ArubaOS 6.1.3.6

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

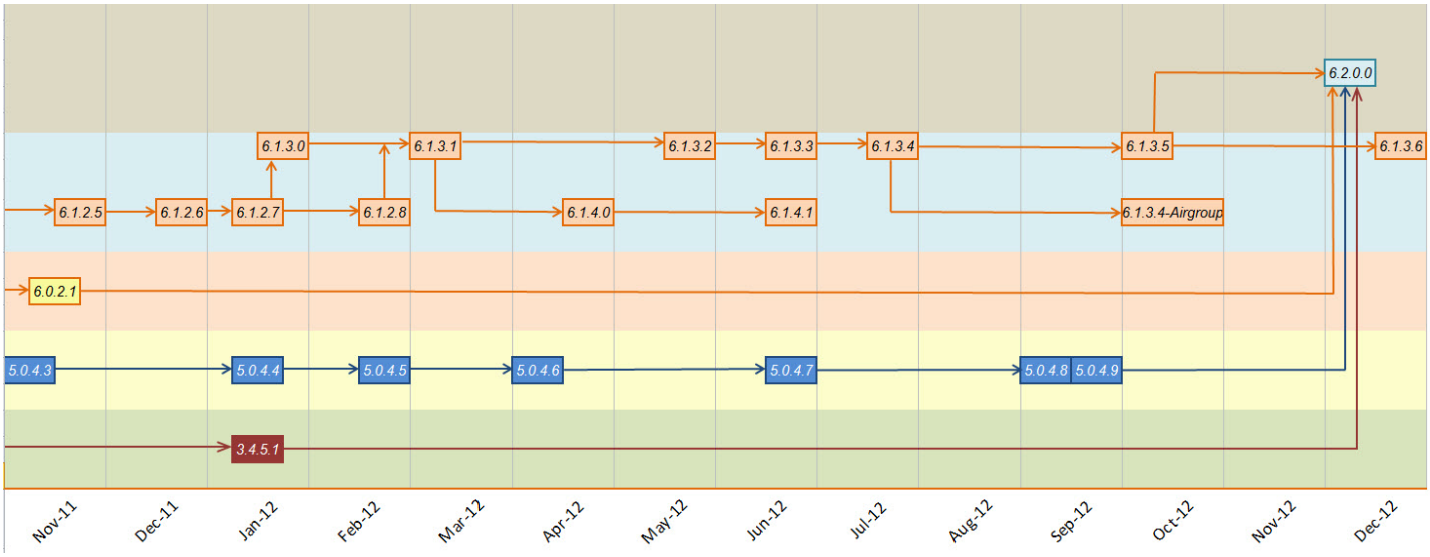
ArubaOS 6.1.3.6 is a general availability patch release that introduces fixes to many previously outstanding issues. All critical and minor security and stability fixes will be applied to subsequent patches of this general availability release until the ArubaOS 6.1.3.x branch merges into a future major GA release. For more information, refer to the End-of-Life policy at http://www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/.

To upgrade to ArubaOS 6.1.3.6, follow the procedures described in "Upgrade Procedures" on page 57.

Release Mapping

The following illustration shows the patches and maintenance releases included in ArubaOS 6.1.3.6.

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

Resolved Issues in ArubaOS 6.1.3.6

The following issues were resolved in ArubaOS 6.1.3.6.

Air Management

Table 4 *Air Management Fixed*

Bug ID	Description
67823	**Symptom:** A large number of BlockACK false positives appeared with the destination MAC address FF::FF::FF::FF::FF::FF. An improved AP channel scanning mechanism prevents this. **Scenario:** This issue was found on a controller with BlockACK detection enabled. The BlockACK detection is enabled on controllers by default to detect attacks when a data frame is received outside the range of expected sequence numbers maintained in APs that detect ADDBA frames. Therefore, when a new ADDBA frame was not detected or if the AP did not detect data frames in its expected range, a BlockACK false positive was triggered.

AP Regulatory

Table 5 *AP Regulatory Fixed*

Bug ID	Description
72390	**Symptom:** AP-175 access points would not come up in AP-mode in the Turkey domain. Support for the Turkey domain on AP-175 APs is included in ArubaOS 6.1.3.6. **Scenario:** This issue was identified on an AP-175 running ArubaOS 6.1.2.7.
73076	**Symptom:** When the RF 802.11g profile was set to channel 13 in European countries, the controller displayed the error message **Invalid channel for 802.11G**. **Scenario:** This issue occurred because support for the 8-12 and 9-13 High Throughput (HT) 40MHz channels for all European countries was not available. Due to this issue, the channel pairs 8-12 and 9-13 were not available in the regulatory domain profile for Germany and APs were not initialized in AP mode in the Turkey domain.This issue was found in 3600 controllers running ArubaOS 6.1.3.4 and later.

AP Wireless

Table 6 *AP Wireless Fixed*

Bug ID	Description
57624	**Symptom:** An AP-105 sometimes used excessive transmit power on the first transmit packet after the device reset. This issue prevented an AP-105 connected to a Cisco POE switch from getting power. This issue was resolved by a software change that defers transmission power or channel changes if any frames are pending. **Scenario:** This issue occurred on APs that aggressively scan outside home channels.

Table 6 *AP Wireless Fixed (Continued)*

Bug ID	Description
65984	**Symptom:** Random AP rebootstrapping was observed along with poor WLAN performance and a ping issue. This issue is resolved in ArubaOS 6.1.3.6. **Scenario:** When a controller configured as default gateway in Layer-2 network responded to a large number of ARP requests, AP rebootstrapping due to high CPU utilization was observed. This issue occurred on controllers running ArubaOS 6.1.3.1 or earlier.
68347	**Symptom:** Clients were unable to send packets on a virtual AP (VAP) that derived more than 32 unique VLANs. The maximum number of supported VLANs per VAP is raised from 32 to 64. **Scenario:** This issue was not limited to any specific controller model. Clients were unable to send any packets on a VAP that had more than 32 unique VLANs. The higher limit resolves this issue.
69034	**Symptom:** A TCP connection between a Panasonic tablet device and an Aruba 802.11n AP timed out frequently in the middle of data transmission. This issue is resolved in ArubaOS 6.1.3.6. **Scenario:** This issue occurred when the tablet device frequently went into power-save mode during data transmission.
72382	**Symptom:** Ping loss (~5%) was observed in clients (laptops) with Intel pre-15.1 chip sets, causing poor voice quality in the voice application running on laptops. This issue is resolved in ArubaOS 6.1.3.6. **Scenario:** This issue occurred on 801.11n APs running on ArubaOS 6.1.3.2.
73874	**Symptom:** An AP-105 frequently stopped sending beacons for up to 1.8 seconds. This issue was resolved in ArubaOS 6.1.3.6. **Scenario:** This issue occurred when four or more clients associated with the AP-105 sent uplink traffic on a DFS channel.

Authentication

Table 7 *Authentication Fixed*

Bug ID	Description
61935, 66647, 67620, 50192	**Symptom:** A user did not derive a VLAN from a user derived rule based on DHCP fingerprinting due to errors in the internal key exchange process. This issue is resolved. **Scenario:** This issue occurred in controllers running ArubaOS 6.1 or later when the SSID used 802.1X authentication.
68412, 74269	**Symptom:** A controller incorrectly used MSCHAPv2 instead of Password Authentication Protocol (PAP) during management authentication. Changes in the internal management authentication process fixed this issue. **Scenario:** This issue occurred when a controller running ArubaOS 6.1.3.0 or later rebooted.
72449	**Symptom:** The AAA RADIUS attributes in the default configuration file were corrupted. This issue is resolved in ArubaOS 6.1.3.6. **Scenario:** When custom RADIUS attributes were added and deleted multiple times with a different attribute ID or vendor ID, incorrect attributes were seen in the configuration file. This issue was not limited to any specific controller model.
72587, 55202	**Symptom:** When a client using MAC authentication roamed, it was incorrectly assigned the default VLAN instead of a MAC authentication derived VLAN. The fix for this issue properly updates the MAC-authentication VLAN so it does not get overwritten. **Scenario:** This issue occurred when MAC authentication was configured to derive a VLAN from a server followed by 802.1X authentication.

Table 7 *Authentication Fixed (Continued)*

Bug ID	Description
74831	**Symptom:** A token and authentication failure issue was observed for some clients that connected in EAP-GTC mode.This issue was fixed by sending EAP-Failure message along with the extended EAP-Failure message to the clients. **Scenario:** When RSA Token server sent a failure message, the controller forwarded the extended EAP-Failure message to the client. A client application was unable to process the extended EAP-Failure message as it was expecting an EAP-Failure message. This issue was observed on controllers running ArubaOS 6.1 or later.

Base OS Security

Table 8 *Base OS Security Fixed*

Bug ID	Description
50189	**Symptom**: User Derivation Rule (UDR) DHCP rules such as DHCP-Option-55 and DHCP-Option-12 rules did not match the DHCP-Option 77 rule configured for client, to place the user in the DHCP derived role. The client is now configured to use the DHCP options supported by UDR and the DHCP rules now match to place the user in the DHCP derived role. **Scenario:** This issue occurred in ArubaOS 6.0.1.0 when the client was configured to use the DHCP options supported by UDR, and the DHCP-Option 77 was not available in the UDR of the AAA profile. The DHCP rules now match and place the user in the DHCP derived role.
70307	**Symptom:** A wired client behind a Layer-3 router could bypass the authentication process on successive connection attempts. This issue was fixed by a change that ensures that these wired clients must reauthenticate to reconnect back to the network after they have aged out. **Scenario:** This issue occurred when multiple wired clients were behind a Layer-3 router. All the wired clients appeared to the controller to have the same MAC address. As a result, after one wired client timed out, a second wired client bypassed the authentication and took over the role associated with the first, aged-out wired client.
72987	**Symptom:** Low memory on the controller resulted in the error message **Failed to add wireless station** appearing in the error log. Memory improvements in ArubaOS 6.1.3.6 resolved this issue. **Scenario:** This issue appeared in a 3200 controller running ArubaOS 6.1.3.3 in a master-local topology.
73454	**Symptom:** The internal controller module that manages authorization temporarily stopped responding, which impacted client authentication on the network. This issue was resolved with a change that ensures that when a Virtual AP (VAP) is disabled or removed, ACLs that are no longer used are not being referenced. **Scenario:** This issue occurred when a network administrator issued the **write mem** CLI command on controllers running ArubaOS 6.1.3.2 and earlier, and configured with ap-group ACLs.
73751	**Symptom:** An Internal controller module stopped responding, affecting the ability of management users on the controller to authenticate using a RADIUS server. This issue was caused by internal management user data that did not get properly deleted from the data tree, and was fixed in ArubaOS 6.1.3.6. **Scenario:** This issue was identified on controllers in a master-standby topology, and occurred when a user configured authentication settings on the master controller, and issued the **write mem** command to save the configuration changes.
74353	**Symptom:** The Universal Database (UDB) module failed on master controller, causing that controller to temporarily lose connectivity to the local controllers. Changes in memory allocation fixed this issue. **Scenario:** This issue occurred on master controller running ArubaOS 6.1.3.4 with more than 255 local controllers.

Table 8 *Base OS Security Fixed*

Bug ID	Description
74537	**Symptom:** The internal controller model that manages authorization temporarily stopped responding, which impacted client authentication on the network. This issue was resolved with a change to an internal statistics table that now bases the columns of the table on server statistics instead of server names. **Scenario:** This issue was identified in ArubaOS 6.1.3.4, and is not limited to any specific controller model.

DataPath/Platform

Table 9 *DataPath/Platform Fixed*

Bug ID	Description
66798, 69102, 68829	**Symptom:** Users experienced low throughput after enabling a bandwidth contract. This issue was resolved by an increase in the queue size for lower contract rates. **Scenario:** This issue occurred when contract rates less than 1 Mbps were applied to bandwidth contracts on controllers running ArubaOS 6.1.3.0.

Dot1x

Table 10 *Dot1x Fixed*

Bug ID	Description
75545	**Symptom:** If a Change of Authorization (CoA) request was used to assign a role to a client, the PMK cache was not updated with the CoA information. In scenarios such as roaming where the PMK cache is used to bypass full authentication, CoA information was lost. A fix was implemented that ensures that the cache is updated with the correct CoA role. **Scenario:** This issue was not limited to a specific controller model, and was first identified in ArubaOS 6.1.3.5.
74955	**Symptom:** The user authentication process on the controller crashed before it sent the EAP-success frame to the client. **Scenario:** The controller's user authentication process crashed when performing EAP for GSM Subscriber Identity Module (EAP-SIM). This issue was fixed in ArubaOS 6.1.3.6. This issue was found in controllers running ArubaOS 6.1.3.2.

IPsec

Table 11 *IPsec Fixed*

Bug ID	Description
72681	**Symptom:** Remote APs failed to establish an IPsec tunnel with the master controller. This issue was a result of high CPU utilization by the internal controller module that handles IPsec, which caused the process to be busy and fail to respond. Changes to how the controller manages stale entries in an internal hash table has resolved this issue. **Scenario:** This issue occurred on a M3 controller in a master-local topology, where the M3 master controller was running ArubaOS 6.1.3.2.

Mesh

Table 12 *Mesh Fixed*

Bug ID	Description
70498	**Symptom:** On an AP-93H mesh point, ports ENET1-4 did not work unless ENET0 was used as well. ENET1-4 now work correctly before ENET0 becomes active. **Scenario:** This issue occurred on an AP-93H configured as a mesh point in which ENET0 is not connected.

RADIUS

Table 13 *RADIUS Fixed*

Bug ID	Description
74748	**Symptom:** When radius-interim-accounting in the AAA profile was enabled for Captive Portal users, the controller missed sending interim packet updates within the configured interval. This issue is fixed by changing the internal code to send interim packet updates in regular intervals. **Scenario**: This issue was observed in controllers running ArubaOS 6.1.3.5.

Remote Access Point

Table 14 *Remote Access Point Fixed*

Bug ID	Description
75141	**Symptom:** Bridge mode clients did not receive an IP address from the external DHCP server. This issue has been resolved in ArubaOS 6.1.3.6. **Scenario:** This issue occurred due to the restart of an internal AP process (STM module) which causes disruptions to client connectivity and packet forwarding.

Role/VLAN Derivation

Table 15 *Role/VLAN Derivation Fixed*

Bug ID	Description
54640	**Symptom:** A controller did not correctly apply a User Derivation Rule (UDR) to a wired client directly connected to the controller. Changes in DHCP option 77 rule processing have resolved this issue in ArubaOS 6.1.3.6. **Scenario**: This issue occurred when an AAA profile on a 6000 controller was configured with a user derivation rule with DHCP option 77.

Startup Wizard

Table 16 *Startup Wizard Fixed*

Bug ID	Description
70791	**Symptom:** A 6000 controller was not configurable using the WLAN wizard, License wizard or Controller wizard, and displayed the error **can't do: cli** when the wizards were launched. Changes to how port data is stored in buffers has resolved this issue. **Scenario:** This issue only appeared on 6000 controllers with an M3 card below a line card with a 2 Gigabit port.

Station Management

Table 17 *Station Management Fixed*

Bug ID	Description
64452	**Symptom:** The warning message **number of VLANs limit exceeded 32** appeared when 32 VLANs were configured on a Virtual AP (VAP). The controller now recognizes that the limit has been reached but not exceeded, and no longer incorrectly returns this message. **Scenario:** This issue occurred when 32 VLANs are configured per VAP.

Switch-Datapath

Table 18 *Switch Datapath Fixed*

Bug ID	Description
72402	**Symptom:** A Layer-2 GRE tunnel could not be established between two controllers. Improvements to internal tunnel lookups have resolved this issue. **Scenario:** This issue occured on two 620 controllers when the GRE tunnel was set to GRE mode 25944 (0x6558) for transparent ethernet bridging.
72867	**Symptom:** A client using a RADIUS server to complete 802.1X and and captive portal authentication with accounting did not send the correct RADIUS accounting information when that client reconnected after an idle timeout. This issue has been resolved by a change that allows network usage statistics to be carried over from the client's last session to its next session. **Scenario:** This issue occurred on a 3600 controller running ArubaOS 6.1.3.3
73518	**Symptom:** An M3 controller running ArubaOS 6.1.3.2 experienced a high amount of dropped packets. This issue has been resolved by a change that increases the number of packet descriptors on the ingress port used to receive the frames on the wire. The increase from 127 to 2000 packet descriptors supports a greater amount of traffic bursts on the 10 Gb link. **Scenario:** This issue occurred on an M3 with a connected 10Gb port.

Switch Platform

Table 19 *Switch Platform Fixed*

Bug ID	Description
65690, 76308, 76435, 76477	**Symptom:** Errors in the datapath or control plane modules caused a M3 or 3000 Series controller to unexpectedly reboot. Changes to internal register access resolved this issue in 6.1.3.6. **Scenario:** This issue occurred on M3 or 3000 Series controllers in a master-local topology
73381	**Symptom:** A controller became unresponsive, and required a reboot to recover. **Scenario:** This issue occurred on an M3 local controller running ArubaOS 6.1.3.4, and was triggered by a loop condition in the wired ports on a remote AP. Changes to how the controller manages MAC address delete and clear requests have resolved this issue.

Voice

Table 20 *Voice Fixed*

Bug ID	Description
65978	**Symptom:** The voice quality of a VoIP softphone call was poor. **Scenario:** This issue occurred when a Session Initiation Protocol (SIP) call was initiated with an update instead of an invite, so the call was not placed into the voice queue. This resulted in poor voice quality. This issue was found in controllers running ArubaOS 6.1.3.0.

VPN

Table 21 *VPN Fixed*

Bug ID	Description
72696	**Symptom:** Clients trying to connect to the wireless network using Aruba VIA received the error **1140 failed to establish the connection** on the VIA client software. This issue was resolved by improvements to how ArubaOS sends RADIUS packets. **Scenario:** This issue occurred when a client tried to connect to a network managed by a 3600 controller running ArubaOS 6.1.2.4, while using EAP-TLS authentication with a RADIUS authentication server and VIA 2.1.0.2.

WebUI

Table 22 *WebUI Fixed*

Bug ID	Description
67304	**Symptom:** A user was unable to provision an AP-61 as a RAP from the WebUI of a master controller. Improvements to how the controller handles Fully Qualified Location Name (FQLN) campus names with special characters fixed this issue. **Scenario:** This issue occurred when a user tried to provision an AP-61 as a RAP from the WebUI of a master controller running ArubaOS 6.1.3.0, and included special characters in the FQLN campus name.

Known Issues and Limitations in ArubaOS 6.1.3.6

The following are known issues and limitations found in this release of ArubaOS. Applicable Bug IDs and workarounds are included.

AP Wireless

Table 23 *AP Known Issues*

Bug ID	Description
74811	**Symptom:** A wireless patient monitor which continuously sends multicast traffic to a wired monitor does not work properly. Packets are not received at the AP when multicast traffic from the wireless monitoring system is sent to wired and wireless clients. **Scenario:** This occured on an AP-65 and ArubaOS 6.1.3.4. **Workaround:** None

Table 23 *AP Known Issues*

Bug ID	Description
74984	**Symptom:** Blackberry devices have severe ping losses when connected to a high throughput SSID. **Scenario:** This issue occurs on AP-135 running on ArubaOS 6.1.3.4 when setting the HT-SSID. **Workaround:** None
75599	**Symptom:** When the diversity-spreading-workaround feature is disabled, the signal strength on the AP is reduced based on the position from which the AP is monitored. **Scenario:** This issue occurs on any deployment with an 802.11n AP running on ArubaOS 6.1.3.2 and later. When this diversity-spreading-workaround 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. The diversity-spreading-workaround behavior changes when the default value changes and this feature is turned off. **Workaround:** Enable diversity-spreading-workaround by disabling the **diversity-spreading-workaround** parameter in the HT-radio profile.

Air Management

Table 24 *Air Management Known Issues*

Bug ID	Description
74285	**Symptom:** A **WMS module busy** message appeared when executing the **show run** command on a standby-master controller. **Scenario:** This issue was first identified on a controller running ArubaOS 6.1.2.0 and is not specific to any controller platform. It occurs in a master-local topology, but the trigger is not yet known. **Workaround:** None
74324	**Symptom:** A crash on the internal WMS module has been observed on an M3 controller running ArubaOS 6.1.3.1.When this occurs, no WMS-related CLI commands or the **write mem** CLI command can be executed. **Scenario:** This issue occurs on master controllers running ArubaOS 6.1.3.1 or later, and is possibly caused by an internal process malfunction. **Workaround:** None.

Authentication

Table 25 *Authentication Known Issues*

Bug ID	Description
55867	**Symptom:** The client is placed in the VLAN provided by 802.1X default role, instead of the Vendor Specific Attributes (VSA) VLAN. **Scenario:** This issue is found in controllers where the role-based VLAN derivation is configured for a machine role and 802.1X default role, with a RADIUS server sending the VLAN through the VSA. The client is placed in the VLAN provided by the 802.1X default role, because the VLAN provided by the 802.1x default role overrides the VLAN sent through the VSA.This issue is found in controllers running ArubaOS 6.0.0.0 and later with 802.1X configured and machine authentication enabled. **Workaround:** Remove the VLAN from the 802.1X authenticated role and machine authentication.

Base OS Security

Table 26 *Base OS Security Known Issues*

Bug ID	Description
55419	**Symptom:** An internal ArubaOS process (Certmgr) becomes busy when the OCSP server is unreachable. **Scenario:** The users are unable to authenticate because certmgr is busy queuing the OCSP requests. (All users doing dot1x, IKE, mgmt-auth are affected). This issue is observed on all controllers running ArubaOS 6.1.3.6. **Workaround:** None

73130	**Symptom:** When a client reconnects, the 802.1X role is assigned instead of the defined Aruba External Services Interface (ESI) syslog parser role.
	Scenario: This issue occurs because the 802.1X role is cached and the role assigned by the ESI server is overwritten when the client reconnects.
	Workaround: Delete the cache entry of the client:
	`aaa authentication dot1x key-cache clear [station-mac]`
	or delete user entry before the 802.1X role is triggered again:
	`aaa user delete mac <a:b:c:d:e:f >`

74837	**Symptom:** The controller reboots when the user authentication process fails. **Scenario:** This issue occurs when the Novell eDirectory service sends the `equivalentToMe` and `SecurityEquals` optional parameters to the Aruba controller. This issue is not limited to any specific controller model. **Workaround:** Disable the optional parameters in Novell eDirectory service before sending the response to the Aruba controller.
76233	**Symptom:** In ArubaOS 6.1.3.6, the Access Control List (ACL) limit is reduced by the number of roles defined. **Scenario:** This limitation can occur on a controller running ArubaOS 6.1.3.6. This limitation exists because two ACLs are created for every user role that is added. Of these two ACLs, one is actively used for assigning user roles (stateful ACL) and the other is not used for any operation (stateless ACL). The **show right <role-name>**, **show acl acl-table**, and **show ap global acl-table** commands can be used to identify which ACL is actively being used. **Workaround:** None.
76291	**Symptom:** An internal controller process (resolvewrap) crashes at random interval when a RADIUS authentication server is configured with a host name. **Scenario:** This crash does not have any impact on the ArubaOS operation as the resolvewrap process is used only periodically for resolving the host name configured for the authentication server. If host-name resolution fails due to a crash, then subsequent attempts to resolve the host name are a success. **Workaround:** If this crash is observed continuously use an IP address instead of a host name in the server authentication profile.
74777	**Symptom:** Clients were incorrectly assigned the default gateway IP address. If the validuser ACL on the controller did not contain the gateway IP address, those clients experienced traffic loss and network connectivity issues. **Scenario:** This issue was observed on controllers running ArubaOS 6.1.3.2 and Windows 7 clients. **Workaround:** Add the gateway IP address to the validuser ACL.
75754	**Symptom:** The user table showed that some 802.1X authenticated clients managed by an external XML-API server were using Web authentication, even though there was no captive portal authentication configured for those clients. **Scenario:** This issue occurred on a controller configured with a 802.1X default role with an ACL that sends traffic through the GRE tunnel to a SafeConnect appliance. In this scenario, Layer-3 authentication is managed by the SafeConnect XML API, which updates the user role to a Layer-3 authenticated role. **Workaround:** None

Table 26 *Base OS Security Known Issues (Continued)*

Bug ID	Description
75565	**Symptom:** A wired user is incorrectly assigned the initial user role instead of a user role derived from DHCP fingerprinting. **Scenario:** This issue is found in ArubaOS 6.1.3.4, and is not specific to any controller platform. **Workaround:** Delete the user and verify that the corresponding bridge entry is removed from the datapath before reconnecting the user.

Controller Platform

Table 27 *Controller-Platform Known Issues*

Bug ID	Description
69739	**Symptom:** A controller could not upgrade from ArubaOS 6.1.3.2 to ArubaOS 6.1.3.6, and displayed the error message **Could not determine version number of config file**. **Scenario:** This issue occurs because a configuration file without a configuration version cannot be downloaded into a new controller. **Workaround:** Access the controller command-line interface, issue the command **write memory** and copy the image to the controller once again.
72185	**Symptom:** Campus APs are not coming up when control plane security is enabled. **Scenario:** This issue occurs when the whitelist database is not synchronized between the master and local controllers, and is observed on controllers running ArubaOS 6.1.3.1. **Workaround:** Clear the whitelist database on all local controllers and synchronize the whitelist from the master controller before enabling control plane security.
72485, 72859, 74297, 74857, 75400, 75428	**Symptom:** The M3, 3600 and 6000 controllers reboot unexpectedly due to **User-Pressed Reset** and **Control Plane Kernel Panic** causes. **Scenario:** This issue is found in M3, 3600 and 6000 controllers running ArubaOS 6.1.2.4 or later. The 6000 and M3 controllers reboot stating **User Pressed Reset** as the cause, while the 3600 controllers fail due to a **Control Plane Kernel panic** issue. **Workaround:** None
75463	**Symptom**: An internal controller process fails to respond, preventing CLI access to the controller for 10-15 seconds while the process restarts. **Scenario**: This issue is not limited to any specific controller model. **Workaround**: None, as the process will restart automatically.

Dot1x

Table 28 *Dot1x Known Issues*

Bug ID	Description
50785	**Symptom:** Multicast key rotation is not working with 802.1x clients in bridge mode. **Scenario:** This occurs only with bridge mode clients in a wireless network managed by a controller running ArubaOS 6.0 and later. **Workaround:** Disable multicast key rotation by accessing the CLI in config mode and issuing the command **aaa authentication dot1x default no multicast-keyrotation**, or increase the timer.
71363	**Symptom:** A client configured to use both machine and user authentication cannot authenticate on the network. **Scenario:** This issue was observed on clients using a Dell 1520 wireless with the 1/7/2011 driver in a wireless network managed by a controller running ArubaOS 6.1.3.2. **Workaround:** Configure a client to use machine or user authentication, but not both.

Table 28 *Dot1x Known Issues*

Bug ID	Description
74663	**Symptom:** Clients are not able to reauthenticate after rebooting or logging off the networks. **Scenario:** This issue was observed on a client running Windows 7 with machine authentication, and connected to a Cisco phone. This issue occurred when the eapol-logoff feature that handles EAPOL-LOGOFF messages is enabled in the controller's 802.11X radio profile. **Workaround:** Ensure that the **eapol logoff** setting in the 802.11X radio profile is disabled.

IPv6

Table 29 *IPv6 Known Issues*

Bug ID	Description
47868	**Symptom:** The IPv6 alias cannot be created, because there is no **Name** option for netdestination6. **Scenario:** The **Name** option is currently not available for netdestination6. Due to this limitation, the IPv6 alias cannot be created for DNS Name queries. This issue is found in ArubaOS 6.1.0.0 or later, and is not limited to any specific controller model. **Workaround:** Provide the host or network IP address of the required destination to set the URL.
47882	**Symptom:** Clients in the IPv6 whitelist do not bypass the Captive Portal login and connect to the desired URL. **Scenario:** This issue occurred because the IPv6 netdestination is not supported inside a whitelist. This issue is found in controllers running ArubaOS 6.1.0.0 or later. **Workaround:** None
57059	**Symptom:** The IPv6 routing fails when the maximum number of IPv6 VLAN interfaces are configured in the controller. **Scenario:** When more than 300 IPv6 VLAN interfaces are configured with three global addresses each on an 3600 controller, IPv6 routing fails. Currently the following IPv6 interface addresses are supported: • 600 Series, 3200 controllers: 32 IPv6 VLAN interfaces * 3 IPv6 addresses per interface = 96 IPv6 addresses • 3400, 3600 controllers: 64 IPv6 VLAN interfaces * 3 IPv6 addresses per interface = 192 IPv6 addresses • M3 controllers: 128 IPv6 VLAN interfaces * 3 IPv6 addresses per interface = 384 IPv6 addresses This issue is in ArubaOS 6.1.3.6 or earlier, and is not limited to any specific controller model. **Workaround:** Reduce the number of IPv6 VLAN interfaces to the supported limit.
74367	**Symptom**: Clients using temporary IPv6 addresses are not be able to communicate as traffic is getting dropped. **Scenario**: A client can support up to four IPv6 addresses. The usage of temporary IPv6 addresses on the clients generates additional IPv6 addresses and sends traffic using all these IPv6 addresses, which exceeds the limitation of four IPv6 entries for the client in the user-table. The issue occurs on the controllers that support IPv6 clients. **Workaround**: • Delete unused IPv6 addresses from the user-table with the command `aaa ipv6 user delete <ip address>`. • Increase the time that a client keeps the temporary IPv6 address before changing to a new address. • Avoid the usage of temporary IPv6 addresses.

Local Database

Table 30 *Local Database Known Issues*

Bug ID	Description
75662, 75659	**Symptom:** An incomplete or incorrect upgrade procedure occurs when an 3600 controller crashes after upgrading. **Scenario:** This issue occurs on controllers upgrading from ArubaOS 6.1.2.2 to ArubaOS 6.1.3.5. **Workaround:** None
75701	**Symptom:** An incomplete or incorrect upgrade procedure occurs. The internal controller process (UDB Server module) fails after upgrading from ArubaOS 6.1.2.3 to ArubaOS 6.1.3.4. **Scenario:** This issue occurs on M3 controllers upgrading from ArubaOS 6.1.2.3 to ArubaOS 6.1.3.4. **Workaround:** None

Management Auth

Table 31 *Management Auth Known Issues*

Bug ID	Description
74274	**Symptom:** A user was not deleted from a user table after the user was idle for a period that exceeded the AAA user idle timeout. **Scenario:** This issue was observed on a local controller in a master-local topology with multiple local controllers, and may be associated with an idle timeout value that is out-of-sync between the datapath and the controller's authentication settings. Workaround: None
75665	**Symptom:** A 3rd generation iPad running iOS 6.0.1 is incorrectly assigned to the default VLAN. **Scenario:** This issue occurs in ArubaOS 6.1.3.5, when a Virtual AP is configured with both MAC authentication and 802.1X authentication, a VLAN derivation rule is configured on the MAC authentication server, and the derived VLAN is different from the VAP's default VLAN. **Workaround:** None

MAC-Based Authentication

Table 32 *MAC-Based Authentication Known Issues*

Bug ID	Description
56130	**Symptom:** A client receives a logon user role instead of a mac-authentication user role when that client roams between a wireless and wired connection to the network. **Scenario:** This issue occurs when a client associates to an AP that is connected to one controller, but terminates on another controller. It was observed in controllers running ArubaOS 6.1.2.0 **Workaround:** None

Master-Redundancy

Table 33 *Master-Redundancy Known Issues*

Bug ID	Description
75367	**Symptom:** Web-server debug logging configured through the l**ogging level debugging system subcat webserver** CLI command does not take effect until the internal httpd process is restarted. **Scenario:** This issue occurs when web-server debug logging mode is enabled, and is not specific to any controller model. **Workaround:** Issue the CLI command **process restart httpd** to manually restart the httpd process.
70343	**Symptom**: Custom captive portal pages are not synced between master and standby when set up to do so. **Scenario**: For any software version, when the standby controller becomes the master, the custom captive portal page no longer shows up during captive portal authentication. The **database synchronize** command only copies database files and RF plan floor plan backgrounds. **Workaround:** None

Mobility

Table 34 *Mobility Known Issues*

Bug ID	Description
63163	**Symptom:** There is an increase in datapath CPU utilization in the controller. **Scenario:** This issue occurs in a Layer-3 IP mobility enabled network, where a wired 802.1X client is connected to an untrusted port and the IP address of the client changes rapidly. The Layer-3 IP mobility edits the bridge table entries for such clients. This results in an increased CPU utilization. This issue is found in controllers running ArubaOS 6.1.3.6 or earlier. **Workaround:** Do not change the IP address of the wired client at a rapid rate.
63164, 63144	**Symptom:** The Layer-3 IP Mobility process fails in the controller. **Scenario:** This issue occurs when a network administrator enables and disables the **router mobile** command, and leads to the incomplete cleanup of client states or controller malfunction. This issue is not limited to any specific controller model or version of ArubaOS. **Workaround:** Reboot the controller when the status of the **router mobile** command changes.

Port-Channel

Table 35 *Port-Channel Known Issues and Limitations*

Bug ID	Description
75044	**Symptom**: After enabling LACP between Aruba 3200XM controllers and Juniper EX4200 switches, some of the ports did not come up. **Scenario**: This issue was observed on a 3200XM controller running ArubaOS 6.1.3.5.

RAP

Table 36 *RAP Known Issues*

Bug ID	Description
51546	**Symptom:** RAP5 drops off from the network randomly. **Scenario:** This is a hardware issue with Sierra 312 USB modem causing the RAP5 to drop off from the network. This issue is observed when Sierra 312 USB modem is used on 3600 controllers running ArubaOS 6.1 or earlier. **Workaround:** Upgrade the firmware of Sierra 312 USB modem from sierrawireless.com, or use a different modem.

Roles/VLAN Derivation

Table 37 *Roles/VLAN Derivation Known Issues*

Bug ID	Description
66261	**Symptom:** When the **Even VLAN** and **Preserve VLAN** features are enabled in the Virtual APs (VAPs) and a client moves from one VAP to another, it is placed in a VLAN of the current VAP instead of the new VAP. **Scenario:** This issue occurs when the client moves from one VAP to another with **Even VLAN** and **Preserve VLAN** features enabled. As the client is placed in the VLAN of the current VAP and if the client VLAN does not exist in the new VAP, the client connection fails. **Workaround:** Check with the Aruba Support team before you enable the **Even VLAN** and **Preserve VLAN** features.

SNMP

Table 38 *SNMP Known Issues*

Bug ID	Description
75570	**Symptom:** An SNMP query from Airwave timed out when the query was directed to the master controller out at peak hours. **Scenario:** This issue occurs on a master controller running ArubaOS 6.1.3.2 or later. **Workaround:** None.

Station Management

Table 39 *Station Management Known Issues*

Bug ID	Description
72194	**Symptom:** When VLAN pooling is used with the assignment type EVEN, the user VLAN changes when the client roams from one AP to another, the IP address remains the same until a release/renew is executed on the client device. **Scenario:** This issue can occur on any controller model with the VLAN mobility and preserve VLAN features enabled. When these features are enabled, the controller's bridge table keeps user entries for 12 hours. This issue occurs when the controller's STM module (an internal process) does not find the entry in the bridge lookup result. **Workaround:** Disable VLAN mobility and preserve VLAN.

VIA

Table 40 *VIA Known Issues*

Bug ID	Description
76377	**Symptom:** When a Windows XP client restarts VIA, VIA returns a message stating that the IPSec process could not be enabled. **Scenario:** This occurs on Windows XP clients running VIA. Clients running other operating systems are not affected. **Workaround:** None.

WebUI

Table 41 *WebUI Known Issues*

Bug ID	Description
66521	**Symptom:** Two **Apply** buttons are displayed in the WebUI when adding users to the internal database. **Scenario:** While creating a new user in the WebUI, two **Apply** buttons appear in the **Configuration > Security > Authentication > Internal DB** page due to incorrect labeling of the buttons. This issue is not limited to a specific controller model. **Workaround:** Use the **Apply** button at the top to add a new user. Use the **Apply** button at the bottom to apply any user list changes.
73170	**Symptom:** Numerous error messages appear in the error log file where internal processes (such as STM and WMS) are not able to get data from the database. **Scenario:** This issue occurs on a M3 master controller after upgrading from ArubaOS 6.1.3.0 to ArubaOS 6.1.3.4. This issue is caused by a MySQL index file that is inconsistent with its data file. This causes the MySQL server to restart continuously thus preventing other processes that are using the database from inserting or modifying database entries. **Workaround:** Contact Aruba Tech Support at http://support.arubanetworks.com/.
74227	**Symptom:** The **Monitoring** tab of the WebUI and the output from the **show ap active** command do not match. The WebUI shows more APs than are actually up and the output of **show ap active** displays the correct number. **Scenario:** This can occur on any controller model acting as a master and running ArubaOS 6.1.3.2 or later if the bootstrap threshold in the ap system profile is set to more than 40 minutes. In this instance, these APs were powered off when the controller attempted to send a configuration update. The APs failed to receive the update, and the controller marked the APs as down but did not update the AP database as well. **Workaround:** None.

WMM

Table 42 *WMM Known Issues*

Bug ID	Description
68503	**Symptom:** The controller chooses incorrect WMM priority (background instead of best-effort) in the downstream traffic. When same DSCP value is mapped to two different access categories, the lower of the two is used for the downstream traffic. **Scenario:** This issue is observed on controllers running ArubaOS 6.1.3.6 or lower in Tunnel and Decrypt-Tunnel modes. **Workaround:** None.

Issues Under Investigation

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

AP

Table 43 *AP Issues Under Investigation*

Bug ID	Description
69424	**Symptom:** An AP-125 crashes after upgrading to ArubaOS 6.1.3.6, but recovers on subsequent reboots, resulting in a longer upgrade cycle.. **Scenario:** This occurs when upgrading to ArubaOS 6.1.3.6 from ArubaOS 6.1.3.2 and later in any deployment with an AP-125. **Workaround:** None
72203	**Symptom:** APs are not coming up and are unable to establish an IPsec tunnel with the controller. This issue is observed on controller running ArubaOS 6.1.3.4.The cause has not been identified.
72618	**Symptom:** An unexpected reboot of an AP-125 terminating on controller running ArubaOS 6.1.3.3 has been observed.
74074	**Symptom:** APs with an **Up** status on a local controller are listed as **Down** in the AP database of the master controller.
75513	**Symptom:** Clients connected to an AP-135 in a network running ArubaOS 6.1.3.4 take more than 30 seconds to complete the 802.1x authentication, while they are roaming in the network.
75373	**Symptom:** AP-135s in a network running ArubaOS 6.1.3.2 and terminated on the 3600 controller crash due to IPSec encryption failures.
75564	**Symptom:** An unexpected reboot of an AP-135 terminating on controller running ArubaOS 6.1.3.3 has been observed.

Authentication

Table 44 *Authentication Observed Issues*

Bug ID	Description
75832	**Symptom:** EAP-TLS authentication fails for the MAC clients connected to a Remote AP in split-tunnel mode. This issue is observed on controller running ArubaOS 6.1.2.6.

Base OS Security

Table 45 *Base OS Security Observed Issues*

Bug ID	Description
67287	**Symptom:** When Layer-3 mobility is enabled and the **auth-sta-roam** option is disabled in a network, the alternate home agent for a client does not work and the client is not able to roam.
73373	**Symptom:** Captive portal authentication for wireless users does not work in some cases as the users are not able to access the Captive Portal login page. The same issue is seen in wired users when they try to access the Web configuration login page.

Table 45 *Base OS Security Observed Issues*

Bug ID	Description
74631	**Symptom:** Wired users in tunnel mode, connected to a RAP-5, show up as wired (remote) users when the forward mode of the wired port is changed from split to tunnel. This issue is seen in ArubaOS 6.1.3.4.
75082	**Symptom:** A controller failed to properly detect or report a MAC/IP spoofing event.
75022	**Symptom:** A standalone 3200 controller running ArubaOS 6.1.3.2 experiences unusually high CPU utilization.

Controller-Datapath

Table 46 *Controller-Datapath Observed Issues*

Bug ID	Description
68211	**Symptom:** An unexpected controller reboot occurs. The cause has not been identified.
72359, 73057, 73246, 73256, 74050, 74575, 75700, 75753, 76731	**Symptom:** An unexpected timeout in an internal datapath process caused a controller to unexpectedly reboot.
73350	**Symptom:** A high number of IPsec encryption failures caused an AP-135 remote AP to reboot.
74942	**Symptom:** Wireless clients experienced degraded network throughput when the user count on a controller reached 2500 users. This issue has also been associated with a high number of buffer allocation failures.
75137	**Symptom:** Wireless clients are unable to communicate with a multicast router using a VLAN that does not have a configured IP address.

Dot1x

Table 47 *Dot1x Observed Issues*

Bug ID	Description
75860	**Symptom:** A 3rd generation iPad cannot roam between APs in bridge mode. This issue is associated with a PMK caching failure in bridge mode.

Mesh

Table 48 *Mesh Observed Issues*

Bug ID	Description
75705	**Symptom:** An AP-175P used as a mesh point fails to connect to an AP-175P mesh portal after an upgrade to ArubaOS 6.1.3.5.

Switch-Platform

Table 49 *Switch Platform Observed Issues*

Bug ID	Description
74778	**Symptom:** A controller upgrading from ArubaOS 6.1.2.6 to ArubaOS 6.1.3.3 loses connectivity and displays the message **Retrieving Configuration...will take approximately 1 minute**.

UI-Monitoring

Table 50 *UI-Monitoring Observed Issues*

Bug ID	Description
73459	**Symptom:** The output of the **show acl hits** CLI command and the firewall hits information on the UI Monitoring page of the controller WebUI shows inconsistent information.

Improved Interference Immunity

The Non-Wi-Fi Interference Immunity feature helps improve performance on a 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**.

Enhancements to cfgm

The following parameter descriptions for the **cfgm** command are changed:

- cfgm set sync-type <complete>
- cfgm set sync-type <snapshot>

The new parameters are as follows:

Table 1 *CLI enhancements*

Parameter	Description	Range	Default
`sync-type complete`	The master sends full configuration file to the local.	—	—
`sync-type snapshot`	The master sends only the incremental configuration to the local. Note: By default, this configuration is enabled.	—	Enable

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`.

CLI Changes

The following changes have been made to the ArubaOS CLI in ArubaOS 6.1.3.2.

Table 2 *CLI Changes in ArubaOS 6.1.3.2*

Command	New Parameter add in 6.1.3.2	Description
`aaa user`	`stats-poll`	Enables user stats polling
`ipv6 firewall`	`ext-hdr-parse-len <100-300>` Default: 100	Threshold in bytes beyond which IPv6 header will not be parsed and the packet will be dropped.
`ap provisioning-profile`	`usb-modeswitch`	All the parameters that is required to be passed to usb_modeswitch utility
`rf dot11a-radio-profile`	`cell-size-reduction`	Reduce cell size by controlling Wi-Fi Rx sensitivity. Use this to manage dense deployments and to increase overall system performance/capacity by minimizing co-channel interference and optimizing channel reuse. 0: default sensitivity. 1 - 55: sensitivity reduction from default (dB).
`show ap debug`	`config-msg-history ap-name`	Provides a history of the last 10 control messages sent to and received between a specific AP and the controller.
`show ap debug`	`config-msg-history ip-addr`	Provides a history of the last 10 control messages sent to and received between a specific AP and the controller.
`show ipc statistics app-name`	`sapm`	Provides visibility into the sapm-related IPC messages to and from the STM module's queues.

Table 2 *CLI Changes in ArubaOS 6.1.3.2*

Command	New Parameter add in 6.1.3.2	Description
`show ipc statistics app-name`	`stm-lopri`	Provides visibility into the Station Management Low Priority-related IPC messages to and from the STM module's queues.
`show ipc`	`forwarding-statistics`	Shows statistics about packets forwarded to internal processes from remote nodes.
`show datapath debug`	`opcode`	Shows datapath opcode statistics.

Chapter 3

Issues Fixed in Previous 6.1.3.x Releases

The following issues have been fixed in the previous ArubaOS 6.1.3.x patch releases.

Fixed in 6.1.3.5

Air Management - IDS

Table 1 *Air Management - IDS Issue Fixed*

Bug ID	Description
69419	An M3 controller with a large number of AP-92 remote APs deployed as hotspots no longer displays incorrect values for the bandwidth usage or users on each associated AP. This issue was identified in ArubaOS 5.0.3.3, where incorrect values written to the `wlsxWlanStationStatsTable` MIB were attributed to personal hotspots on the client devices that used the same MAC address as the client's connection to the Aruba AP.

AP

Table 2 *AP Issues Fixed*

Bug ID	Description
68151	An issue was fixed where corrupted memory caused the AP to reboot with the message "NMI Watchdog interrupt on Core 0x0".
70133, 71208	An issue was fixed where the Cell size reduction (CSR) value setting did not work in the case of an AP-105. High CSR values in dense deployments (APs at short range from each other) were causing throughput issues.
71330	The issue was fixed where, in previous releases, clients that were not associated to the first VAP (Virtual AP) on an AP did not get handed off even with low signal strength and handoff assist enabled.
72382	An issue was fixed where frequent packet (ping) loses were observed in clients (laptops) with Intel 6200/6205/5100 chipsets. This caused bad voice quality when voice application were used on the laptops. This issue was found in the ArubaOS 6.1.3.2 and 802.11n APs.

Authentication

Table 3 *Authentication Issues Fixed*

Bug ID	Description
69840	An issue was fixed where the EAP-TLS authentication failed when new certificates were used by clients to connect to a network.

Table 3 *Authentication Issues Fixed (Continued)*

Bug ID	Description
72112	The AAA 802.1X authentication default timer values have been changed as follows to support Apple iOS devices: • timer idrequest_period - 5 (previously 30) • server server-retry-period - 5 (previously 30) • server server-retry - 3 (previously 2) • max-requests - 5 (previously 5)

Captive Portal

Table 4 *Captive Portal Issue Fixed*

Bug ID	Description
72465	Clients reassociating in a network using an external XML-API server for Layer-3 authentication were presented with incorrect roles. This issue is now fixed.

Configuration

Table 5 *Configuration Issue Fixed*

Bug ID	Description
69321	An issue was fixed where some of the 3600 controllers in a network consisting of 3600 and M3 controllers did not come up after an upgrade from ArubaOS 6.1.2.6 to 6.1.3.3.

Hardware Management

Table 6 *Hardware Management Issue Fixed*

Bug ID	Description
58963	An issue was fixed where adding member ports to the port-channel, blocked the ports, resulting in packet drops. This occurred when the static port-channel was configured and spanning tree was disabled on the controller. This issue was observed in controllers running ArubaOS 6.1.3.2.

Interface

Table 7 *Interface Issue Fixed*

Bug ID	Description
69140	An issue was fixed where the GE 1/0 - 1/3 port on the 650 controller did not link up and transmit packets because of an error in the static configuration of the Full duplex setting. This issue was observed in ArubaOS 3.4.5.0, 5.0.2.1, 5.0.4.7, 6.0.2.1, 6.1.2.5, 6.1.3.1, and 6.1.3.3 with the 650 controller.

IPsec

Table 8 *IPsec Issue Fixed*

Bug ID	Description
71991	A memory issue related to how the controller processes public keys was fixed. In ArubaOS 6.1.1.0, this issue created a memory leak that caused a reset to the controller process that handles IKE exchanges for remote APs, VPNs, and APs using control plane security.

IPv6

Table 9 *IPv6 Issue Fixed*

Bug ID	Description
68037	An issue was fixed where stateless DHCPv6 did not work properly and DHCPv6 packets sent through the VLAN interface were dropped. The issue occurred when the `ipv6 mld snooping` command was enabled on the VLAN interface.

Mesh

Table 10 *Mesh Issue Fixed*

Bug ID	Description
73343	Support for band-3 channels (100 - 140) has been added for AP-60, AP-61, AP-70, and AP-85 for Saudi Arabia.

Mobility

Table 11 *Mobility Issue Fixed*

Bug ID	Description
72258	An issue was fixed where Apple devices running iOS 6 were not able to establish VPN tunnel using their built-in VPN client. This issue was seen in 3200 controller running ArubaOS 6.1.3.3.

M-Switch Software

Table 12 *M-Switch Issue Fixed*

Bug ID	Description
67847	An unexpected reboot observed on an AP-125 due to a databus error was fixed.

Platform/Datapath

Table 13 *Platform/Datapath Issues Fixed*

Bug ID	Description
67178	An issue was fixed where an incorrect tunnel became a part of the VLAN multicast group, resulting in unexpected behavior and wastage of bandwidth in an IPsec tunnel environment. This issue was observed in controllers running ArubaOS 6.1.2.7.
70878	An issue where the status of the NTPD module was busy on controllers running ArubaOS 6.1.2.4, was fixed.

Port-Channel

Table 14 *Port-Channel Issue Fixed*

Bug ID	Description
70840	An issue was fixed where a spanning tree loop occurred between the controller and the catalyst after the controller was rebooted. This issue was seen in controllers running ArubaOS 6.1 when a port-channel was configured and spanning tree was enabled. When adding the member ports to the port-channel, the events generated during the process were not serviced in the expected order leading to the member ports to go into blocked state.

RADIUS

Table 15 *Radius Issue Fixed*

Bug ID	Description
68008	An issue was fixed where a controller running ArubaOS 6.1.x failed to send STOP accounting messages to ClearPass Guest (acting as a RADIUS server) when a large number of users aged out from the WLAN network at the same time. This resulted in multiple stale active sessions on ClearPass Guest. Starting from ArubaOS 6.1.3.6, the controller re-transmits the failed STOP accounting messages to the ClearPass Guest server.

Remote AP

Table 16 *Remote AP Issues Fixed*

Bug ID	Description
71027	An issue was fixed where clients using the split-tunnel forwarding mode were assigned incorrect roles on the RAP following a change in configuration. Clients (iPads) could not log in after the configuration change. This issue was seen in ArubaOS 5.0.4.7 and was attributed to clients' ACL/ role not getting correctly updated to reflect the new configuration in the RAP.
72167	An issue was fixed, where the remote AP always shows the current overlay network as Enhanced High Rate Packet Data (eHRPD) mode instead of displaying its actual network i.e 3G/4G. This is seen in the output of `show ap debug usb ap-name <ap-name>` CLI command field **Current Network Service**. eHRPD is now enhanced to display the actual network -- 3G/4G. This is applicable only when the remote AP is provisioned to use UML290 as an uplink connection.

Security

Table 17 *Security Issues Fixed*

Bug ID	Description
66107, 66330, 71142	An issue was fixed where the Auth module on the local controller crashed when a wired user was configured with more than one IP addresses (probably multiple clients behind a router). This issue occurred when the first IP address created for this user timed out while the rest of them were still reachable. This issue was seen in M3, 3400, 3200, and 6xx running ArubaOS 6.1.3.1.
68304	An issue was fixed where the User Derivation Rules (UDRs) after the 127th rule were not processed when the UDRs were configured using the `conf t aaa derivation-rules user <udr_name>` command.
68315, 73121, 73497	The `show global-user-table list` command now works correctly and displays the list of current users both on the master and the local controllers.
69447	An issue was fixed where the client failed to authenticate with the RSA token server after the controller was upgraded to ArubaOS 6.1.3.1. The issue occurred when EAP-PEAP with EAP-GTC (Generic Token Code) was configured in the AAA Authentication dot1x profile.
70170	An issue was fixed where the ClearPass (CP) users were not able to access the CP login page causing network issues. This issue was seen in 3600 running ArubaOS 6.1.3.2 with AP-93 RAPs. The root cause was identified as the authentication module not responding due to a loop condition.
72627	An issue was fixed where after a successful authentication, clients connected to the guest SSID were shown the "Web Authentication is disabled" error page.
73418	An issue is resolved where a large number of `Dropping EAPOL packet` and `EAP-ID mismatched` entries were seen in the error log. These entries now no longer appear as error messages. This issue occurred when a client roamed from one AP to the another AP without completing authentication at the first AP.
73664	An issue was resolved when wired users connected to a controller acting as a multiplexer client failed to establish a 802.1X authentication upon moving from one port of the controller to another. This issue occurred when a controller was deployed as a multiplexer server (running ArubaOS 6.1.3.2/6.1.3.3/6.1.3.4), and another controller was used as a multiplexer client.

SNMP

Table 18 *SNMP Issue Fixed*

Bug ID	Description
59292, 66990	An issue was fixed where compile errors were sometimes produced when importing an ArubaOS 6.1.3.1 MIB to HP OpenView 9.10 or above. This may have occurred if you were using a newer MIB browser.

Station Management

Table 19 *Station Management Issues Fixed*

Bug ID	Description
65810	An issue was fixed where station management (STM) process crashed in the controller causing APs to rebootstrap and failover to a backup controller. This issue was observed in controllers running ArubaOS 6.1.2.7.

Table 19 *Station Management Issues Fixed (Continued)*

Bug ID	Description
72319, 73672	An issue was fixed where the Station Management module on a 6000 controller running ArubaOS 6.1.3.1 crashed causing the APs to rebootstrap. This issue was seen when frames sent by non-Vocera clients on port 5002 were parsed as Vocera frames causing incorrect memory access, leading to the crash.

WebUI

Table 20 *WebUI Issues Fixed*

Bug ID	Description
69039	An issue was fixed where the arci-cli-helper process that handles WebUI commands crashed in the controller, resulting in a slow WebUI response time. This occurred when there was a failure in authenticating WebUI users. This issue was observed in controllers running ArubaOS 6.1.3.2.
68497, 70106	The **Configuration > Network > Ports > Port-Channel** page of the WebUI now correctly displays the number of **Allowed VLAN IDs**.

Fixed in 6.1.3.4

Access Points

Table 21 *Access Points Issues Fixed in 6.1.3.4*

Bug ID	Description
52183	Uplink VLAN tagging now works with Point-to-Point Protocol over Ethernet (PPPoE) enabled for a Remote AP (RAP).
63909	The frequency band and regulatory maximum EIRP settings for Saudi Arabia have been updated.
66477, 66476	An issue was fixed where APs with the country code CO could use channels 12 and 13, which are not specified for that country code.
67622	AP-68 and AP-68P now support the Egypt (EG) regulatory domain.
68549	AP-92 and AP-93 now support the Bahrain (BH) regulatory domain. However, AP-134 and AP-135 will not support this regulatory domain due to pending regulatory approvals.

Air Management (IDS)

Table 22 *Air Management (IDS) Issue Fixed in 6.1.3.4*

Bug ID	Description
68614	An issue that was causing the controller to inefficiently fetch information from the database was fixed. Prior to this fix the controller functioned properly but the CPU utilization was higher than it should be. This issue was seen on all controllers for ArubaOS 5.0.x to 6.1.3.3. This fix will lower the CPU utilization related to gathering certain types of information from the database.

DHCP

Table 23 *DHCP Issue Fixed in 6.1.3.4*

Bug ID	Description
68613	A controller running ArubaOS 6.1.3.2 configured as a DHCP Relay Agent with IP Helper, requests an IP address using its uplink IP address as the source IP. The DHCP server, however, responds back to the controller's user VLAN IP address. Because of this source IP mismatch, the firewall between the controller and the DHCP server drops the response from the DHCP server. A fix has been introduced that allows the controller to send the user VLAN IP address as the source IP.

Guest Provisioning

Table 24 *Guest Provisioning Issue Fixed in 6.1.3.4*

Bug ID	Description
68796	Management users can now log in to the controller by using the DOMAIN\Username format and view guest users that they have created.

Mobility

Table 25 *Mobility Issues Fixed in 6.1.3.4*

Bug ID	Description
69155	An issue where an Apple iOS/MacOS device sometimes took longer than a minute to get an IP address from the DHCP server after resuming from sleep was fixed. This was observed when IP mobility was enabled on controllers running ArubaOS 6.1.3.0.
73446	The issue where VPN does not work with Apple IOS6 certificate-based authentication was fixed. Apple IOS6 certificate-based authentication could not establish an L2TP/IPSEC connection with the controller and therefore caused VPN to not work. This issue impacted the 600 series, 3200, 3400, 3600 and M3 controller running ArubaOS 6.1.3.4 and earlier.

Other

Table 26 *Other Issue Fixed in 6.1.3.4*

Bug ID	Description
68004	The `phonehome now` command functions as expected if executed after an auto-report is generated. In ArubaOS 6.1.2.8, executing the `phonehome now` command after an auto-report was generated resulted in the following warning message: `*** WARNING ***: PhoneHome service is disabled (phonehome enable) Ignoring any report upload operation.`

Platform/Datapath

Table 27 *Platform/DataPath Issues Fixed in 6.1.3.4*

Bug ID	Description
67966	An issue was fixed where enabling the “VIA SSL Fallback” option caused a datapath crash and controller reboot. This issue was observed in Aruba 3000 Series/6000 series controllers running ArubaOS 6.1.3.0.
69058, 70619	A controller supports up to four IPv6 addresses in a user table entry for a MAC address. A race condition occurred due to the control plane and data plane going out of sync with respect to the maximum number of IPv4/6 addresses for a MAC address in the user table. This race condition resulted in a datapath crash causing the controller to reboot. This issue has now been fixed.
67886	In a master-local topology with more than 255 local controllers, the status of APs displayed incorrectly (down) in the master controller and correctly (up) in local controllers. This issue was fixed and the AP status is now displayed correctly in the master controller.
68069, 68673	An issue where the configuration management process in the controller crashed occasionally during Virtual Router Redundancy Protocol (VRRP) failover and fallback operations was fixed. This issue was found in master controllers running ArubaOS 6.1.3.1 or later from the core file generated due to configuration management process crash.
68088	Controllers running ArubaOS 6.1.3.1 configured with large number of VRRP instances rebooted after executing the `write memory` or the `show running-config` commands. This issue, which occurred due to the large number of VRRP instances, was fixed.
68277	An issue where the `halt` command accidently displayed panic messages in controllers (3000 Series/6000 series) running ArubaOS 6.1.3.2 has now been fixed. The `halt` command now functions as expected and gracefully shuts down the controller.

Port Channel

Table 28 *Port Channel Issue Fixed in 6.1.3.4*

Bug ID	Description
68841	An issue was observed in ArubaOS 6.1.3.2 and 5.0.4.6 where a new VLAN could not be associated to port channel 7 using the WebUI. This issue has now been fixed.

RADIUS

Table 29 *RADIUS Issue Fixed in 6.1.3.4*

Bug ID	Description
67619	An issue is now fixed where the controller running ArubaOS 6.1.3.1 did not send `aruba-user-role` Vendor Specific Attributes (VSA) in response to the accounting request message sent by the RADIUS server. This issue was observed after upgrading the controller from ArubaOS 5.0.4.x to ArubaOS 6.1.3.x.

Remote AP

Table 30 *Remote AP Issues Fixed in 6.1.3.4*

Bug ID	Description
57639, 57637	The log message `rap_stm_user_agent_update_handle` incorrectly appeared in the error logs of a controller with RAPs serving split tunnel and bridge clients. This was fixed so the message correctly shows up in the debug logs and no longer appears in the error logs.
68637	Fixed an issue where AP-134 and AP-135 devices running ArubaOS 6.1.0 or later did not forward source Network Address Translation (NAT) traffic from clients using bridge or split-tunnel forwarding mode to devices connected on the uplink port of the AP.

Security

Table 31 *Security Issues Fixed in 6.1.3.4*

Bug ID	Description
68336	Fixed an issue that caused the authentication process to crash in the controller. This issue was observed when User Derivation Rules (UDR) were configured on the Remote AP and the wired client had more than one IP address.
68652	In a master-standby setup, VRRP configured on untrusted ports between controllers caused the Auth module to crash in the master controller. An Auth module crash can disconnect active users and prevent new users from getting authenticated. This issue was observed in controllers running ArubaOS 6.1.3.2 and has now been fixed.

SNMP

Table 32 *SNMP Issues Fixed in 6.1.3.4*

Bug ID	Description
68423	An issue where a controller did not send the *wlsxAuthServerTimedOut* trap when the authentication (RADIUS) server timed out or was out of service was fixed. This issue was observed in controllers running ArubaOS 6.1.x.

Station Management

Table 33 *Station Management Issues Fixed in 6.1.3.4*

Bug ID	Description
56666, 63279	The output of the `show ap association` or `show ap bss` CLI commands no longer displays entries for clients that are no longer associated to an AP. In previous releases, communication between an AP and a controller might be interrupted by heavy network traffic. In this case, the AP did not notify the controller that a client has left, the controller did not remove the expired user entry.
67544	A controller correctly generates the SNMP trap *wlsxNAccessPointIsUp*.
73194-67737	The issue where clients failed to authenticate with a rejection status of 17 was fixed. This occurred when an AP was brought up with one of the radios disabled and after 50 days of uptime the radio was enabled. Clients were not able to connect due to an error in the management frame throttle detection. The AP rejected the 802.11 authentication with status 17. To avoid this issue, reboot the AP after enabling the radio or set the management frame throttle limit to 0 in the radio profile.

WebUI

Table 34 *WebUI Issues Fixed in 6.1.3.4*

Bug ID	Description
61561	Accessing the WLAN Wizard from the WebUI no longer results in a blank page.
61674	You can now successfully configure 4G-LTE USB modems when provisioning a RAP using the WebUI.
63952, 66355, 68121	The **Edit** button on the **Configuration** > **Management** > **Guest Provisioning** page now allows you to modify existing users.
64427	You can use the WebUI to configure a policy to redirect traffic to an ESI group. This option is now available on controllers with the ESI, PEFNG or VPN licenses. In previous releases, only the ESI license supported this feature.
67027	When creating a new guest user on the **Guest Provisioning** page, the browser no longer freezes after clicking **Create & Print**.
68466	A fix has been made that allows the controller to update the changes made to the year or month in the **Configuration** > **Management** > **Guest Provisioning** page of the WebUI.
69608, 64017	A fix has been made to **Configuration** > **Network** > **Ports** > **Port Channel** tab of the WebUI where the default member VLAN of the controller was not pre-selected from the VLAN list, causing an error in applying the configuration changes. This fix affects controllers running ArubaOS 6.1.3.0.

Fixed in 6.1.3.3

Table 35 *Bugs fixed in 6.1.3.3*

Bug ID	Description
68712	A problem where VIA failed to start because of an expired certificate has been corrected.

Fixed in 6.1.3.2

Table 36 *Bugs Fixed in 6.1.3.2*

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.

Table 36 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
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 was 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.
62978	Ghana (GH) regulatory domain support is available for the AP-120 Series.
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.
64111	Bosnia and Herzegovina (BA) and Macedonia (MK) regulatory domain support is available for the AP-105.
64178	Bosnia and Herzegovina (BA) and Macedonia (MK) regulatory domain support is available for the AP-93H.
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.
64926	An AP process failure that occurred when the AP received a specific type of malformed 802.11 frame was 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.

Table 36 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
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.
65953	Morocco (MA) regulatory domain support is available for the AP-105.
66129	The issue of a AP-135 terminating on a local controller rebooting due to a crash was 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 was 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 such as ACKs were still being sent on multiple chains even when CSD Override was enabled.
66386 66610, 66611	An issue is 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.
67158, 68187	An unexpected reboot on an AP-125 due to a databus error was fixed.
67277	An issue was 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 Control Plane Security enabled, APs no longer become stuck and unable to upgrade. The upgrade now completes successfully.
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.
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.
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) was fixed.

Table 36 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
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.
65415	An issue is 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.
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).
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 is resolved so if a controller sees an ESI server is up, it will retry updating its datapath until it succeeds.
64817	Transceivers are now correctly identified when connected to M3 controllers.
48194	An issue is 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 is 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.
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.
54249	The 4-way dot1x handshake failure on a mesh link when EAPOL frames are sent at higher rates was 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, was fixed. Enabling the ARM/WIPS override in these radio profiles led to problems in the ARP resolution thereby causing mesh point reboots.

Table 36 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
63368	The issue of 802.11n capable mesh points failing with the message *authentication time-out* following their association with the mesh port, was 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 was fixed. The root cause was attributed to an invalid rate computed by the driver which triggered an assertion in the APs.
54015	Wired clients connected to an Layer-2 switch can now successfully push traffic when an untrusted port-channel uplink is used between the Layer-2 switch and a local controller configured to use Layer-3 mobility. Previously the clients would obtain an IP address but fail to push traffic.
56326	An issue that could cause traffic to be temporarily disrupted on controllers using OSPF routing is resolved through improved validation of OSPF Link-State Advertisements (LSAs) in traffic packet headers.
56326	An issue that could cause traffic to be temporarily disrupted on controllers using OSPF routing is resolved through improved validation of OSPF Link-State Advertisements (LSAs) in traffic packet headers.
49325	An issue is 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 is 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 was 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 is 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 was fixed.
62484	A controller reboot that occurred when `write mem` was executed from the CLI or WebUI shortly after a license was added was 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 is resolved where APs rebootstrap due to excessive ARPs in the network. Optimizations have been implemented in the controller to mitigate this.
62818	An issue is 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.

Table 36 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
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 was fixed.
63843	An issue is resolved where APs terminating on M3 local controllers were entering into a GRE tunnel teardown/setup loop when the Layer-2 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 is 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.
65499	An issue is 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 is 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 was 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, was fixed.
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.
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.
57005	Incorrect traffic counters reported by a RADIUS *Accounting Stop* message after a user session is terminated was 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 was fixed.
65622	A user with more than one IPv4 address is now accounted appropriately in a RADIUS server.
64269	A limitation in the number of supported radius request IDs leading to increased bad authenticator count in RADIUS statistics was fixed.

Table 36 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
59019	An issue with remote APs behind a firewall not reconnecting to controller after the firewall restart was fixed.
62226	The number of IPsec retries in PPPoE remote APs are equal to number configured in the `number_ipsec_retries` field.
62733	Issue was 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.
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 Layer-3 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.
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.
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, was 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 Layer-3 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 was 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” was fixed.

Table 36 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
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 was 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) was 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.
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 Control Plane Security 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.
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 is 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.
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 was fixed.

Table 36 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
59668	An internal controller process malfunction that resulted in a reboot was 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.
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 is 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 is 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.
67090	VRRP running on an untrusted port now works correctly.
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, was 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 was fixed.
60757	An issue was 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 was 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 was fixed.
64566	The issue where the WebUI failed to locate rogue APs after upgrading to ArubaOS 6.1.3.0 is 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.
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** was fixed. Click on the **ap-group name** link to edit the ap-group and the **Delete** button to delete the ap-group.

Table 36 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
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.
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.
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.

Fixed in 6.1.3.1

Table 37 *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 is 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” was 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, was 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.

Table 37 *Bugs Fixed in 6.1.3.1*

Bug ID	Description
64322	Users coming through a Layer-2 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.
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 was 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 was 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() was 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.

Table 37 *Bugs Fixed in 6.1.3.1*

Bug ID	Description
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 38 *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 was 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 ArubaOS. The Croatia country code was enabled in the controller and the AP's regulatory domain was integrated in ArubaOS.
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.

Table 38 *Bugs Fixed in 6.1.3.0*

Bug ID	Description
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 was fixed.
53897, 52825, 55118, 53365, 59274, 61930	An AP-125 crash caused by a node leak was 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.

Table 38 *Bugs Fixed in 6.1.3.0*

Bug ID	Description
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).
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” was 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.

Table 38 *Bugs Fixed in 6.1.3.0*

Bug ID	Description
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.
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 Layer-2 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.

Table 38 *Bugs Fixed in 6.1.3.0*

Bug ID	Description
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.
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 Layer-3 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 was 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 was 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	Layer-2 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.

Table 38 *Bugs Fixed in 6.1.3.0*

Bug ID	Description
58895	Applying a “noe-acl” no longer causes RTP packets to be dropped for IP Touch 310/610 phones.
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 Releases

This chapter describes the known issues and limitations identified in previous 6.1.3.x versions of ArubaOS.

Supported Browsers

Starting 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

An Aruba 651 controller reboots 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 an 802.11g 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, and save the configuration.

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

Known Issues

Access Point

Table 2 *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.
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.
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 of the Aruba 651 controller. To disable the radio for a specific AP, please follow the instruction provided in "Aruba 651 Internal AP" on page 57.
64014	When an AP rebootstraps due to loss of connection to a controller, a process on the AP crashes due to corrupted memory. There is no identified trigger for this issue. Workaround: None.
69019	PPPoE RAPs may rebootstrap due to missed heartbeats in a network with high traffic on the wired AP interface. This issue is seen in ArubaOS6.1.3.0.
69367	APs flooded with packets in a network with large number of datapath sessions sometimes drop the ping command. This issue is seen in AP-105 running ArubaOS 6.1.3.2.
71291	With the addition of DFS channel support on the AP-124 and AP-125 in ArubaOS 6.1.3.2, DFS channels are now automatically assigned by ARM to `ap regulatory-domain-profile "default."` However, these channels do not appear in the default profile's channel plan. This can lead to connectivity issues for voice and data clients.
72938	The internal controller process that manages AP management and user association can become overloaded and trigger APs to rebootstrap. This issue occurs when there are many APs associated with the controller and the adaptive resource management (ARM) feature changes the AP power settings on all APs at the same time. Workaround: Disabling ARM may help resolve this issue.
73184, 74037	A subset of APs connected to a local controller are up on the local but are marked as down on the master controller. This occurs when campus APs (CAPs) on master or local controllers, not using control plane security, discover the master using DNS, DHCP, or ADP and connect to the master before moving to the local controller configured in the AP system profile. An entry is created on the master and local controllers simultaneously. When the AP is aged out on the master, it is marked as down. Workaround: Execute the command `clear gap-db lms <lms-ip>` on the master using the IP of the local controller. This should make the LMS send an update of all the APs marked UP and the master should show the correct status. Additionally, this issue can be resolved by rebooting the APs.

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.
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.
70343	Custom captive portal (CP) pages are not synchronized between the master and standby controllers. This occurs when captive portal pages are configured in a master/standby setup. If the standby controller becomes a master, the custom portal page no longer shows up during CP authentication.

Control Plane Security

Table 5 *Control Plane Security Known Issue and Limitation*

Bug ID	Description
66413	Occasionally, the Control Plane Security (CPSec) whitelist database entries are not synced between the master controller and the local controller. The lossy network between the master and local causes some whitelist sync fragments to be lost.

DHCP

Table 6 *DHCP Known Issue and Limitation*

Bug ID	Description
69145	Starting with ArubaOS 6.1.3.2, if your controller supports clients behind a wireless bridge or virtual clients on VMware devices, you must disable the **broadcast-filter arp** setting to allow those clients to obtain an IP address.

IPsec

Table 7 *IPsec Known Issue and Limitation*

Bug ID	Description
69430	After upgrading to ArubaOS 6.1.3.2, a Campus AP (CAP) reboots with the message `switching to clear. Error:RC_ERROR_IKEP1. Ipsec not successful after reboot`. The reboot occurs when the CAP is unable to establish an IPSec connection with the controller. There is no applicable workaround for this issue.

IPv6

Table 8 *IPv6 Known Issue and Limitation*

Bug ID	Description
57059	When the number of IPv6 Layer-3 interfaces exceeds the supported platform limit, it affects the routing on the controller. Do not exceed the maximum number of IPv6 Layer-3 interfaces.

Mobility

Table 9 *Mobility Known Issue and Limitation*

Bug ID	Description
74272	Traffic from a wireless client on the home agent (HA) to a wired client on the foreign agent (FA) fails when Layer-3 mobility is enabled. This issue is seen in 6000 and 3000 Series controllers running ArubaOS 6.1.x and is triggered after the wireless client does multiple HA to FA roams. Workaround: None

Platform/Datapath

Table 10 *Platform/Datapath Known Issues and Limitations*

Bug ID	Description
62096	M3 controllers may unexpectedly reboot with the reason `User pushed reset`. This issue is seen when there is high traffic between the control plane and the datapath. Workaround: Configure VLAN bandwidth contracts to reduce the traffic to the control plane.
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.
73901	The ports on a controller go into the blocking state when spanning tree is enabled globally and disabled on the interfaces, and the spanning tree on VLAN command is executed twice. Adding a spanning tree on a VLAN which already has a spanning tree causes all the ports in that VLAN to go into the blocking state. This issue was observed in 3200 controllers running ArubaOS 6.1.3.4 and 6.1.3.5. Workaround: Flap the spanning tree state on the ports to recover the controller.

Remote AP

Table 11 *Remote AP Known Issues and Limitations*

Bug ID	Description
51546	While using the 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.
67845	In a deployment of a RAP using the UML290 modem, the RAP rebootstraps when an user is connected to the split tunnel mode VAP and the corp ACL has a VLAN/subnet other than its split VAP client subnet.This setup sends the client broadcast data (like netbios) over the USB uplink without source NATing it thereby causing the rebootstrap of the USB uplink. One of the following workarounds may be used: • Add the client subnet as part of the corp alias of the split VAP user role ACL. • Add an entry in split VAP user role ACL, which will deny the netbios broadcast. • Disabling the netbios on the client also solves the issue.

Security

Table 12 *Security Known Issues and Limitations*

Bug ID	Description
72843	An issue has been identified where slower network performance and response times occur with 6000 and 3000 Series controllers running ArubaOS 6.1.3.2 in networks that support mostly client-to-client traffic experience. Workaround: None
73130	The ArubaOS Syslog Parser might not change user roles for clients (that have dot1x enabled) in sleep mode. As a workaround, clear the pmk-cache for a successful authentication.

Station Management

Table 13 *Station Management Known Issues and Limitations*

Bug ID	Description
66261	If the **even VLAN** and **preserve VLAN** features are enabled in the VAPs and a client moves from one VAP to another, and if the client VLAN does not exist in the new VAP, the client connection fails. Check with Aruba TAC before you enable these features.
72717	An internal controller process failure (STM module) can occur after upgrading from ArubaOS 6.1.x.x to ArubaOS 6.1.3.x.This condition is rare and may be the result of an incomplete or incorrect upgrade procedure. Please contact Aruba support to seek help to restore normal operation.

Voice

Table 14 *Voice Known Issue and Limitation*

Bug ID	Description
62515, 71202	It has been observed that the SIP ALG does not prioritize the SIP media ports which results in poor traffic quality and disconnections due to frame loss or delay. This issue is seen in controllers running ArubaOS 6.1 with SIP clients configured to use video capability.

WebUI

Table 15 *WebUI Known Issue and Limitation*

Bug ID	Description
66521	When creating a user in the WebUI, 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.

Chapter 5

Upgrade Procedures

This chapter details software 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:

Important Points to Remember and Best Practices

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

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any other changes to your network during the upgrade, such as configuration changes, hardware upgrades, or changes to the rest of the network. This simplifies troubleshooting.
- Know your network. Please verify the state of your network by answering the following questions.
  - How many APs are assigned to each controller? Verify this information by navigating to the **Monitoring > Network All Access Points** section of the WebUI, or by issuing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the controller (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS is currently on the controller?
  - Are all controllers in a master-local cluster running the same version of code?
  - Which services are used on the controllers (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software images to the controller. FTP is faster then TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to ArubaOS 6.1.3.6, assess your software license requirements and load any new or expanded licenses you require. For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the user guide.

Memory Requirements

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

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

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.

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

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

Backing up Critical Data

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

- Configuration data
- WMS database
- Local user database
- Licensing database
- Floor plan JPEGs
- Custom captive portal pages
- x.509 certificates
- Controller Logs

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

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

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, and enter the following command:

   ```
   (host) # write memory
   ```
2. Use the **backup** command to back up the contents of the Compact Flash file system to the flashbackup.tar.gz file.

   ```
   (host) # backup flash
   Please wait while we tar relevant files from flash...
   Please wait while we compress the tar file...
   Checking for free space on flash...
   Copying file to flash...
   File flashbackup.tar.gz created successfully on flash.
   ```
3. Use the **copy** command to transfer the backup flash file to an external server:

   ```
   (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
   ```
4. Use the **restore** command to untar and extract the flashbackup.tar.gz file to the compact flash file system:

   ```
   (host) # restore flash
   ```

Upgrading in a Multi-Controller Network

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

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 6.1.3.6:

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

ArubaOS 6.x is supported only on the newer MIPS controllers (M3, 3000 Series and 600 Series). Legacy PPC controllers (200, 800, 2400, SC1 and SC2) 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 67.)

Caveats

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

- Control plane security is disabled when you upgrade from 3.4.x to 6.0.1 (control plane security 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*.

Install using the WebUI

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

Upgrading From an Older version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. If you are running one of the following versions of ArubaOS, you must download and upgrade to an interim version of ArubaOS before upgrading to ArubaOS 6.1.3.6.

- For ArubaOS 3.x.versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.
- For ArubaOS RN-3.x or ArubaOS 5.0.x versions earlier than ArubaOS 5.0.3.1, download the latest version of ArubaOS 5.0.4.x.
- For ArubaOS versions 6.0.0.0 or 6.0.0.1, download the latest version of ArubaOS 6.0.1.x.

Follow step 2–step 11 of the procedure described in "Upgrading From a Recent version of ArubaOS" on page 69 to install the interim version of ArubaOS, then repeat step 1–step 11 of the procedure to download and install ArubaOS 6.1.3.6.

Upgrading From a Recent version of ArubaOS

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

- 6.0.1.x or later
- 5.0.3.1 or later (If you are running ArubaOS 5.0.3.1 or the latest 5.0.x.x, review "Upgrading With RAP-5 and RAP-5WN APs" on page 69 before proceeding further.)
- 3.4.4.1 or later

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

1. Download ArubaOS 6.1.3.6 from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Log in to the ArubaOS WebUI from the PC or workstation.
4. Navigate to the **Maintenance > Controller > Image Management** page. Select the **Upload Local File** option, then click **Browse** to navigate to the saved image file on your PC or workstation.
5. Select the downloaded image file.
6. In the **partition to upgrade** field, select the non-boot partition.
7. In the **Reboot Controller After Upgrade** option field, best practices is to select **Yes** to automatically reboot after upgrading. If you do not want the controller to reboot immediately, select **No**. Note however, that the upgrade will not take effect until you reboot the controller.
8. In Save **Current Configuration Before Reboot** field, select **Yes**.
9. Click **Upgrade**.
10. When the software image is uploaded to the controller, a popup window displays the message **Changes were written to flash successfully**.Click **OK**. If you chose to automatically reboot the controller in step 7, the reboot process starts automatically within a few seconds (unless you cancel it).
11. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > Controller > Controller Summary** page to verify the upgrade.

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

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

Upgrading With RAP-5 and RAP-5WN APs

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

1. Check the provisioning image version on your RAP-5/RAP-5WN Access Points by executing the **show ap image version** command.

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

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

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

   ```
   show ap image version
   ```

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

If you omit the above process or fail to complete the flash (Provisioning/Backup) image upgrade to 5.0.4.x and the RAP-5/RAP-5WN was reset to factory defaults, the RAP will not be able to connect to a controller running ArubaOS 6.1.3.6 and upgrade its production software image.

Install using the CLI

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

Upgrading From an Older version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. If you are running one of the following versions of ArubaOS, you must download and upgrade to an interim version of ArubaOS before upgrading to ArubaOS 6.1.3.6.

- For ArubaOS 3.x.versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.
- For ArubaOS RN-3.x or ArubaOS 5.0.x versions earlier than ArubaOS 5.0.3.1, download the latest version of ArubaOS 5.0.4.x.
- For ArubaOS versions 6.0.0.0 or 6.0.0.1, download the latest version of ArubaOS 6.0.1.x.

Follow step 2 –step 7 of the procedure described in "Upgrading From a Recent version of ArubaOS" on page 70 to install the interim version of ArubaOS, then repeat step 1–step 7 of the procedure to download and install ArubaOS 6.1.3.6.

Upgrading From a Recent version of ArubaOS

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

- 6.0.1.x or later
- 5.0.3.1 or later. (If you are running ArubaOS 5.0.3.1 or the latest 5.0.x.x, review "Upgrading With RAP-5 and RAP-5WN APs" on page 69 before proceeding further.)
- 3.4.4.1 or later

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

1. Download ArubaOS 6.1.3.6 from the customer support site.

2. Open a Secure Shell session (SSH) on your master (and local) controller(s).
   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>
   ```

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

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

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

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

   or

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

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

   ```
   (hostname)# show image version

   ---------------------------------
   Partition               : 0:1 (/dev/ha1) **Default boot**
   Software Version        : ArubaOS 6.1.3.6 (Digitally Signed - Production Build)
   Build number            : 36462
   Label                   : 36462
   Built on                : Fri Dec 14 00:03:14 PDT 2012
   ---------------------------------
   Partition               : 0:1 (/dev/ha1)
   Software Version        : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)
   Build number            : 33796
   Label                   : 33796
   Built on                : Fri May 25 10:04:28 PDT 2012
   ```

6. Reboot the controller:

   ```
   (hostname)# reload
   ```

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

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

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

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

Downgrading

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

If you upgraded from 3.3.x to 5.0, the upgrade script encrypts the internal database. New entries created in ArubaOS 6.1.3.6 are lost after the downgrade (this warning does not apply to upgrades from 3.4.x to 6.1).

If you do not downgrade to a previously-saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from ArubaOS 6.1.3.6 to 5.0.3.2, changes made to WIPS in 6.x prevents the new predefined IDS profile assigned to an AP group from being recognized by the older version of ArubaOS. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.

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

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

Before you Begin

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

1. Back up your controller. For details, see "Backing up Critical Data" on page 66.
2. Verify that control plane security is disabled.
3. Set the controller to boot with the previously-saved pre-6.1 configuration file.
4. Set the controller to boot from the system partition that contains the previously running ArubaOS image.

   When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next controller reload. An error message displays if system boot parameters are set for incompatible image and configuration files.
5. After downgrading the software on the controller:

- Restore pre-6.1 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.1.3.6 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 6.1.3.6, the changes do not appear in RF Plan in the downgraded ArubaOS version.
- If you installed any certificates while running ArubaOS 6.1.3.6, you need to reinstall the certificates in the downgraded ArubaOS version.

Downgrading using the WebUI

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

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

Downgrading using the CLI

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

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

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

   or

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

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

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

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

   In the following example, partition 0, the backup system partition, contains the backup release 6.1.3.2. Partition 1, the default boot partition, contains the ArubaOS 6.1.3.6 image:

```
#show image version
-----------------------------------
Partition               : 0:1 (/dev/ha1)
Software Version        : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)
Build number            : 33796
Label                   : 33796
Built on                : Fri May 25 10:04:28 PDT 2012
-----------------------------------
Partition               : 0:1 (/dev/hda2) **Default boot**
Software Version        : ArubaOS 6.1.3.6 (Digitally Signed - Production Build)
Build number            : 36462
Built on                : 2012-12-14 2:11:59 PST 2012
```

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