reported in ArubaOS, but have not been confirmed. We are unable to reproduce these issues and the root cause has not been identified. 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 91: *AP-Wireless Observed Issues*

Bug ID	Description
82813	**Symptom:** An old generation Sony PlayStation® 3 randomly stops passing traffic after upgrading from ArubaOS 6.1.4.1 to 6.2.0.3. **Scenario:** The issue occurs when a user tries to stream videos, download movies, and log into a Netflix account. This issue is observed after upgrading the controller from 6.1.4.1 to 6.2.0.3.

AP-Platform

Table 92: *AP-Platform Observed Issues*

Bug ID	Description
88009 88319 85662	**Symptom:** Although the APs are shown as down in the master controller, they are functional in the local controller and are associated to clients.

Controller-Platform

Table 93: *Controller-Platform Observed Issues*

Bug ID	Description
88107	**Symptom**: A 3600 controller running ArubaOS 6.2.1.2 stops responding and reboots. The log files for the event lists the reason for the crash as **User pushed reset**.
87952 88241 88240 88242 88243	**Symptom:** An unexpected reboot of an M3 controller due to an internal process (WMS) error is observed.

Chapter 6
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

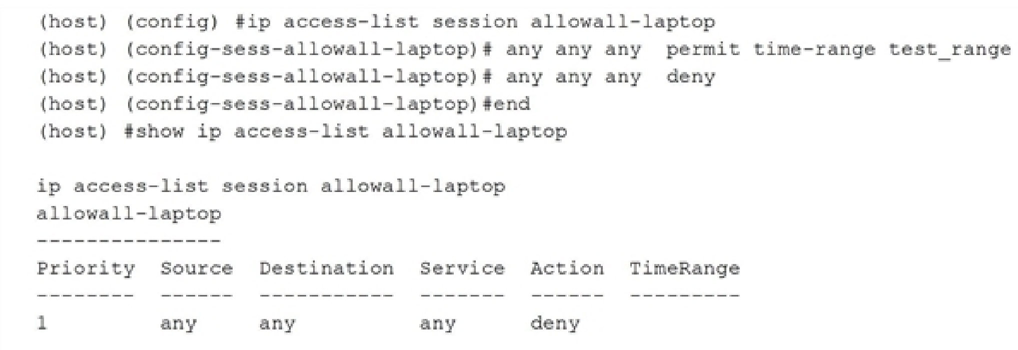
Before upgrading to any version of ArubaOS 6.3, take note of these known upgrade caveats.

- ArubaOS 6.3.1.2 is not recommended for customers with AP-120 Series access points that routinely see over 85 clients associated to an AP. Please contact support if you have any questions.
- Beginning in ArubaOS 6.3.1, the local file upgrade option in the 600 Series controller WebUI has been disabled.
- The ArubaOS WebUI does not support the following special characters for AP Name and AP Group in ArubaOS 6.3.1:
  - AP Name: % = + \ | ' " &
  - AP Group: * ( ) + [? \ = | ' " &
- The local file upgrade option in the 7200 Series controller WebUI does not work when upgrading from ArubaOS 6.2 or later. 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.
- Aruba 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 considers 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 versions and your configuration contains an ACL with redundant firewall rules, upon upgrading, only the last rule remains.

  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
```

- ArubaOS 6.3.1.2 is supported only on the newer MIPS controllers (7200 Series, M3, 3200XM, 3400, 3600, and 600 Series). Legacy PPC 2000, 800, 2400, SC1/SC2, and 3200 controllers are not supported. DO NOT upgrade to 6.3.x if your deployments contain a mix of MIPS and PPC in a master-local setup.
- 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 68.)

Installing the FIPS Version of ArubaOS 6.3.1.0

Download the FIPS version of software from https://support.arubanetworks.com.

Before Installing FIPS Software

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 cannot 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.
- In the Common Criteria evaluated configuration, software loading through SCP (secure copy) is the only supported option. Loading software through TFTP, FTP, or the WebUI 'Local File' option are not valid options.
- 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 6.3.1.0, 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 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 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 **tar clean crash** command 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 **tar clean flash** command 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 **tar clean logs** command 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 6.3.1.0:

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 6.3.1.2.

- For ArubaOS 3.x.versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.
- For ArubaOS RN-3.x or 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 (If you are running ArubaOS 5.0.3.1 or the latest 5.0.x.x, review Upgrading With RAP-5 and RAP-5WN APs on page 69 before proceeding further.)
- 3.4.4.1 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 6.3.1.0 from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.

3. Validate the SHA hash for a software image:
    a. Download the file **Aruba.sha256** from the download directory.
    b. To verify the image, load the image onto a Linux system and execute the **sha256sum <filename>** command or use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
    c. Verify if the output produced by this command matches the hash value found on the support site.

NOTE

The ArubaOS image file is digitally signed, and is verified using RSA2048 certificates pre-loaded onto the controller at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the controller does not load a corrupted image.

4. Log in to the ArubaOS WebUI from the PC or workstation.
5. 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.
6. Select the downloaded image file.
7. In the **partition to upgrade** field, select the non-boot partition.
8. In the **Reboot Controller After Upgrade** option field, the best practice 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 does not take effect until you reboot the controller.
9. In Save **Current Configuration Before Reboot** field, select **Yes**.
10. Click **Upgrade**.
11. 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).
12. 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. Login to 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 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.

Upgrading With RAP-5 and RAP-5WN APs

If you have completed the first upgrade, hop to the latest version of ArubaOS 5.0.4.x, and your WLAN includes RAP-5/RAP-5WN APs. Do not proceed until you complete the following process. Once complete, proceed to step 5 on page 69. Note that this procedure can only be completed using the controller's command line interface.

1. Check the provisioning image version on your RAP-5/RAP-5WN Access Points by executing the **show ap image version** command.
2. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses.
3. For each of the RAP-5/RAP-5WN APs noted in the step 2, upgrade the provisioning image on the backup flash partition by executing the following command:

    ```
    apflash ap-name <Name_of_RAP> backup-partition
    ```

    The RAP-5/RAP-5WN reboots to complete the provisioning image upgrade.

4. When all the RAP-5/RAP-5WN APs with a 3.3.2.x-based RN provisioning image have successfully upgraded, verify the provisioning image by executing the following command:

   ```
   show ap image version
   ```

   The flash (Provisioning/Backup) image version string should now show a version that does not contain the letters “rn”, for example, 5.0.4.8.

If you omit the above process or fail to complete the flash (Provisioning/Backup) image upgrade to 5.0.4.x and the RAP-5/RAP-5WN was reset to factory defaults, the RAP cannot connect to a controller running ArubaOS 6.3.1 and upgrade its production software image.

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 6.3.1.0.

- For ArubaOS 3.x.versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.
- For ArubaOS RN-3.x or 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. (If you are running ArubaOS 5.0.3.1 or the latest 5.0.x.x, review Upgrading With RAP-5 and RAP-5WN APs on page 69 before proceeding further.)
- 3.4.4.1 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 6.3.1.0 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)**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
----------------------------------
Partition                : 0:1 (/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
```

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                : 0:0 (/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

   ----------------------------------
   Partition                : 0:1 (/dev/ha1)**Default boot**
   Software Version         : ArubaOS 6.3.1.0 (Digitally Signed - Production Build)
   Build number             : 40232
   Label                    : 40232
   Built on                 : Fri Oct 07 00:03:14 2013
   ```

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. Login to the command-line interface to verify all your controllers are up after the reboot.
2. Issue the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Issue the **show ap database** command 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 6.3.1.2 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 6.3.1.0 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 6.3.1.0 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 6.3.1.0, the changes do not appear in RF Plan in the downgraded ArubaOS version.
   - If you installed any certificates while running ArubaOS 6.3.1.0, 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 6.3.1.0 image:

```
#show image version
----------------------------------
Partition               : 0:0 (/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
----------------------------------
Partition               : 0:1 (/dev/hda2)**Default boot**
Software Version        : ArubaOS 6.3.1.0(Digitally Signed - Production Build)
Build number            : 40232
Label                   : 40232
Built on                : Fri Oct 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.