ArubaOS 6.1.3.2

Release Notes

Open Source Code

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

http://www.arubanetworks.com/open_source

Legal Notice

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

Warranty

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

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

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

The ArubaOS 6.1.3.2 release is an important upgrade that introduces significant performance and stability fixes and enhancements for networks running ArubaOS versions 3.4.5.x and above. In addition, this release also provides fixes and enhancements for networks running legacy Aruba controllers. Some of the key areas of enhancements in this release are:

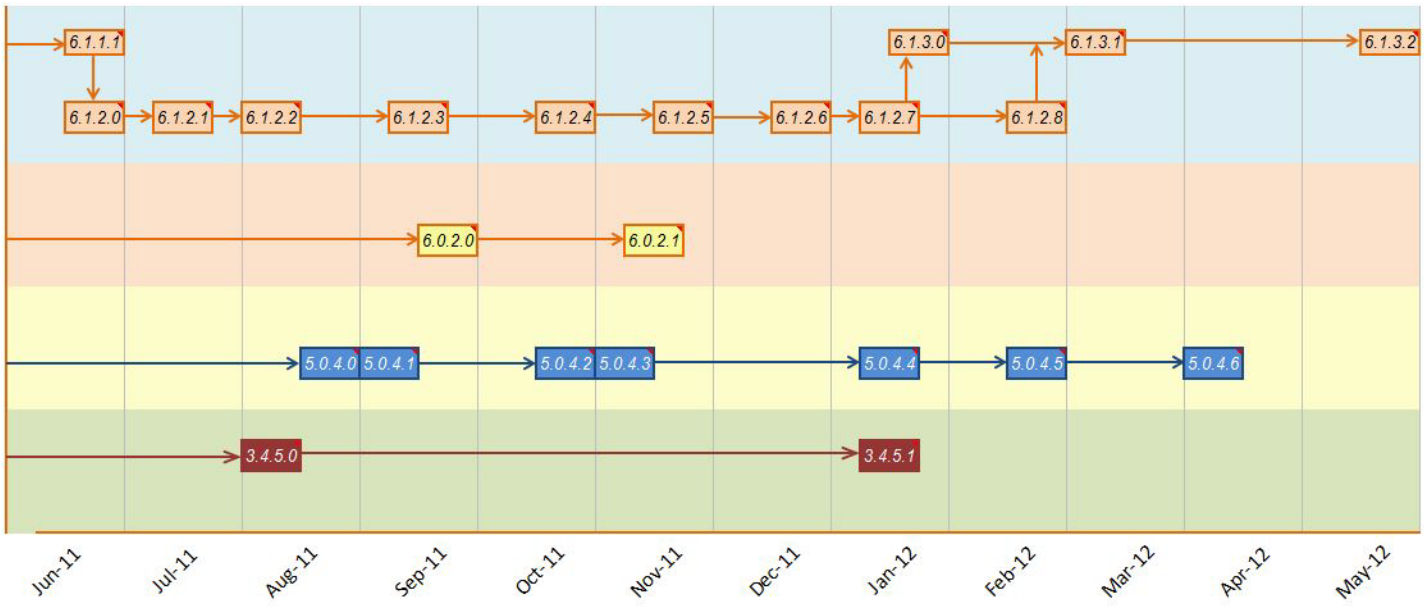
- Various enhancements have been introduced for APs and RAPs that improve their performance. See Table 1 on page 11 for list of fixed issues for APs and Table 18 on page 18 for the list of fixed issues for RAP.
- Improved security features. See Table 20 on page 18 for the list of fixed issues on Security.
- The ArubaOS WebUI has been enhanced to improve user-experience. See Table 25 on page 21 for the list of fixed issues on WebUI.
- Implemented fixes to enhance authentication processes for all network deployments and also those that include RAPs, mobile devices (smartphones, tablets, wireless handhelp devices), and third party network equipment. See Table 4 on page 13 for the list of fixed issues.
- Enhanced multimedia and mobility performances. See Table 23 on page 21 for the list of fixed issues on multimedia and Table 12 on page 15 for fixes in mobility.

To easily upgrade to ArubaOS 6.1.3.2, follow the procedures mentioned in Chapter 5, “Upgrade Procedures” on page 43 section.

Release Mapping

The following illustration shows which patches and maintenance releases are included in their entirety in ArubaOS 6.1.3.2.

Figure 1 *ArubaOS Releases and Code Stream Integration*



Contacting Support

Table 1 *Web Sites and Emails*

Web Site	
• Main Site	http://www.arubanetworks.com
• Support Site	https://support.arubanetworks.com
• Software Licensing Site	https://licensing.arubanetworks.com/login.php
• Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support/wsirt.php
Support Emails	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

Table 2 *Contact Phone Numbers*

Telephone Numbers	
• Aruba Corporate	+1 (408) 227-4500
• FAX	+1 (408) 227-4550
Support	
United States	800-WI-FI-LAN (800-943-4526)
Universal Free Phone Service Number (UIFN): Australia, Canada, China, France, Germany, Hong Kong, Ireland, Israel, Japan, Korea, Singapore, South Africa, Taiwan, and the UK	+800-4WIFI-LAN (+800-49434-526)
All other countries	+1 (408) 754-1200

This chapter provides a list of all the bugs fixed and new known issues identified in this release, as a well as a brief summary of the any new features included in this version of ArubaOS.

New Features and Enhancements

Improved Interference Immunity

The Non-Wi-Fi Interference Immunity feature can help improve performance on an unhealthy network significantly impacted by high levels of non-802.11 noise from devices such as Bluetooth headsets, video monitors and cordless phones. ArubaOS 6.1.3.2 introduces support for a more granular configuration for this feature, with seventeen different configurable settings (levels 0-16). Previous releases supported six different levels only (levels 0-5).

Higher immunity levels provide increased immunity to non-Wi-Fi interference, but some immunity levels can affect the reported noise floor, receive sensitivity of higher modulations, and the receive range of the radio. Most healthy RF environments have a noise floor below -85 dB. The Interference Immunity feature is designed for non-healthy environments and may raise the noise floor above this level. Client and AP throughput should be used to judge the health of the network with a higher noise floor.

Use this feature with caution, as it can have a negative impact on healthy networks with low levels of interference. Best practices are to first configure this feature with the default setting (level 2) then gradually increase the level one step at a time until network performance improves. Higher settings may reduce the coverage area of the AP.

Upgrade Issues

When a device using this feature is upgraded to ArubaOS 6.1.3.2, its previous Interference Immunity behavior is retained, although the actual level number may be changed to match the updated configuration scheme. For example, an AP using the Interference Immunity feature at level 4 in ArubaOS 6.0 will convert to Interference Immunity level 13 when it upgrades to ArubaOS 6.1.3.2, though the actual behavior of the feature will not change.

Updated WebUI and CLI

The **Non-Wi-Fi Interference Immunity field** in an AP's 802.11a and 802.11g radio profiles now support values from 0-16. The CLI commands **rf dot11a-radio-profile <profile> interference-immunity** and **rf dot11g-radio-profile <profile> interference-immunity** also support an increased value range (0-16).

Cell Size Reduction

The Cell Size Reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an AP's coverage area, thereby minimizing co-channel interference and optimizing channel reuse. This value should only be changed if the network is experiencing performance issue

The possible range of values for this feature is 0-55 dB. The default 0 dB reduction allows the radio to retain its default Rx sensitivity value. Values from 1-55 dB reduce the power level that the radio can hear by that amount.

Impact on Network Performance

If you configure this feature to use a non-default value, **you must also reduce the radio's transmission (Tx) power to match its new received (Rx) power level.** Failure to match a device's Tx power level to its Rx power level can result in a configuration that allows the radio to send messages to a device that it cannot hear.

Updated WebUI and CLI

An AP's 802.11a and 802.11g radio profiles now include a **Reduce Cell Size (Rx Sensitivity)** field. This feature can be configured in the CLI using the commands **rf dot11a-radio-profile <profile> cell-size-reduction** and **rf dot11a-radio-profile <profile> cell-size-reduction**.

Suppress-ARP and Broadcast-Filter ARP

Beginning with ArubaOS 6.1.3.2, `suppress-arp` on the VLAN interface and `broadcast-filter arp` on the VAP profile are enabled by default. Behaviors associated with these settings are enabled upon upgrade to ArubaOS 6.1.3.2. Note that `suppress-arp` has been modified such that gratuitous ARP will still be flooded on all AP tunnels.

WMS Configuration Changes

WMS configuration has been moved to profiles to prevent busy WMS from interfering with the completion of a `write mem` on the master controller. This change encompasses the `wms general`, `wms-local system`, and `rap-wml commands`. The newly added profiles are:

```
ids wms-general-profile
ids wms-local-system-profile
ids rap-wml-server-profile
ids rap-wml-table-profile
```

Upon upgrading to ArubaOS 6.1.3.2, WMS configuration, except `rap-wml`, will be moved under these profiles.

Single-chain-legacy is Renamed CSD-override

Starting with ArubaOS 6.1.3.2, the `single-chain-legacy` parameter in high-throughput radio profile has been renamed to `csd-override`. When this feature is enabled, all legacy transmissions will be sent using a single antenna. This enables interoperability for legacy or high-throughput stations that cannot decode 802.11n cyclic shift diversity (CSD) data, and changes 802.11n transmission by restricting CSD spreading.

This parameter is enabled by default, and will be enabled when you upgrade to ArubaOS 6.1.3.2, regardless of whether the `single-chain-legacy` setting was enabled or disabled before the upgrade. Do not disable this feature unless you do not need to support legacy or high-throughput stations that cannot support 802.11n CSD data.

Use the command `rf ht-radio-profile <profile> csd-override` to enable this feature, or disable it using the command `rf ht-radio-profile <profile> no csd-override`.

Software Retry is Renamed Temporal Diversity

Beginning with ArubaOS 6.1.3.2, the `sw-retry` parameter under the command `wlan ht-ssid-profile <profile>` has been renamed `temporal-diversity`. Additionally, the output of the command `show wlan ht-ssid-profile [<profile>]` now displays `Temporal Diversity Enable` instead of `Software Retry Enable`.

Bugs Fixed in this Release

The following issues have been fixed in the ArubaOS 6.1.3.2. For a list of issues fixed in previous versions of ArubaOS 6.1.3.x, see Chapter 3, “Issues Fixed in Previous 6.1.3.x Releases” on page 27.

Access Points

Table 1 *Access Point Issues Fixed*

Bug ID	Description
46411	Crash due to memory corruption on APs that use Dynamic Frequency Selection (DFS) channels is now resolved.
47936	The command `show ap debug system-status` returns complete and correct information for APs with more than 25 virtual APs configured.
54939, 60800	AP information is no longer missing from the SNMP table *wlanAPIpAddress*. APs with a MAC address ending with `::fe` or `::ff` were ignored if more than one AP with such a MAC address was connected to a controller.
56856	Fixed a rare crash occurring in all APs (especially AP-120 Series) that was caused by performing noise floor calibration when the radio was not ready. Upgrading to this release should fix any AP crashes where ‘ath_hal_reg_read’ is in the crash log file. Crash info can be viewed by running `show ap debug crash-info <ap-name>` in the CLI. This version verifies that the radio is ready to calibrate the noise floor before beginning a calibration.
59375	If guest account expiry date/time is not set, then the maximum account expiry time window setting in the internal DB is honored.
59611	An unexpected reboot that occurred on all 802.11n APs (except the AP-135) due to an internal process malfunction has been fixed.
60534	Root/Admin users can now create a guest user entry with expiration date beyond the maximum account expiry time window setting in the internal DB.
62110	A remote AP’s power LED no longer turns off after a while when there is no Ethernet connection.
62245, 59343	Dot1x SSID is now visible to the user when the controller is upgraded from ArubaOS 5.0.3.3 to 6.1.2.5 and when there are over 32 VLANs configured in the VAP profile.
62767	An issue was resolved in the controllers internal messaging system, where under high load, APs could randomly rebootstrap due to missed polls. Typically this issue is only seen on controllers approaching 512 APs in an environment where the APs are sending a lot of messages to the controller.
63808	Campus APs and remote APs configured with a virtual AP in bridge forwarding mode no longer experience repeated crashes due to a kernel panic. This kernel panic was caused by the code that handles client mobility in bridge mode.
64562	An AP-135 using control plane security no longer crashes and reboots unexpectedly when packet capture is initiated using the `pcap` command. This problem is specific to AP-135 and occurs when packet capture is enabled when control plane security is also on.
64874	Fixed an issue that caused the AP-61 to crash and reboot with a “Reboot caused by kernel page fault at virtual address c052d250, epc == c054271c, ra == c005426dc or ath_rx_tasklet” message in the crash log. This was due to accessing memory outside of allocated space and occurred when VAPs were created and/or deleted frequently or when scanning was enabled.
64889	The AP-105 supports the Uruguay regulatory domain.

Table 1 *Access Point Issues Fixed (Continued)*

Bug ID	Description
64926	An AP process failure that occurred when the AP received a specific type of malformed 802.11 frame has been fixed.
65034, 66243	Fixed an issue that caused the AP-65/AP-61 to reboot under high-traffic scenarios due to memory corruption.
65344, 62556, 65973	APs no longer prematurely reboot before a TFTP transfer of ArubaOS is completed.
65593	APs do not crash and reboot occasionally when a UAPSD (Unscheduled Automatic Power Save Delivery) enabled client is connected to the AP.
65869	Fixed an issue that caused AP-125s with 64Mb RAM to run out of memory and reboot after upgrading to 6.1.3.1. This occurred when too many clients (~120) associated to the AP.
66129	The issue of a AP-135 terminating on a local controller rebooting due to a crash has been fixed.
66178	The AP database on a local controller falls out of sync with the master controller when the command `clear gap-db` is executed for an AP terminating on the local controller while the local is coming up or has just gone down. This caused APs that were up on the local controller to appear as down on the master controller. This issue has been fixed.
66246	Fixed an interoperability issue between Cisco 7921/7925 and AP-130 Series in which client-transmit-frame retry percentages were very high. This occurred because control frames (e.g., ACKs) were still being sent on multiple chains even when CSD Override was enabled.
66386 66610, 66611	An issue has been resolved where the packet loss rate on 802.11n APs was high and unstable. This was caused by a problem in the packet retry mechanism. A workaround for this issue is to enable software retries and increase the number of retries in the AP. In addition, ensure that EAPOL rate optimization is not enabled when sw-retry is enabled on the AP.
66841	This release fixed an issue where the AP intermittently failed to detect the power management state of client devices and would send data to the device when it was in sleep mode.
67095	AP-70, AP-85 and AP-60 series devices configured to use the Turkey regulatory domain now fully support channels 100-140. This resolves an issue that could cause APs using channels 100-140 in the Turkey regulatory domain to stop responding or unexpectedly reboot.
67277	An issue has been fixed where the AP-135 rebooted due to an “out of memory” condition caused by a memory leak due to a failure to decrypt IPsec packets.
67284	When downgrading from 6.1.3.2 to 6.1.3.1 or older or upgrading from any release older than 6.1.3.2 with CPSec enabled, APs no longer become stuck and unable to upgrade. The upgrade now completes successfully.

Air Management (IDS)

Table 2 *Air Management (IDS) Issues Fixed*

Bug ID	Description
54574	Improvements to the Hotspotter attack detection feature enabled in the controller’s IDS Impersonation profile make this feature less likely to identify valid APs as Hotspotter attack devices.

ARM

Table 3 *Adaptive Radio Management Issues Fixed*

Bug ID	Description
65408	This release resolves an issue where changing the *allowed band for 40MHz channels* setting from “all” to “a-only” would improperly allow some APs using that ARM profile to continue to use 40MHz channels on the 802.11g radio band.

Authentication

Table 4 *Authentication Issues Fixed*

Bug ID	Description
53035	Remote APs must have different internal and external IP addresses. If the addresses are the same, an error message is currently displayed to indicate the problem.
61987	User table entries of clients that move from bridge forwarding mode to tunnel mode between SSIDs is updated appropriately.
63392	Incorrect out-of-service messages (due to wrong passwords) encountered by mobile users (specifically iPhone and Blackberry) has been fixed.
66776	An issue that caused MAC authentications to fail after an upgrade from 5.0.4.x to 6.1.3.0 has now been fixed. Best practices are to configure a default MAC server group to avoid MAC authentication failures.

Captive Portal

Table 5 *Captive Portal Issues Fixed*

Bug ID	Description
65415	An issue has been resolved where BlackBerry V5 and V7 phones connecting to an internal or hosted captive portal through a guest network with a single-character SSID name now get properly forwarded to the correct captive portal landing page, and no longer triggering an error stating “The protocol specified is not supported by the handheld. Please try a different URL.”
67114	The wired authentication profile is now assigned the “default” AAA profile. In previous releases, the wired authentication profile had no default value. This change resolves an issue where a wired client connected to a remote AP Ethernet port in tunnel forwarding mode could not access the captive portal login page.

Certificate Manager

Table 6 *Certificate Manager Issues Fixed*

Bug ID	Description
65390	The certificate installed on the Aruba mobility controller was successfully migrated after a code upgrade. In previous releases, the certificate was removed if the file name of the imported certificate exceeded 32 bytes (CERT_NAME_SIZE).

ESI

Table 7 *ESI (External Services Interface) Issues Fixed*

Bug ID	Description
65493	If a controller has both port-channel interfaces and PVST+ enabled, it might take a few seconds for the network route to converge. Until then, the controller will not accept an ESI server entry. If a controller running ArubaOS 6.1.2.0 receives a ping response from a ESI server during this delay period, then the server will be marked as UP (alive), but the update to the datapath will not succeed. Starting with ArubaOS 6.1.3.2, this issue has been resolved so if a controller sees an ESI server is up, it will retry updating its datapath until it succeeds.

Hardware Management

Table 8 *Hardware Management Issues Fixed*

Bug ID	Description
64817	Transceivers are now correctly identified when connected to M3 controllers.

IPsec

Table 9 *IPsec Issues Fixed*

Bug ID	Description
48194	An issue has been resolved where datapath routes were not updated without reloading the controller when the subnet mask for the source/destination network was changed in the ipsec-map for Site-Site VPN.
63678	When a controller comes back online after a software upgrade, the APs associated with that controller will correctly retain their proper “ap-role” user roles. This resolves an issue where a VIA client or a campus or remote AP using IPsec could revert to the “guest” (initial) user role after the controller upgrade, because the controller would erroneously remove entries for the AP from the user table along with stale VPN user entries. This issue prevented the AP from upgrading its own image, as the FTP protocol required for AP upgrades is blocked for APs using the guest user role.
64451	An issue has been resolved where a slow memory leak due to continuous failure to establish IKE SA can cause a controller in a Site-Site VPN, Master-Local, Redundant-Master, Cluster-Cluster or Remote-node topology to fail to establish IPsec tunnels or change any IPsec configuration.

Local Database

Table 10 *Local Database Fixed*

Bug ID	Description
59375	If guest account expiry date/time is not set, then the controller honors the maximum account expiry time window setting in the internal database.
60534	Root/Admin users can now create a guest user entry with an expiration date beyond the maximum account expiry time window setting in the internal database.

Mesh

Table 11 *Mesh Issues Fixed*

Bug ID	Description
54249	The 4-way dot1x handshake failure on a mesh link when EAPOL frames are sent at higher rates has been fixed. This issue occurred when a mesh link is encrypted and a mesh point sees a mesh portal with a low Signal-to-Noise Ratio (SNR). To fix this, a new setting, eapol-rate-opt, has been added to the ap mesh-radio-profile. When this setting is enabled, a more conservative rate is chosen for EAPOL frames and mesh echoes.
54518	The issue of AP-85 and other legacy mesh points randomly dropping broadcast frames in some cases, when the 'ARM/WIPS override' is enabled in the dot11a-radio-profile or the dot11g-radio-profile, has been fixed. Enabling the ARM/WIPS override in these radio profiles led to problems in the ARP resolution thereby causing mesh point reboots.
63368	The issue of 802.11n capable mesh points failing with the message *authentication time-out* following their association with the mesh port, has been fixed. The problem was particularly seen at lower SNR or when the max-retries parameter in the mesh-radio-profile was set to 4 rather than the newer default of 8. The root cause was identified as the failure to correctly mark EAPOL frames so as to benefit from rate optimization.
63463, 63640, 67424	An issue of the 802.11n mesh APs rebooting when they are configured in the 5GHz band has been fixed. The root cause was attributed to an invalid rate computed by the driver which triggered an assertion in the APs.

Mobility

Table 12 *Mobility Issues Fixed*

Bug ID	Description
54015	Wired clients connected to an L2 switch can now successfully push traffic when an untrusted port-channel uplink is used between the L2 switch and a local controller configured to use L3 mobility. Previously the clients would obtain an IP address but fail to push traffic.

OSPF

Table 13 *OSPF Issues Fixed*

Bug ID	Description
56326	An issue that could cause traffic to be temporarily disrupted on controllers using OSPF routing has been resolved through improved validation of OSPF Link-State Advertisements (LSAs) in traffic packet headers.

Platform/Datapath

Table 14 *Platform/Datapath Fixed Issues*

Bug ID	Description
49325	An issue has been resolved where passive FTP transfer did not work when Destination NAT was enabled for the user role on the controller. ArubaOS enhancements handle passive FTP with duplex data sessions (forward and reverse data sessions that are NATed.
54001	An issue has been resolved where the datapath module crashed on the controller when duplicate DNS entries were created in the netdestination whitelist.
56792, 67615	Datapath timeout issues causing occasional crashes in the 6000 controller have been fixed. The issue occurred when a packet with the corrupted header hit the datapath.
57450	The controller lost uplink communication to all the devices that are connected externally to the controller when Per-VLAN Spanning Tree (PVST) was disabled in LACP. This issue has been fixed.
59313	A fix to a previously known issue prevents memory leaks caused by continuous port flapping from triggering multiple reboots on M3 and 3000 Series controllers.
60792	An issue has been resolved where the controller crashes due to a datapath bug after upgrading to 6.1.2.4 and 6.1.2.5. The bug is triggered by IGMP Group member configuration change for ex. deletion of a slot/port member from an IGMP group.
61101	An issue of a 651 controller unexpectedly rebooting due to a memory allocation failure during a low memory state has been fixed.
62484	A controller reboot that occurred when `write mem` was executed from the CLI or WebUI shortly after a license was added has been fixed. Please note that in some cases the controller does not reboot but does experience an internal process malfunction.
62527	Executing the `phonehome` command from the ArubaOS WebUI on a heavily-loaded system no longer causes a disruption in WebUI access.
62609	An issue has been resolved where APs rebootstrap due to excessive ARPs in the network. Optimizations have been implemented in the controller to mitigate this.
62818	An issue has been resolved where user entries were not deleted from the user table even after the clients were disconnected from the network. This caused IP spoofing issues as the DHCP server allocated IP addresses of the disconnected clients to the newly connecting clients in the network.
63386	Control messages between the controller and its APs contain a sequence number between 0 and 64k. In some cases, when the sequence number rolls back to 0, the message with sequence number 0 was erroneously being dropped which triggered a timeout message in the error log. This issue has been fixed.
63843	An issue has been resolved where APs terminating on M3 local controllers were entering into a GRE tunnel teardown/setup loop when the L2 VLAN of the controller connecting the APs was same as the user VLAN configured in the virtual AP profile. As a best practice, avoid this issue by using different VLANs for the users and the AP connecting to the controller. Also, do not generate an link up event if the link is already up.
64569, 66005	An issue has been resolved where the controller rebooted due to memory buffer depletion caused by heavy IPv6 and user traffic.
65349	Enabling mobileIP and user-level debug logs on 6000-series, 3000-series and some legacy Aruba controllers running ArubaOS 6.0.x, 6.1.x, 5.0.4.x, and 3.4.5.x caused the mobileIP process to crash. This has now been fixed.

Table 14 *Platform/Datapath Fixed Issues (Continued)*

Bug ID	Description
65499	An issue has been resolved where a TFTP/FTP failure occurred when the remote APs tried to FTP the image from the master controller. This issue occurred because the controller did not lower its MTU value, causing an FTP failure for the remote APs. It is recommended to have networks with the MTU value less than the Ethernet size.
65749	An issue has been resolved where the standalone master controller crashed due to malformed multicast Microsoft Network Load Balancer packets. This issue was observed on networks configured with Microsoft TMG firewall network load balancing.
65853	An internal process malfunction on the 650 controller leading to an unexpected reboot has been fixed. This issue occurred when a split VAP had not been initialized when a station attempted to join.
66879	An issue where an internal controller hangs, causing the controller to become inaccessible, has been fixed.

PPPoE

Table 15 *PPPoE Issues Fixed*

Bug ID	Description
63840	Fragmented packets from an AP terminating on a 651, M3 or 3000 Series controller with a PPPoE uplink are no longer dropped. Improved parsing of PPPoE data, discovery packets and PPPoE encapsulated IP and IPv6 traffic resolves an issue where GRE fragments from APs could get sent to different fast paths on a multi-CPU controller, causing dropped packets and degraded traffic throughput.

PPTP

Table 16 *PPTP Issues Fixed*

Bug ID	Description
63052	Clients using a PPTP-based Virtual Private Network (VPN) to connect to a controller enabled with the AAA fast-age feature are no longer incorrectly assigned a logon user role. This resolves an issue that prevented PPTP clients from authenticating and receiving their correct user role.

RADIUS

Table 17 *RADIUS Issues Fixed*

Bug ID	Description
57005	Incorrect traffic counters reported by a RADIUS *Accounting Stop* message after a user session is terminated has been fixed.
55311	An issue with aging out IPv6 entries of dual stack clients sending incorrect *RADIUS accounting stop* messages for IPv4 entries have been fixed.
62337	An issue with AP-Group and AP-Location-Id fields in RADIUS requests being empty for wired users connected to a remote AP has been fixed.
65622	A user with more than one IPv4 address is now accounted appropriately in a RADIUS server.

Table 17 *RADIUS Issues Fixed (Continued)*

Bug ID	Description
64269	A limitation in the number of supported radius request IDs leading to increased bad authenticator count in RADIUS statistics has been fixed.

Remote AP

Table 18 *Remote AP Issues Fixed*

Bug ID	Description
59019	An issue with remote APs behind a firewall not reconnecting to controller after the firewall restart has been fixed.
62226	The number of IPsec retries in PPPoE remote APs are equal to number configured in the `number_ipsec_retries` field.
62733	Issue has been fixed where remote APs connected to a broadband router configured as a DHCP server took a longer time than usual to failover.
63222	Slower upgrades and remote AP reboots have been resolved in scenarios where multiple remote APs are connected to a broadband router or are behind a firewall such that the remote APs appear as coming from a single Public IP to the controller.

Roles/VLAN Derivation

Table 19 *Roles/VLAN Derivation Fixed Issues*

Bug ID	Description
50850	Role derivation for bridge mode users is now properly working when machine authentication and 802.1x authentication are configured at the same time. Previously, the user was incorrectly placed in the machine auth role even after successful machine authentication and user 802.1x authentication occurred.
63348	ArubaOS now accurately derives a role and VLAN for wired clients connected to the controller through an L3 device over trunk ports.
55503	Server role derivation for wired VPN users authenticating against a RADIUS server now works as expected. A bug that caused the default VPN role to be assigned to authenticated users is now fixed.
60102	ArubaOS now displays the correct VLAN for all users after successful MAC authentication.

Security

Table 20 *Security Issues Fixed*

Bug ID	Description
52016	The error message “Save failed: Module Authentication is busy. Please try later” is no longer triggered by adding 100 user roles each with six or more session ACLs.
52629	SNMP tables now include information for clients associated to a remote AP in bridge mode. The IP address matching for bridge mode users is now properly handled.

Table 20 *Security Issues Fixed (Continued)*

Bug ID	Description
54675	For ArubaOS versions greater than 6.1.x, the system now properly allows selection of 2048-bit server certificates for use with EAP Offload.
55206	The `show user ip/mac` command output now properly displays all output data. This command was displaying truncated data in ArubaOS 5.0.
59915	The issue of the controller incorrectly counting the VPN stations and VPN users which led to an "User license count error" in the controller log when a large number of VPN clients (around 2000) connected and disconnected, has been fixed. This issue may have caused the VPN client license count to run out in the system. As part of the fix, the output of the `show license-usage user` CLI command has also been refined.
60454	Ethertype ACLs now work for clients that do not have IP addresses. The Ethertype ACL information was not properly populating when the client that was sending traffic did not have an IP address and no L3 entry.
61547	The Auth module now operates properly on the controller while trying to read an invalid ap-name string in a received message. The ap-name string length on both the sender and receiver sides are explicitly checked thus avoiding corruption of the ap-name string.
61964	ArubaOS accurately displays ACL details upon running the command `show acl ace-table acl <#>`. The bug resolution is applicable when the number of Access Control Entries (for ACLs) exceeds 200. This has been fixed as the controller now properly fetches entries.
62800	The issue that caused the controller to generate the error "authmgr[1542]: Error sending the trap to SNMP agent" has been fixed.
63115	The client now properly associates with the new SSID when it switches from one split-SSID to another split-SSID on the same remote AP.
63771	A slow memory leak that eventually causes the authentication manager process to restart has been fixed. This happened when a client used EAP-TLS with termination enabled on the controller.
63914	The AuthMgr authentication process functions properly under heavy traffic stress. Previously, the AuthMgr process crashed randomly due to a segmentation fault.
64764	The show user CLI command did not work properly. The problem occurred while running the show user command in a system with a large (100 plus) number of users with long character names (200 plus characters) has been fixed.
65047	Access Control List (ACL) entries (ACE) on the controller now work properly and Mobile IP user entries are aged out appropriately. Previously, the controller would run out of ACE buffer as mobile IP visitors (users) were not aged out that prevented configuration of new ACLs.
65294	Machine authentication credentials now work properly and are no longer stored in cache after the machine has been deleted from the local user database.
65385, 60667	Authentication improvements allow TACACS command accounting to function correctly, even in environments with up to 400milliseconds delay between the controller and the TACACS server.
65688	The controller now supports a netdestination when it is being used both as source and destination in a policy and a host is added to it. An incorrect reference count for a netdestination had caused the auth process to crash on removal of policies using that netdestination.
66260	The AuthMgr authentication process functions properly when the default VLAN (1) interface is removed from the configuration. Previously, the AuthMgr process crashed with a segmentation fault when the default VLAN (1) interface was removed from the configuration.

Table 20 *Security Issues Fixed (Continued)*

Bug ID	Description
66306, 53218	The AuthMgr authentication process no longer crashes during certain LDAP authentication scenarios and LDAP authentication now works properly. Previously, the AuthMgr process crashed when LDAP referral timeouts happened.
67592	When CPSec is enabled and an AP's DHCP lease expires after the DHCP goes down, the AP will correctly reboot after it is unable to reconnect to the DHCP server.

SNMP

Table 21 *SNMP Issues Fixed*

Bug ID	Description
52186	Interface statistics now display 64-bit counter values when a user polls both *ifHCIn0ctets* and *ifHC0ut0ctets* OIDs on an M3 controller. This bug was due to 32-bit counters based implementation that resulted in incorrect values.
67190	An issue has been resolved where the SNMP process on the controller crashed multiple times. This issue occurred when MMS was used to poll the controller and when the user manually polled arubaGetTable.
60546	The snmpwalk command now performs properly. Previously, an "OID was not increasing" error displayed when users were performing an snmpwalk on *wlanAPBssidAPMacAddress* on a 651 controller.

Station Management

Table 22 *Station Management Issues Fixed*

Bug ID	Description
44866	An AP's IDS general profile no longer incorrectly references other profiles that do not exist, which could cause the controller to lose contact with its APs.
59515	The AP association table no longer shows clients with long association times who are not on the network and absent from the user table, when DOS prevention is enabled in the virtual AP profile.
51453	VLAN 217 is no longer automatically added to all virtual AP profiles on ArubaOS 6.x.
57476	A brief disruption in WebUI access caused by an internal controller process malfunction has been fixed.
59668	An internal controller process malfunction that resulted in a reboot has been fixed. The malfunction was occurred when the ACL configuration was queried by the CLI.
62305	The SNMP OID *wlsxSwitchTotalNumAccessPoints* returns the correct value (as shown in the WebUI Monitoring tab and `show ap active`) for an AP with no virtual AP and secure jack.
65158	ICMP fragmentation is now handled correctly for remote APs when the switch-IP and the LMS-IP are different. This issue occurred on all APs except the AP-130 Series, when the switch-IP and LMS-IP were different and the AP's uplink had an MTU value less than 1400.

Voice

Table 23 *Voice Issues Fixed*

Bug ID	Description
59278	A “DIGITMAP get_dialplan_profile profile not found” warning message was displayed repeatedly after upgrading ArubaOS to 5.0.3.2. This occurred because the default “Dialplan profile” was not configured with a value. Configuring the default “Dialplan profile” and adding an **X. %e** to the dialplan value resolves the issue.
62865	An issue has been resolved where an internal process stopped responding and caused the controller to reboot when the controller tried reaching a NAT-enabled SCCP client (with a private IP address) on the network.
65361	An issue has been resolved where Motorola EWP2100 phones connected to an AP-135 experienced choppy voice quality. The root cause was traced to AP-135s ignoring trigger frames from the handset for a specified period.

VRRP

Table 24 *VRRP Issues Fixed*

Bug ID	Description
67090	VRRP running on an untrusted port now works correctly.

WebUI

Table 25 *WebUI Issues Fixed*

Bug ID	Description
55993	A WebUI issue where the configuration for mapping the access-group to the cellular interface was not saved in the **Configuration** > **Network** > **Ports** > **Cellular** page, has been fixed.
64152	In the WebUI, the user was not able to create guest users with the guest provisioning account when the **end-date** checkbox was disabled in the **Configuration** > **Management** > **Guest Provisioning** page. It is now possible to create guest users with the guest provisioning account even when the **end-date** checkbox is disabled.
63236	The user was not able to configure the CHAP secret along with the PAP username in the WebUI. This issue has been fixed.
60757	An issue has been fixed where incorrect information was displayed when logging into the WebUI with a guest provisioning account in Internet Explorer 9.
52321	The **port-channel enable** checkbox in the **Configuration** > **Network** > **Ports** > **Port-channel** page now accurately reflects the status of the port-channel.
66210	An issue where the IPv6 address configured in the VLAN interface was not displayed in the WebUI has been fixed.
62519	You can now access the **Controller** > **AP** > **Status** page using Internet Explorer 8. The page did not render due to a JavaScript error and the issue has been fixed.
64566	The issue where the WebUI failed to locate rogue APs after upgrading to ArubaOS 6.1.3.0 has been resolved. The user was able to see a list of rogue APs in the **Dashboard** > **Security** page, but was not able to find out details about the physical location of the rogue AP using the **locate** link.

Table 25 *WebUI Issues Fixed (Continued)*

Bug ID	Description
66388	The message for a successful AAA test authentication in the WebUI is now displayed in green. Previously it was displayed in red which could have been interpreted as a failure of the test. AAA servers can be tested on the **Diagnostics** > **Network** > **AAA test server** page.
66230	An usability issue in the WebUI with respect to the **Edit** and **Delete** buttons corresponding to the AP Groups in the **Configuration** > **WIRELESS** > **AP configuration** > **AP Group** has been fixed. Click on the **ap-group name** link to edit the ap-group and the **Delete** button to delete the ap-group.
67091	Extremely long user names caused the **Dashboard** > **Client** page to display a blank page due to a JavaScript error. Usernames up to 64 characters are recommended.

Wireless Management System (WMS)

Table 26 *WMS Issues Fixed*

Bug ID	Description
61660	The controller's Wireless Management System (WMS) can consistently classify APs or wireless clients as rogue or valid devices, and is no longer disrupted by issuing the command **show wms client probe** in the command-line interface or viewing clients on the **Monitoring** > **Controller** > **Clients** page in the WebUI. This resolves an issue where WMS processes could be disrupted by running the commands for a monitored AP or client in a dense network environment, where the monitored AP or client could be seen by at least 115 other Aruba APs.

Wireless Mobility Management (WMM)

Table 27 *WMM Issues Fixed*

Bug ID	Description
65161	Changes to how MAC-level protocol data units (MPDUs) are counted has resolved a known issue that could make the output of the **show ap debug** CLI command display inaccurate data for transmitted WMM frame (Tx WMM) counters. This issue did not impact WMM traffic, just how WMM traffic statistics were displayed.

New Known Issues

The following issues have been identified since the last release. For a list of known issues found in previous versions of ArubaOS 6.1.3.x, see Chapter 4, “Known Issues Identified in Previous 6.1.3.x Releases” on page 35.

Access Point

Table 28 *Access Point Known Issues and Limitations*

Bug ID	Description
59177	The Aruba 651 controller may become unstable and crash frequently with cfgm, arc cli, and nanny. This may be due to the controller running out of memory. Making the internal AP inactive will prevent the crash.

Table 28 *Access Point Known Issues and Limitations (Continued)*

Bug ID	Description
56678	The Goodput (bps) values displayed on the **Dashboard>Access Points** and **Dashboard>Clients** pages in the controller WebUI appears lower than the expected value. As a workaround, view the usage data on the **Dashboard>Usage** page.

Authentication

Table 29 *Authentication Known Issues and Limitations*

Bug ID	Description
56236	A replay counter mismatch might be observed during the 4-way handshake in WPA2-AES mode with Cisco 7921 and 7925 handsets. This usually happens after the clients come back up from power save mode. This mismatch will not be seen on the next attempt.
61935	A DHCP fingerprinting user-derived rule with a **set-vlan** action does not work with 802.1x authentication. This type of rule does work on an open system network.

Platform/Datapath

Table 30 *Platform/Datapath Issues and Limitations*

Bug ID	Description
56242	The VPN Site-to-Site IPsec tunnel is unstable when a high rate of traffic is generated. This is caused by a miscalculation of the IPsec tunnel's idle timeout that triggers the Dead Peer Detection (DPD) exchange. As a workaround, disable the DPD on both controllers to prevent the tunnel from failing.

Remote AP

Table 31 *Remote AP Issues and Limitations*

Bug ID	Description
61428	In some cases, if an authentication process restart on controllers that have ACLs configured with large number of ACEs could cause APs to reboot. As a workaround, reboot the controller.

Role/VLAN Derivation

Table 32 *Role/VLAN Derivation Issues and Limitations*

Bug ID	Description
51691 56746	When using DHCP user derivation rules and captive portal authentication, the client is assigned to the wrong role after a DHCP-Renew. All controllers running version ArubaOS 6.1.0.0 are affected. DHCP user derivation rules and captive portal cannot be used together.

SNMP

Table 33 *SNMP Issues and Limitations*

Bug ID	Description
66990 59292	When using HP OpenView MIB version 9.10+, you may see errors while importing the MIB. This may occur if you are using a newer MIB browser. As a workaround: Select the MIBs that have errors and change: TEXTUAL-CONVENTION to: TEXTUAL-CONVENTION FROM SNMPv2-TC **NOTE:** Make sure you do not have a comma ',' at the end when updating.

Startup Wizard

Table 34 *Startup Wizard Issues and Limitations*

Bug ID	Description
66893	The campus WLAN wizard throws error when deleting a WLAN using **Exit Now** link in Step 1 after modifying the WLAN multiple times with regards to authentication type and internal/guest mode. As a workaround, delete the WLAN using WebUI or CLI.

Issues Under Investigation

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

Access Points

Table 35 *Access Points Observed Issues*

Bug ID	Description
66820	An AP-65 model access point reboots continuously. This may be related to the fact that the device was simultaneously upgraded and moved from a 5.0.x release an older Aruba 200 controller to a 6.1.x release on newer 3000 Series controller.

Air Management - IDS

Table 36 *Air Management - IDS Observed Issues*

Bug ID	Description
65946	The tables in the **Monitoring>Network>All Access Points** page of the WebUI and in the output of the `show wms ap list` command in the CLI show an incorrect number of users.

OSPF

Table 37 *OSPF Observed Issues*

Bug ID	Description
62839	The OSPF process on the controller may not function correctly when OSPF routing, OSPF neighbors, and a DHCP helper IP address are configured, causing the controller to reboot.

Platform/Datapath

Table 38 *Platform/Datapath Observed Issues*

Bug ID	Description
66612	iPad and iPhone VPN clients disconnect after five to ten minutes if their IP address is NATed on the controller.
66725, 66275, 66338, 66361, 65690, 65632, 65984	An internal controller process malfunction, leading to a controller reboot, has been observed.
66359	High datapath utilization was observed on a controller, which resulted in user connectivity issues and packet loss.
66798	After upgrading to ArubaOS 6.1.3.0, it has been reported that slower-than-expected throughput has been experienced when bandwidth contracts are enabled.

Security

Table 39 *Security Observed Issues*

Bug ID	Description
62099	When connecting a client to an untrusted wired port, user entries appear in the `show user-table` output and are not aged out. To avoid stale user entries from consuming user licenses on the controller, use the `aaa user delete` command to delete unwanted user names.
65629	When a user with the same MAC address as another IP user who has not aged out tries to connect to the controller using three different IPv4 addresses (simultaneously or in succession), the Auth module crashes and the Auth process restarts. As a workaround, avoid a situation where a user with the same MAC address has more than two IP addresses.

Station Management

Table 40 *Station Management Observed Issues*

Bug ID	Description
65810	An internal controller process malfunction, which causes APs connected to that controller to rebootstrap and failover to a backup controller, has been observed.

WebUI

Table 41 *WebUI Observed Issues*

Bug ID	Description
66516	When APs are distributed in multiple pages in the WebUI in the **Configuration** > **WIRELESS** > **AP Installation** > **Provisioning** tab, the UI sorts only the APs in the current page and not the entire list.
66521	In the WebUI, while creating an user you see two **Apply** buttons in the **Configuration** > **Security** > **Authentication** > **Internal DB** page. The **Apply** button at the bottom of the page does not add the user but does apply any user list changes that already exist. Click the **Apply** button at the top to add a new user. After the screen refreshes, click the **Apply** button at the bottom to apply any user list changes.

WMS

Table 42 *WMS Observed Issues*

Bug ID	Description
65702	The controller's Wireless Management System (WMS) utilizes a large amount of CPU resources, preventing users from changing or saving their controller’s configuration.

Chapter 3

Issues Fixed in Previous 6.1.3.x Releases

The following issues have been fixed in this release of ArubaOS.

Fixed in 6.1.3.1

Table 1 *Bugs Fixed in 6.1.3.1*

Bug ID	Description
60276	Serbia regulatory domain support is available for the AP-130 Series.
61191	An issue has been resolved where RX frames which were not mapped to an RX descriptor could cause an AP to unexpectedly reboot.
62391	Improvements to RX queue access resolved an issue that could cause an AP to unexpectedly reboot.
62405	Argentina regulatory domain support is available for the AP-130 Series, the AP-175P, and MSR2K23NO.
62507	Oman regulatory domain channels were updated for the AP-124 and AP-125.
62650	Ukraine regulatory domain support is available for the AP-130 Series.
62710	Algeria regulatory domain support is available for the AP-130 Series.
63155	Support for the AP-105, AP-125, and AP-130 Series has been added for Peru, Venezuela, Tunisia, and Israel.
63273	An AP-134 crash and reboot with reboot reason “Reboot caused by kernel panic: Fatal exception” has been fixed.
63909	The frequency band and regulatory maximum EIRP settings for Saudi Arabia have been updated.
63338	Deauthentication messages are no longer sent over the air for internal ageouts if NI is not found.
63978	An issue in which clients were intermittently unable to connect to an AP-135 and once connected, experienced slow throughput, has been fixed.
64576	Enabling EAPOL optimization no longer reduces the number of retries of EAPOL frames.
60152	Clients sending user credentials to the AP before the “Interval between Identify requests” wait time defined in the 802.1x authentication profile could not complete 802.1x authentication after association.
64322	Users coming through a L2 GRE tunnel are now correctly placed in the role defined per the VLAN wired AAA profile.
60119	A controller interface can be configured with both a interface description and a trusted VLAN with an assigned AAA profile.
61232	A configuration option has been added in the connection profile to display a banner message to all VIA users accessing the system.

Table 1 *Bugs Fixed in 6.1.3.1*

Bug ID	Description
57612	Site-to-Site IKEv2 with certificate and fragmentation now works correctly when MOBIKE is enabled.
63838	An isakmpd module crash that occurred when ArubaOS received a DPD packet and message did not point to isakmp_sa has been fixed.
43835	XFP-based ports no longer incorrectly stays up after removing the XFP module or the cable connected to the XFP module.
64273	An unexpected controller reboot caused by STM module crash due to a non-noe voice client hitting noe alg has been fixed.
57831	Improvements to the datapath module increase controller stability, and prevent the controller from failing to respond due to datapath exceptions.
57950	Improved serialized access of data in the Adjacency Protocol (AMAP) module has resolved an issue that caused the fpapps process to stop responding.
60811	Changes to the handling of unknown unicast MAC addresses has resolved an issue where the datapath bridge table could get saturated and cause high levels of datapath utilization.
62095	Upon upgrading, if an additional image is required due to missing ancillary files, the controller now displays stating the ancillary files is missing and the flash may need to be cleared.
65288	ArubaOS now supports prioritization of Lync RTCP packets.
61586	CSS now works correctly with RAPs in split-tunnel mode.
54621	Improvements to RF Plan resolved an issue where heat-maps displayed in the WebUI did not always take their expected shape.
62694	Improvements to the format of RF Plan files allow files to be imported using the RF Plan WebUI without triggering XML errors.
56267, 62052	An auth memory leak for the memory allocated in user_add_af_ap() has been fixed.
61921	Memory improvements increase the stability of the auth module.
54413, 53711, 55123, 57512	Resolved an SNMP issue triggered by internal user IP address lookup.
62455	The ifIndex value returned by the IP table during an SNMP walk on a 620 controller correctly matches the MIB value returned in the ifDescr table.
61259, 61261	A new configuration setting has been added to enabled or disable Domain Pre-connect under the VIA connection profile.
63521	Audio and Video sessions with the same session ID no longer cause the STM module to stop responding after both sessions age out.

Fixed in 6.1.3.0

Table 2 *Bugs Fixed in 6.1.3.0*

Bug ID	Description
63112	The default ap regulatory-domain profile does not contain any 40 Mhz channels defined for 5 GHz. So, an AP that supports DFS channels (AP-120 Series) will randomly choose any channel from the DFS and non-DFS 40 Mhz pairs.
63083, 65595	Controller reboots due to datapath exception triggered by a race condition when bandwidth contracts are configured, is now resolved.
59484	Nothing is written into the HAL registers (disable or enable interrupts) if reset/chan change is in progress.
44112	This release has resolved an issue that caused RAP-2WG APs to perform unwanted reboots has been fixed.
52450	APs no longer ignore association requests if all the APs associated to a local controller rebootstrap at the same time.
61340 61342	Improvements to the **pppd** service and timer checks prevents Remote APs from performing unwanted reboots.
61720	The default regulatory domain profile for the country code JP3 contains all valid channels for that regulatory domain.
62267	Heartbeats from an AP-125 correctly appear in the output of the **show ap debug system-status** command.
59027	The bridge user-entry now correctly ages out, if the user has roamed to another remote AP on a different management VLAN.
52892	AP-68P no longer drops frames greater than 1468 bytes for a bridged VAP with a VLAN.
53835	AP-124 and AP-125 now accept FCC DFS channels.
55939	A Regulatory domain for AP-124 and AP-125 in Croatia had been approved but was not enabled in AOS. The Croatia country code was enabled in the controller and the AP's regulatory domain was integrated in AOS.
57249	Client can associate as 40Mhz capable with ZA regulatory domain. Before the fix, with ZA regulatory domain client could associate only as 20Mhz capable.
58380	AP-125 no longer crashes after repeated VAP enable or disable attempts.
58534	AP-125 no longer crashes after upgrading to new build.
58261	AP-105 crash with a raw call trace `tlb_do_page_faults` no longer occurs.
57578	AP kernel panic messages no longer occur.
51460	AP-125 no longer crashes due to a kernel page fault at the virtual address.
54256, 54609, 57659	An AP crash due to a kernel page fault caused by a stack corruption has been fixed.

Table 2 *Bugs Fixed in 6.1.3.0*

Bug ID	Description
53897, 52825, 55118, 53365, 59274, 61930	An AP-125 crash caused by a node leak has been fixed.
59367, 59371	An unwanted AP reboot caused by a kernel panic at ath_process_uapsd_trigger message no longer occurs.
59643	An unwanted AP reboot caused by a kernel panic at bogus non HT station count 0 - ieee80211_node_leave no longer occurs.
56707	The show AP database command no longer displays the Local controllers down on the Master, when all the APs on the Local controllers are up.
53438	AP-61 no longer incorrectly reboots with "Kernel Panic Error."
57802	The ESI-installed blacklist entries are no longer unexpectedly installed as "Permanent" instead of being governed by the Virtual AP's “Blacklist Timeout”.
59239	Better mechanisms to debug low free memory on APs are now available.
59706, 61804	An unwanted AP reboot caused by a kernel panic at aruba_deferred_set_channel message no longer occurs.
53389, 61564	The packet capture no longer triggers an ARM channel change with reason "INV".
56272	Incorrectly encoded redirect URLs from a captive network no longer cause a problem.
45571, 58833	Captive portal is now working on the local controllers when the guest VLAN has “ip nat inside” enabled.
58729	The command `ipv6 cp-redirect-address disable` now works correctly.
48961	When the port status is changed to "down," the speed/duplex configuration is no longer incorrectly removed.
52248	The manual blacklist command now accepts the MAC address without a colon.
48836, 51456	The `backup flash` command no longer falsely displays an error on legacy platforms.
51159	M3 no longer sticks in bootloop due to configuration corruption.
43431, 50855	Client blacklisting now works correctly when `max-authentication-failures` is set to 2 or a larger value.
48793	The disconnect ACK now uses the correct source IP address and Amigopod does not drop it.
57802	The ESI-installed blacklist entries are no longer unexpectedly installed as “Permanent” instead of being governed by the Virtual AP's “Blacklist Timeout”.
53189	Improvements to the syslog process allow you to change user roles through the Extended Services Interface (ESI).

Table 2 *Bugs Fixed in 6.1.3.0*

Bug ID	Description
49504	The `show inventory` command now correctly displays the serial number and other data on M3 slot #1.
49956	The syslog is now sent out following a fan failure.
62298	On a 3000 Series controller, using SFP-SX transceivers, the link state will indicate going up continuously in the syslog. The actual link state itself does not flap. However due to the link up transitions internally, STP, OSPF, LACP will not converge. If you are not running any of these protocols on that port, there should be no effect.
56371	A Redundant-Master controller will no longer reboot with “Reboot Cause: Nanny rebooted machine - isakmpd process died."
53218	Auth module no longer crashes during an LDAP authentication timeout.
53391	The local user DB now adds the Remote IP correctly even when the first octet of the IP address is greater than 127.
55202, 55003	After failing MAC authentication and falling into the Initial-Role of the AAA profile, if the user attempts to reconnect, MAC authentication will correctly happen again.
53984, 63277, 53904	AMs no longer report rogues with SSID 'tarpit' in environments where no wireless neighbors should be seen. No SSID 'tarpit' was configured. And this was reported from multiple devices.
62296, 62297, 62502, 62477, 62468	An Aruba 651 controller is no longer susceptible to continuous rebooting if its internal AP (radio) is configured in Air Monitor mode (am-mode).
58601	The controller no longer gets SQL syntax error messages after upgrading.
55740	Mesh points no longer crash in node_cleanup() after downgrading the controller.
56398	The loopback address can now be advertised through OSPF when the loopback address is in a different subnet than any configured VLANs.
52093	Issuing the CLI command l**ocal-userdb-guest del username <name>** and **local-user del username <name>** no longer causes a controller to run low on memory and unexpectedly reboot.
52492, 53600, 56561, 54231, 57302, 55620, 61152, 61155, 56928	An unexpected controller reboot due to a hard watchdog accompanied by “reason for reboot: unknown” has been fixed. Additionally, a change has been made to ArubaOS to prevent the use of “reason for reboot: unknown” for unexpected reboots. Unknown reboots we caused by flash write failures. Now, the flash write is retried by performing an erase followed by another write.
53332	Improvements to the **Datapath** module prevent the controller from performing unwanted reboots.
60373	Improvements to SOS crash dump collection allow datapath crashes to recover more quickly.
60431, 63006	Issuing the CLI command show trunk no longer causes the **fpapps** module to stop responding when the controller includes a large number of non-contiguous VLANs.

Table 2 *Bugs Fixed in 6.1.3.0*

Bug ID	Description
46116	The TCP maximum segment size for TKIP tunnels has been reduced to better accommodate the WEPCRC length.
58502	Packets are now sent from the trunk port on the controller to a client on the trunk port behind a remote AP with a proper VLAN tag.
52845	Proxy-arp now provides support for split-tunnels.
54191, 55794	FTP data transfer and reuse of a stray session no longer triggers a race condition and datapath timeout exception.
54943	Users are now able to get IP address on VMWare Fusion.
52092	Client with .255 IP address can now ping across L2 GRE.
52732	M3 datapath no longer crashes.
60670	The 620 controller no longer reboots due to a datapath exception when connected to a Bell ADSL modem.
59078	Controller tagged VLAN traffic received through trunk port is no longer sent out the egress port without a PPPoE header.
53821, 54053, 55125, 55130, 55616, 56657, 59457, 62102, 62006, 62206	The mysql process now begins before any other processes to help prevent an unexpected controller reboot that occurred following a number of module crashes.
50914	The cfgm local is now able to successfully create a socket for connecting to the cfgm master and receive its configuration.
54194, 54238	Improvements to the PAPI timeout handler prevent memory errors that could trigger unwanted controller reboots. The PAPI timeout handler now validates the buffer before taking any action.
58097	A local 620 controller connected through a DSL modem using PPPoE is now able to reach the master controller.
53709	A RADIUS packet no longer limits a client's username to 32 bytes when EAP termination is enabled on the controller.
59723, 59743	User traffic will be passed normally if the client connects to a VAP in split-tunnel forwarding mode, the client has a initial user role of **denyall** (any any any deny), even if the wireless adapter on the client is disabled then reenabled.
60167	If PPPoE remote APs using certificates and IKEv2 have a static inner IP addresses but then later change their outer IP address or port during rebootstrap, the inner IP route is retained when the remote APs establish a new IKE SA to the controller.
61000	Improvements to the handling of HELLO packets allow remote APs to be able to properly associate to their controller upon upgrading to ArubaOS 6.1.3.

Table 2 *Bugs Fixed in 6.1.3.0*

Bug ID	Description
60458	Remote AP mesh portal and wired bridging are no longer failing. Customer required LAN extension by using enet port of mesh point to locally bridge via Remote Mesh Portal. This bridge failed as the incoming user on the mesh point did not pickup a valid user ACL. All traffic (except ARP) was blocked by the firewall on the Remote Mesh Portal.
53408	When the VLAN ID is not set in the virtual-ap profile, the VAP survives when connectivity to the controller is lost and the AP is rebooted.
59744	The RAP-2WG now correctly switches to the second controller IP returned by the DNS server when the first one is not reachable.
44973	The Group Key is now present on a bridge/split virtual AP and now correctly matches with the controller auth.
45719	The remote AP now comes up when connected to a DSL modem (Dlink) with a DHCP scope in the range of 192.168.11.x, and 192.168.11.1 as its own IP.
47990	Backup SSID users correctly show up on the L3 user table and do not incorrectly age out.
59036	Clients can now send traffic if the controller is not reachable from a remote AP, clients are connected to backup/always/persistent bride mode virtual AP's, and no PEF-NG license is installed.
55438	The dhcp-option user derivation rules that involve multiple dhcp-options now work correctly.
57474	This release includes ability to filter the IPsec mirroring to a single peer with the CLI command **firewall session-mirror-ipsec peer <peer_ip>**.
61551	Improvements to the **Auth** module prevent the controller from performing unwanted reboots.
52494	An unexpected controller reboot due by an auth module crash caused by a memory leak has been fixed.
55519	Auth module now operates correctly on the controller and Authmgr no longer registers 100% busy.
51888	Successful authentication no longer incorrectly displays the error log.
52592	The "show global-user-table" command no longer takes 2 minutes to respond in a master/backup scenario.
52181	Rule can now be removed from an ACL
59661	An unexpected controller reboot due by an auth module crash caused by a memory leak has been fixed.
58786	The "authmgr get segfault" message no longer occurs while processing a new user and trying to perform "devid cache lookup mac."
51393	MIPT phones no longer reboot with "any any udp 68 deny rule" in validuser ACL.
53988	L2 roams now generate the `wlsxUserEntryAttributesChanged` message.
54334	Upgrading no longer corrupts the wlanAPBssidAPMacAddress OID.
60667	Authentication improvements allow TACACS command accounting to function correctly, even in environments with up to 400milliseconds delay between the controller and the TACACS server.
58895	Applying a "noe-acl" no longer causes RTP packets to be dropped for IP Touch 310/610 phones.

Table 2 *Bugs Fixed in 6.1.3.0*

Bug ID	Description
57869	High CPU in STM no longer causes APs to drop from controller due to certain netservice configuration.
58554	The CAC call status for an Alcatel OmniTouch 8128 phone properly resets back to zero after session termination.
44110	Cisco Phones plugged in the wire behind the remote AP are no longer unnecessarily re-registering with Call Manager.
54467	When an AP is provisioned with a white space in between the AP name (example: "AP NAME"), the AP provisioning page no longer comes up blank.
55205	The Netdestination entries can now be deleted.
52453	WPA-PSK Pre-Shared Keys are now accepted by the controller GUI.
54387	There is no issue with VLAN pool in the GUI.
54516	Alcatel-Lucent SR-1-123255069: IE no longer has a Red Cross mark in the Guest Provisioning (Page Design field).
58485	WebUI now correctly displays the EVENTS and REPORTS tab.
55949	WebUI Mesh now correctly shows "Rate RX/TX" in the "Last Update" field.
50500	Client activity is now displayed properly on WebUI for wired clients on Remote AP.
60529	Trying to emulate WISPr client using wget no longer gets wrong redirection if custom SSL cert is used.
58882	A RADIUS accounting start message will not be sent to the RADIUS server if a user is deleted via an XML API **user_delete** command issued from an external XML API server.
49321	The Radius attributes in "Aruba-Location-Id" are filled correctly when forward mode is split-tunnel.

Chapter 4

Known Issues Identified in Previous 6.1.3.x Releases

This chapter describes the known issues and limitations in this version of ArubaOS.

Supported Browsers

Beginning with ArubaOS 6.0, the following browsers are officially supported for use with the ArubaOS WebUI:

- Microsoft Internet Explorer 8.x on Windows XP, Windows Vista, Windows 7, and MacOS
- Mozilla Firefox 3.x on Windows XP, Windows Vista, Windows 7, and MacOS
- Apple Safari 5.x on MacOS

Maximum DHCP Lease Per Platform

Exceeding the following limits may result in excessive CPU utilization, and unpredictable negative impact on controller operations.

Table 1 *Maximum DHCP Lease Per Platform*

Platform	Description
M3	512
3200	512
3400	512
3600	512
600 Series	512

Aruba 651 Internal AP

It has been observed that an Aruba 651 controller will reboot unexpectedly when the internal AP is enabled (bug 60722 and duplicates). to disable the internal AP, complete one of the following procedures:

In the CLI

1. Create a dot11g radio profile and disable the radio

```
(Aruba651) #configure terminal
(Aruba651) (config) # rf dot11g-radio-profile disable-radio
(Aruba651) (802.11g radio profile "disable-radio") #no radio-enable
(Aruba651) (802.11g radio profile "disable-radio") #exit
```

2. Apply the radio profile to a specific AP.

```
(Aruba651) (config) #ap-name <ap-name>
(Aruba651) (AP name "<ap-name>") #dot11g-radio-profile disable-radio
(Aruba651) (AP name "<ap-name>") #end
```

3. Save the configuration

```
(Aruba651) #write memory
```

In the WebUI

Creating a Profile

1. Navigate to **Configuration > Wireless > AP Configuration**. Select the AP Specific tab.
2. Click the Edit button by the AP for which you want to create a new RF management profile.
3. In the Profiles list, expand the RF Management menu, then select 802.11g radio profile.
4. Click the 802.11g radio profile drop-down list in the Profile Details window pane and select NEW.
5. Enter a name for your new 802.11g radio profile “disable-radio”
6. Uncheck the “Radio Enable” checkbox to disable the radio then click Apply to save your settings.

Access Point

Table 2 *Access Point Known Issues and Limitations*

Bug ID	Description
64248	When using Iperf to measure throughput, in one case, Last_ACK_SNR was seen to drop from 45 dB (idle) to 20 dB. When the client is idle or not running Iperf, the two SNR values are very close. There is no applicable workaround, as this is an observation while testing throughput using Iperf.
62672, 63154, 61669	Rarely, it has been observed that a 651 controller reboots after some days if its internal AP (radio) is configured in Air Monitor mode (am-mode). This could be triggered if memory becomes full by air monitoring statistics or excessive monitoring events for a number of days. As a workaround, reconfigure the internal AP (radio) in Access Point mode (ap-mode). Alternatively, you may disable the radio if not needed.
61938	In a rare situation a remote AP may fail to renew ip-address through DHCP after rebootstrap event. A remote AP will reboot when it is stuck in this state, as it will hit retry-ipsec count. After rebooting the remote AP will recover from this state.

57624	AP-105s might not come up when connected to a Cisco PoE switch (WS-C6509-E:WS-X6148A-GE-45AF). The APs are not powering up despite the maximum amount of power being allocated to the port the AP is connected to. The following error messages were returned when a `shutdown` or `no shutdown` was executed on the port the AP was connected to:
	`%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEthernet9/48 (not half duplex), with SEP001BD5E87C32 Port 1 (half duplex).`
	`%C6K_POWER-SP-1-PD_HW_FAULTY: The device connected to port 3/2 has a hardware problem. Power is turned off on the port.`
	`%C6K_POWER-SP-1-PD_HW_FAULTY: The device connected to port 3/2 has a hardware problem. Power is turned off on the port.`

Table 2 *Access Point Known Issues and Limitations (Continued)*

Bug ID	Description
60722, 61100, 57925, 60846, 64517, 66118, 66128, 66185, 66659, 64526, 61539, 61196, 67435, 67670 67671, 67673, 67871, 67872, 67977, 63460, 65049, 62111, 66409, 66136	Aruba 651 controller might crash and result in unexpected reboot when the internal AP is enabled. As a workaround, disable the radio on the internal AP on Aruba 651 controller. To disable the radio for a specific AP, please follow the instruction provided in "Aruba 651 Internal AP" on page 35.

ARM

Table 3 *ARM Known Issues and Limitations*

Bug ID	Description
62878	If band steering is enabled, errors in the voice-aware band steering feature can cause active 802.11a/g capable voice clients to be disassociated from an AP if those clients roam to a new 802.11g radio.
56760	Per-SSID bandwidth contracts do not work well with decrypt-tunnel mode with UDP traffic. For example: • the actual bandwidth allocation is around 25% off compared to the configured bandwidth allocation. With tunnel mode, the error rate is only 5-10%. • the maximum UDP throughput for a single client is only 155 Mbps, which is about 30Mbps off when compared to 183 Mbps in tunnel mode.

Authentication

Table 4 *Authentication Known Issues and Limitations*

Bug ID	Description
56130	When roaming between wireless and wired users, a user may fall into a logon role instead of a mac-auth role.

IPv6

Table 5 *IPv6 Issues and Limitations*

Bug ID	Description
57059	When maximum number of IPv6 L3 interfaces exceeds the supported platform limit, it affects the routing on controller. Be sure not to exceed the maximum number of IPv6 L3 interfaces.

Management

Table 6 *Management Issues and Limitations*

Bug ID	Description
61423	Some old user entry in the user table may not age out even after the client disconnects from the network. As a workaround use the command `aaa user delete` to clear such old stale entry.
63800	Valid APs might be incorrectly and randomly classified as unknown on local controller in a multi-controller environment. As a workaround, manually reclassify those AP as valid.
62852, 64110	In few cases, we noticed a controller may restart unexpectedly due to wms module restart. It does not have any operational impact on clients. As a workaround, delete WMS entries from the controller database and restore wms-backup.db. Your local Aruba Support or Sales contact can help restoring this.
56666, 63279	In some cases, the station table might show a large number of stale entries. As a workaround, use the command `aaa user delete` to clear the user entries.

Mesh

Table 7 *Mesh Issues and Limitations*

Bug ID	Description
56642	An AP-135 configured as a mesh point will fail to upgrade if the mesh link to the 2 spatial stream Series (10x,9x,12x, 175 series) mesh portal is using HT mode. As a workaround, do not enable HT on an 2 spatial stream mesh portal or change the default supported-MCS from 0-23 to 0-15."

Mobility

Table 8 *Mobility Issues and Limitations*

Bug ID	Description
62988	Wireless clients might incorrectly be assigned to the wrong VLAN when VLAN mobility is enabled. As a workaround, set firewall bandwidth contract to Default.
63163	Mobility-enabled datapath bridge entries are getting deleted for untrusted users. Mobility is deleting and adding the datapath bridge entry for the clients even when there is active traffic going on. It happens only when Mobility is turned on.
63164	The mobile IP module might crash when there are several hundred mobile clients in addition to another 1000+ users, and all are L2 roaming.

OCSP/CRL

Table 9 *OCSP/CRL Known Issues and Limitations*

Bug ID	Description
55419	The certmgr module becomes busy when a large number of OCSP requests hit the certmgr while the OCSP server is unreachable. This issue will appear whenever there is misconfiguration or outage between the controller and the OCSP responder.

Platform/Datapath

Table 10 *Platform/Datapath Known Issues and Limitations*

Bug ID	Description
58011, 64524, 64517	An Aruba 651 controller with the internal AP enabled is susceptible to unexpected rebooting due to an internal memory leak. As a workaround, disable the internal AP.
63140	A controller may experience a datapath timeout if 2,000 users are created from an untrusted port with upstream and downstream per-user bandwidth contracts.
62838	If an AP comes up on an untrusted port where the first port rule is allow all, that AP's sessions may be denied.
62238	In a network where the user VLANs extend from the controller to an uplink Cisco switch, there are certain applications that try to reach the users connected behind a RAP. The Cisco environment has the ARP Ageout and the Cam table ageout set to 4 hours. This causes any traffic sent to the controller for any user who has aged out to get flooded to all users in that VLAN.
63359, 62551	The kernel module crashed on the standby controller while running ArubaOS 6.1.2.5. The Reboot Cause shows `User pushed reset` when we are not able to write the cause of the reboot. The cause could be software watchdogs, SOS crashes, bus/cache errors, and busy CPUs.
58487	In some cases, with control plane security enabled, APs might take a long time (more than 30 minutes) to come up. This is due to control plane security SA setup timing out because the AP is not receiving the fourth IKE packet from the controller.

Port Channel

Table 11 *Port Channel Known Issues and Limitations*

Bug ID	Description
62936	If the native VLAN of a trunk LACP port channel is set as untrusted, LACP member ports may stop responding upon upgrading the controller to ArubaOS 6.1.3 or later.

PPTP

Table 12 *PPTP Known Issues and Limitations*

Bug ID	Description
55177	A Mac PPTP client connecting to an M3 as a PPTP server might be disconnected if it is idle for 10 minutes.

Remote Access Point

Table 13 *Remote Access Point Known Issues and Limitations*

Bug ID	Description
63073	Saving a backup of a virtual AP on a remote AP to flash memory may fail if the virtual AP has large ACLs with 500 ACE entries. As a workaround, reduce the number of ACE entries on the ACLs before saving the backup.
51546	While using Sierra modem 312 for a 3G uplink on a remote AP; 3G to wired failover may leave the USB in hung state. Rebooting the remote AP will make it recover from this state.

Security

Table 14 *Security Known Issues and Limitations*

Bug ID	Description
47868	The name option under the `netdestination6 ipv6 alias option` does not exist.
55913	After issuing the `aaa user delete all` command, users might be incorrectly placed in the logon role.

61690	In an ACL with the following lines:
	`ip access-list session good`
	`any any any deny blacklist log`
	The ACL has enabled the blacklist option, and the valid client is falling into the MAC auth default role. The non-valid client is being denied but not blacklisted.

62437	The AAA state for the an AP does not get cleared after the AP completes 802.1x authentication. The IP address from the AP's first assigned VLAN stays associated to the AP's MAC address, even after the AP moves to a different VLAN. As a workaround, manually change the AAA state of the AP and reboot the controller.
55898	The command `show user` does not display the correct information for captive portal users when those users are connected through an L3 gateway.
56503	The username shown in the user table is the client's dot1x username instead of the captive portal username when the client disconnects and then reassociates.
57500	Custom captive portal login pages do not work when guest logon is enabled. The guest logon field is not displayed on the custom login page. This issue does not occur with the default Aruba login page. As a workaround, use the default captive portal page or use user logon.

Syslog

Table 15 *Syslog Known Issues and Limitations*

Bug ID	Description
62916	Access Points may send debug log messages to the Syslog server, even if debug log messages are disabled.

Voice

Table 16 *Voice Known Issues and Limitations*

Bug ID	Description
65546	Classified media sessions from Lync clients might not be fast aged after call termination.
56506	SIP ALG might generate an additional CDR with invalid data when DELTS is received while terminating the call. Additionally, an invalid entry is added to the voice call quality table.This is a CLI issue and does not impact functionality.
55058	CLI output might not show the Lync clients getting tagged with the high priority ToS value. This is a CLI display issue and doesn't affect the functionality. It has been seen with Lync clients taking part in conference calls. This issue does not occur with peer-to-peer calls.

WebUI

Table 17 *WebUI Known Issues and Limitations*

Bug ID	Description
61674	You cannot create an AP provisioning profile for RAP 4G-LTE using the WebUI. As a workaround, provision the profile using the CLI.
55040	On the WebUI, the U600 modem in the 4G option is missing from the **Wireless > AP Installation > Provisioning Profile,** preventing you from creating a provisioning profile for the U600 in 4G. Perform one of the following as a workaround: • Create a provisioning profile with 4G parameters (i.e., usb_type = "beeceem-wimax") from the command line and apply that profile to the ap-group. • Choose the correct device type in the USB settings of the AP Installation page through the WebUI

Chapter 5

Upgrade Procedures

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

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

Topics in this chapter include:

All versions assume that you have upgraded to the most recent version as posted on the Aruba download site. For instance, 6.0.x assumes you have upgraded to the most recent version of 6.0.

Important Points to Remember and Best Practices

To optimize your upgrade procedure, take the actions listed below to ensure your upgrade is successful. You should create a permanent list of this information for future use.

- Upgrade during a maintenance window. This will limit the troubleshooting variables.
- Know your topology. The most important path is the connectivity between your APs and their controllers. Connectivity issues will interfere with a successful upgrade. You must have the ability to test and make connectivity changes (routing, switching, DHCP, authentication) to ensure your traffic path is functioning.
- Avoid combining a software upgrade with other upgrades; this will limit your troubleshooting variables.
- Avoid making configuration changes during your upgrade.
- Notify your community, well in advance, of your intention to upgrade.
- List which method each AP uses to discover each controller (DNS, DHCP Option, broadcast), and verify that those methods are operating as expected.
- Verify which services you are using for each controller (for example, Employee Wireless, Guest Access, Remote AP, Wireless Voice).
- Verify the exact number of access points (APs) you have assigned to each controller.
- Verify that all of your controllers in a master-local relationship are running the same software version. The same software version assures consistent behavior in a multi-controller environment.
- Verify your current ArubaOS version. In the WebUI, navigate to **Maintenance > Image Management**.
- Use FTP to upload software images to the controller. FTP is much faster then TFTP and also offers more resilience over slower links.

- Resolve any existing issues (consistent or intermittent) before you upgrade.

If you must use TFTP, ensure that your TFTP servers can send more than 30 MB of data.

- Always upgrade the non-boot partition first. If something happens during 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.

Managing Flash Memory

All Aruba controllers store critical configuration data on an onboard compact flash memory module. To maintain the reliability of your WLAN network, Aruba recommends the following compact flash memory best practices:

- Make sure you have at least 85 MB of free compact flash space (**show storage** command).
- Remove all unnecessary saved files from flash by navigating to **Maintenance > Delete Files**.
- Do not exceed the size of the flash file system. For example, loading multiple large building JPEGs for RF Plan can consume flash space quickly.

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 rebooting.

To verify that you have the requisite amount of free memory:

- Using the CLI, confirm (show memory) that there is at least 85 MB of free memory available. Do not proceed unless this much free memory is available. To recover memory, reboot the controller. After the controller comes up upgrade immediately.
- If one of the above conditions are not true, you must delete files from the file system before attempting a local file upgrade. Run the dir command to list all files (or use WebUI > Maintenance > Files). Delete all unnecessary files including crash files and logs.tar file. To ensure that all temporary (crash) files are removed, perform a tar crash and then remove the crash.tar 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 facility. 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
- Customer captive portal pages
- Customer x.509 certificates

Backup 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. Navigate to the **Maintenance > File > Backup Flash** page.
2. Click **Create Backup** to back up the contents of the Compact Flash file system to the file flashbackup.tar.gz.
3. 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 by navigating to the **Maintenance > File > Copy Files** page.
4. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page. Click **Restore**.

Backup 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. Use the **backup** command to back up the contents of the Compact Flash file system to the file flashbackup.tar.gz:

   ```
   (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.
   ```
2. Use the **copy** command to transfer the backup flash file to an external server:

   ```
   (host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword>
   <remote directory>
   ```

   You can later transfer the backup flash file from the external server to the Compact Flash file system with the copy command:

   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   ```
3. 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 44.

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 6.1.3.2:

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 6.1.x

Caveats

Before upgrading to ArubaOS 6.1 take note of these known upgrade caveats.

- CPSEC is disabled when you upgrade from 3.4.x to 6.0.1(CPSEC is disabled in 6.0.1) and then to 6.1.
- If you want to downgrade to a prior version, and your current ArubaOS 6.1 configuration has control plane security enabled, disable control plane security before you downgrade.

  For more information on configuring control plane security and auto-certificate provisioning, refer to the *ArubaOS 6.1 User Guide*.

Load New Licenses

Before you upgrade to ArubaOS 6.1, assess your software license requirements and load any new or expanded licenses you require prior to upgrading to ArubaOS 6.1.

For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the user guide.

Save your Configuration

Before upgrading, save your configuration and back up your controllers data files (see "Managing Flash Memory" on page 44). Saving your configuration saves the **admin** and **enable** passwords in the proper format.

Saving the Configuration in the WebUI

1. Click on the **Configuration** tab.
2. Click the **Save Configuration** button at the top of the screen.

Saving the Configuration in the CLI

Enter the following command in enable or config mode:

```
(host) #write memory
```

Install ArubaOS 6.1.3.2 using the WebUI

ArubaOS 6.x is supported only on the newer MIPS controllers (M3, 3000 series and 600 series).
Legacy PPC controllers (200, 800, 2400, SC-I and SC-II) are *not* supported.
DO NOT upgrade to 6.x if your deployments contain a mix of MIPS and PPC controllers 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 45.)

When upgrading the controller, the following is required:
- Using the CLI, confirm (**`show memory`**) that there is at least 75 MB of free memory available. Do not proceed unless this much free memory is available. To recover memory, reboot the controller. After the controller comes up upgrade immediately.
- Confirm (**`show storage`**) that there is at least 75 MB of /flash available.
-If one of the above conditions are not true, you must delete files from the file system before attempting a local file upgrade. Run the dir command to list all files (or use **WebUI > Maintenance > Files**). Delete all unnecessary files including crash files and logs.tar file. To ensure that all temporary (crash) files are removed, perform a tar crash and then remove the crash.tar file from the controller.

The following steps describe how to 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. If you are running an ArubaOS 3.x.x.x version earlier than ArubaOS 3.4.4.1, you must download the latest version of ArubaOS 3.4.4.x. Then proceed to Step 4.
2. If you are running:
   a. Any ArubaOS RN-3.x.x version, or
   b. ArubaOS 5.0.x.x version earlier than ArubaOS 5.0.3.1, you must download the latest version of ArubaOS 5.0.4.x. Then proceed to Step 4
3. If you are running ArubaOS versions 6.0.0.0 or 6.0.0.1, you must download the latest version of ArubaOS 6.0.1.x.
4. Download ArubaOS 6.1.3.2 from the customer support site.
5. Upload the new software image(s) to a PC or workstation on your network.
6. Log in to the WebUI from the PC or workstation.
7. Navigate to the **Maintenance>Controller>Image Management** page. Select the **Upload Local File** option, then click **Browse** to navigate to the image file (saved in Step 1 - 4) on your PC or workstation.

   OPTION 1: If upgrading from an ArubaOS 3.x.x.x version earlier than 3.4.4.1:

   a. Select the 3.4.4.x image file downloaded in Step 1.
   b. Follow the procedure in Steps 8 - 12.

   OR

   OPTION 2: If upgrading from any ArubaOS RN-3.x.x version or an ArubaOS 5.0.x.x earlier than 5.0.3.1:

   a. Select the 5.0.4.x image file downloaded in Step 2.
   b. Follow the procedure in Steps 8 - 12.

   OR

   OPTION 3: If upgrading from ArubaOS versions 6.0.0.0 or 6.0.0.1:

   a. Select the 6.0.1.x image file downloaded in Step 3.
   b. Follow the procedure in Steps 8 - 12.

   OR

   OPTION 4: If upgrading from any of the following ArubaOS versions:

   - 3.4.4.1 or the latest 3.4.x.x
   - 5.0.3.1 or the latest 5.0.x.x—Review "Upgrading With RAP-5s and RAP-5WNs" on page 48 before proceeding further
   - 6.0.1.0 or the latest 6.0.x.x
   - 6.1.2.0 or the latest 6.1.2.x

a. Select the ArubaOS 6.1.3.2 image file downloaded in Step 4.

a. Follow the procedure in Steps 8 - 12.

8. Make sure you select the non-boot **partition to upgrade**. To see the current boot and non-boot partitions, navigate to the **Maintenance>Controller>Boot Parameters** page.
9. Select **Yes** for **Reboot Controller After Upgrade**.
10. Click **Upgrade**.
11. When the software image is uploaded to the controller, a popup appears. Click **OK** in the popup window. 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, including country code. The **Country** field displays the country code configured on the controller.


NOTE

If the ArubaOS version on the Controller Summary page shows 6.1.3.2, the upgrade is completed. Proceed with Step 13 to verify that all the APs are up and active and that clients are able to connect to the APs and can access resources successfully.

13. Login into the WebUI to verify all your controllers are up after the reboot.
14. Navigate to **Monitoring > Network Summary** to determine if your APs are up and ready to accept clients.
15. Verify that the number of access points and clients are what you would expected.
16. Test a different type of client for each access method that you use and in different locations when possible.
17. 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 44 for information on creating a backup.
18. Repeat steps 7 (option 4) through 20 to if you require an upgrade hop to complete the upgrade to ArubaOS 6.1.3.2.

Upgrading With RAP-5s and RAP-5WNs

If you have completed the first upgrade hop to the latest ArubaOS 5.0.4.0 version, and your WLAN includes RAP-5/RAP-5WN, do not proceed until completing the following process. Once complete, proceed to step 18 on page 48.

1. Check the provisioning image version on your RAP-5/RAP-5WN Access Points by executing the following command:

```
show ap image version
```

2. If the Flash (Provisioning/Backup) Image Version String shows the letters "rn" for example as 3.3.2.11-rn-3.0, note down those AP names and IP addresses.
3. For each of the RAP-5/RAP-5WN 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 will reboot to complete the provisioning image upgrade.

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

```
show ap image version
```

The Flash (Provisioning/Backup) Image Version String should now show for example 5.0.3.3 and not contain the letters "rn".

5. 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 will not be able to connect to the controller running 6.1.2.x and upgrade its production software image.

Install ArubaOS 6.1.3.2 using the CLI

When upgrading the controller, the following is required:
- Confirm (**`show memory`**) that there is at least 60 MB of free memory available. Do not proceed unless this much free memory is available. To recover memory, reboot the controller. After the controller comes up upgrade immediately.
- Confirm (**`show storage`**) that there is at least 85 MB of /flash available.
- If one of the above conditions are not true, you must delete files from the file system before attempting a local file upgrade. Run the dir command to list all files (or use WebUI>Maintenance>Files). Delete all unnecessary files including crash files and logs.tar file. To ensure that all temporary (crash) files are removed, perform a tar crash and then remove the crash.tar file from the controller.

Follow these steps to upgrade a controller to ArubaOS version 6.1 using the CLI.

1. There are 4 upgrade paths to ArubaOS 6.1.3.2. Depending on the current ArubaOS version running on the Aruba controller(s), you will have to perform an upgrade hop as explained in options 1 to 4.

Option 1: If upgrading from an ArubaOS 3.x.x.x version earlier than 3.4.4.1:

a. Download the latest version of ArubaOS 3.4.4.x

b. Upgrade to ArubaOS 3.4.4.x using the CLI upgrade process in the ArubaOS 3.4.4.x Release Notes

OR

Option 2: If upgrading from

- Any ArubaOS RN-3.x.x version, or
- ArubaOS 5.0.x.x version earlier than 5.0.3.1,

a. Download the latest version of ArubaOS 5.0.4.x

b. Upgrade to ArubaOS 5.0.4.x using the CLI upgrade process in the ArubaOS 5.0.4.x Release Notes

Review "Upgrading With RAP-5s and RAP-5WNs" on page 48 before proceeding to upgrade to ArubaOS 6.1.3.2

OR

Option 3: If upgrading from ArubaOS versions 6.0.0.0 or 6.0.0.1:

a. Download the latest ArubaOS 6.0.1.x version

b. Upgrade to ArubaOS 6.0.1.x using the CLI upgrade process in the ArubaOS 6.0.1.x Release Notes

c. Follow the procedure in Steps 8 - 12.

OR

Option 4: If upgrading from any of the following ArubaOS versions

- 3.4.4.1 or the latest 3.4.x.x
- 5.0.3.1 or the latest 5.0.x.x —Review "Upgrading With RAP-5s and RAP-5WNs" on page 48 before proceeding further
- 6.0.1.0 or the latest 6.0.1.x
- 6.1.2.0 or the latest 6.1.2.1

Proceed with step 2

2. Download ArubaOS 6.1.3.2 from the customer support site.
3. From a laptop/desktop, execute the **ping -t** command to verify all your controllers are up after the reboot following the first upgrade hop in Step 1.
4. Open a Secure Shell session (SSH) on your Master (and Local) Controller(s).
5. Execute the **show ap database** command to determine the state of all your APs.
6. Execute the **show ap active** command to view the already up and running APs ready to accept clients.
7. Cycle between step 5 and step 6 until a sufficient amount of APs are confirmed to be up and running. The **show ap database** command displays all of the APs, up or down. If some access points are down, execute the **show datapath session table <access point ip address>** command and verify traffic is passing. If not, attempt to ping them. If they still do not respond, execute a **show ap database long** command to view the wired mac address of the AP; locate it in your infrastructure.
8. Verify that the number of access points and clients are what you would expect.
9. Test a different type of client for each access method (802.1x, VPN, Remote AP, Captive Portal, Voice) and in different locations when possible.
10. 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 44 for information on creating a backup.
11. Use the following command to check the current running ArubaOS version:

```
(hostname)# show version
Aruba Operating System Software.
ArubaOS (MODEL: 3200-US), Version 6.1.0.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2011, Aruba Networks, Inc.
Compiled on 2011-03-09 at 09:11:59 PDT 6.1.0.0 (Digitally Signed - Production Build)

ROM: System Bootstrap, Version CPBoot 1.0.0.0 (build 21294)
Built: 2009-05-11 16:02:29
Built by: p4build@re_client_21294

Switch uptime is 46 days 9 hours 57 minutes 10 seconds
Reboot Cause: User reboot.
Supervisor Card
Processor XLS 204 (revision A1) with 907M bytes of memory.
32K bytes of non-volatile configuration memory.
256M bytes of Supervisor Card System flash (model=NAND 256MB)
```

12. Execute the **ping** command to verify the network connection from the target controller to the FTP/TFTP server:

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

or

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

13. Make sure you load the new software image onto the non-boot partition. The active boot partition is marked as "Default boot."
14. Use the following command to check the ArubaOS images loaded on the controller's flash partitions:

```
(hostname) #show image version
---------------------------------
Partition               : 0:0 (/dev/mtdblock9) **Default boot**
Software Version        : ArubaOS 5.0.3.3
Build number            : 28008
```

```
Label                  : 28008
Built on               : Thu Apr 21 12:09:15 PDT 2011
----------------------------------
Partition              : 0:1 (/dev/mtdblock10)
Software Version       : ArubaOS 5.0.3.0
Build number           : 26207
Label                  : 26207
Built on               : Tue Nov 30 08:35:45 PST 2010
```

15. Use the **copy** command to load the new image onto the controller:

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

or

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

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

```
(hostname)# show image version
----------------------------------
Partition              : 0:0 (/dev/mtdblock9)
Software Version       : ArubaOS 5.0.3.3
Build number           : 28008
Label                  : 28008
Built on               : Thu Apr 21 12:09:15 PDT 2011
----------------------------------
Partition              : 0:1 (/dev/mtdblock10) **Default boot**
Software Version       : ArubaOS 6.1.3.2
Build number           : 29381
Label                  : 29381
Built on               : Fri Jul 23 00:03:14 PDT 2011
```

17. Reboot the controller:

```
(hostname)# reload
```

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

```
(hostname)# show version
Aruba Operating System Software.
ArubaOS (MODEL: 3200-US), Version 6.1.0.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2011, Aruba Networks, Inc.
Compiled on 2011-03-09 at 09:11:59 PDT 6.1.0.0 (Digitally Signed - Production Build)

ROM: System Bootstrap, Version CPBoot 1.0.0.0 (build 23274)
Built: 2010-01-19 11:11:41
Built by: p4build@re_client_23274

Switch uptime is 4 minutes 24 seconds
Reboot Cause: User reboot.
Supervisor Card
Processor XLS 204 (revision A1) with 890M bytes of memory.
32K bytes of non-volatile configuration memory.
256M bytes of Supervisor Card System flash (model=NAND 256MB)
```

19. Repeat Steps 5 through 10 to verify the WLAN is up and running.

Downgrading

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

If you upgraded from 3.3.x to 5.0, the upgrade script encrypts the internal database. Any new entries that were created in ArubaOS 6.1.3.2 will be lost after downgrade (this warning does not apply to upgrades from 3.4.x to 6.1).

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

1. Verify that Control Plane Security (CPSec) is disabled.
2. Set the controller to boot with the previously-saved pre-6.1 configuration file.

If you do not use a previously-saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from 6.1.3.2 to 5.0.3.2, due to changes made to WIPS in 6.x, the new predefined IDS profile assigned to an AP group will not be recognized by the older version of ArubaOS. This unrecognized profile will prevent associated APs from coming and display 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, use the `show profile-errors` and `show ap-group commands` to view the IDS profile associated with AP Group.

3. 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 that will be used on the next controller reload. An error message displays if a system boot parameters are set for incompatible image and configuration files.

After downgrading the software on the controller:

- Restore pre-6.1 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.1.3.2 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 6.1.3.2, the changes will not appear in RF Plan in the downgraded ArubaOS version.
- If you installed any certificates while running ArubaOS 6.1.3.2, you need to reinstall the certificates in the downgraded ArubaOS version.

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

Be sure to back up your controller before reverting the OS.

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.

Downgrading using the WebUI

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

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.

   In the following example, partition 0, the backup system partition, contains the backup release 5.0.3.3. Partition 1, the default boot partition, contains the ArubaOS 6.1.3.2 image:

   ```
   #show image version
   ---------------------------------
   Partition               : 0:0 (/dev/hda1)
   Software Version        : ArubaOS 5.0.3.3 (Digitally Signed - Production Build)
   Build number            : 20219
   Built on                : 2010-12-11 20:51:46 PST
   ---------------------------------
   Partition               : 0:1 (/dev/hda2) **Default boot**
   Software Version        : ArubaOS 6.1.2.0 (Digitally Signed - Production Build)
   Build number            : 28864
   Built on                : 2011-06-22 2:11:59 PST 2011
   ```

NOTE

You cannot load a new image into the active system partition (the default boot).

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, please 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 controller logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
3. 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 from the controller.
4. 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.
   - a brand new installation.
5. 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.
6. 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.
8. If the problem is reproducible, list the exact steps taken to recreate the problem.
9. Provide any wired or wireless sniffer traces taken during the time of the problem.
10. 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.
11. Provide the controller site access information, if possible.