ArubaOS 6.1.3.9

Release Notes

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1 Release Overview 5
Release Mapping 5
Contacting Support 6

Chapter 2 What's New in this Release 7
Regulatory Updates 7
Resolved Issues 7
AP—Datapath 7
AP—Platform 8
AP—Wireless 8
Base OS Security 9
Command Line Interface 9
Control Plane Security 9
Controller Platform 10
Controller Datapath 10
Guest Provisioning 10
IPsec 10
Mobility 11
Online Certificate Status Protocol (OCSP) 12
RADIUS 12
RAP+BOAP 12
Role/VLAN Derivation 12
SNMP 13
Switch-Platform 13
Switch-Datapath 13
UI-Configuration 14
Voice 15
Issues Under Investigation 15
Controller Datapath 15

Chapter 3 Features Added in Previous 6.1.3.x Releases 17
Support for the New Version of ETSI DFS standard 17
Supported Channels and Country Domains 17
Regulatory Adjustments 19
Improved Interference Immunity 19
Upgrade Issues 19
Updated WebUI and CLI 19
Cell Size Reduction 19
Impact on Network Performance 19
Updated WebUI and CLI 20
Enhancements to cfgm 20
Suppress-ARP and Broadcast-Filter ARP 20
WMS Configuration Changes 20
Single-chain-legacy is Renamed CSD-override 20
Software Retry is Renamed Temporal Diversity 21
CLI Changes 21

Chapter 4 Resolved Issues from Previous Releases 23

Fixed in 6.1.3.8 23
802.1X 23
Air Management - IDS 23
AP Platform 23
AP Regulatory 24
AP Wireless 25
Base OS Security
Controller Datapath 25
Controller Plane Security (CPSec) 26
Controller Platform 27
Mobility 27
RAP+BOAP 27
Role/VLAN Derivation 28
Station Management 28
Voice SIP 29

Fixed in 6.1.3.7 29
AP Platform 29
AP Wireless 29
BaseOS Security 30
Controller-Datapath 30
Controller Platform 31
IPsec 31
Management Authentication 32
Port-Channel 32
Radius 32
RAP-3G (Remote APs with USB 3G wireless cards) 32
Role/VLAN Derivation 33
Security 33
XML API 33

Fixed in 6.1.3.6 33
802.1X 33
Air Management 34
AP Regulatory 34
AP Wireless 34
Authentication 35
BaseOS Security 36
Controller-Datapath 37
Controller Platform 37
IPsec 38
Mesh 38
RADIUS 38
Role/VLAN Derivation 39
Startup Wizard 39
Station Management 39
Voice 39
VPN 40
WebUI 40

Fixed in 6.1.3.5 40
Air Management - IDS 40
AP 40
Authentication 41
Captive Portal 41
Configuration 41
Hardware Management 41
Interface 42
IPsec 42

IPv6 42
Mesh 42
Mobility 42
M-Switch Software 43
Platform/Datapath 43
Port-Channel 43
RADIUS 43
Remote AP 44
Security 44
SNMP 45
Station Management 45
WebUI 45
Fixed in 6.1.3.4 45
Access Points 45
Air Management (IDS) 46
DHCP 46
Guest Provisioning 46
Mobility 46
Other 47
Platform/Datapath 47
Port Channel 47
RADIUS 48
Remote AP 48
Security 48
SNMP 48
Station Management 49
WebUI 49
Fixed in 6.1.3.3 50
Fixed in 6.1.3.2 50
Fixed in 6.1.3.1 59
Fixed in 6.1.3.0 61
Chapter 5 Known Issues observed in Previous Releases 67
Supported Browsers 67
Maximum DHCP Lease Per Platform 67
Aruba 651 Internal AP 67
In the CLI 67
In the WebUI 68
Known Issues 69
Authentication 69
Controller Datapath 69
Controller Platform 69
Mobility 70
Access Point 70
Air Management - IDS
AP Platform
AP Wireless
ARM 72
Authentication 73
BaseOS Security 75
Controller-Datapath 75
Controller Platform 75
DHCP 77
802.1X 77
IPv6 77
Management Auth 78

Mobility 78
Platform/Datapath 78
RADIUS 79
Security 79
SNMP 79
Station Management 79
Voice 81
WebUI 81
WMM 81
Issues Under Investigation 83
AP Platform 84
BaseOS Security 84
Controller Datapath 84
Controller-Platform 84
Hardware Management 85
WebUI 85

Chapter 6 Upgrade Procedures 87

Important Points to Remember and Best Practices 87
Memory Requirements 88
Backing up Critical Data 88
Backup and Restore Compact Flash in the WebUI 88
Backup and Restore Compact Flash in the CLI 89
Upgrading in a Multi-Controller Network 89
Upgrading to 6.1.x 90
Caveats 90
Install using the WebUI 90
Upgrading From an Older version of ArubaOS 90
Upgrading From a Recent version of ArubaOS 91
Upgrading With RAP-5 and RAP-5WN APs 91
Install using the CLI 92
Upgrading From an Older version of ArubaOS 92
Upgrading From a Recent version of ArubaOS 92
Downgrading 94
Before you Begin 94
Downgrading using the WebUI 95
Downgrading using the CLI 95
Before You Call Technical Support 96

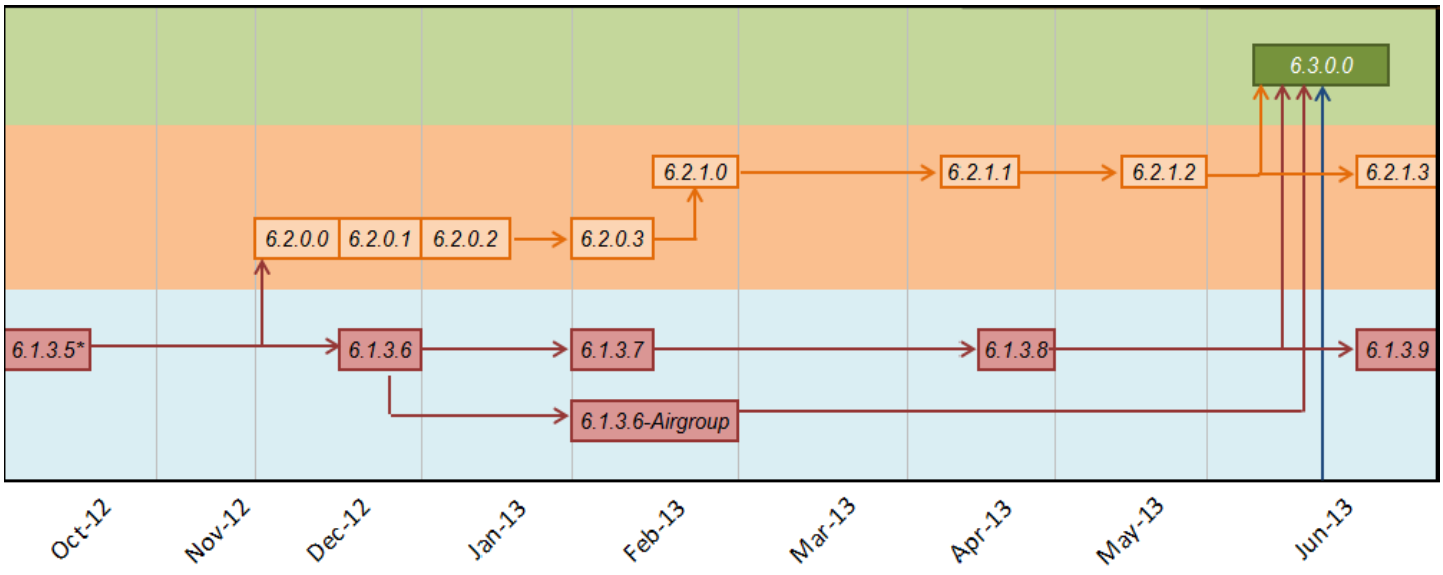
ArubaOS 6.1.3.9 is a general availability (GA) patch release that fixes many previously outstanding issues. All critical and minor security and stability fixes will be applied to subsequent patches of this GA release, until the ArubaOS 6.x branch merges into a future major GA release. For more information, 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 this version of ArubaOS, follow the procedures described in "Upgrade Procedures" on page 85.

Release Mapping

The following illustration shows the patches and maintenance releases included in ArubaOS 6.1.3.9:

Figure 1 *ArubaOS Releases and Code Stream Integration*



*6.1.3.0 contains 6.0.1.2, 5.0.3.3. and 3.4.4.2 patch content

Contacting Support

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

This chapter describes regulatory changes and lists bugs fixed in the ArubaOS 6.1.3.9 release. In addition, it lists bugs discovered since the prior release but not resolved yet, and lists customer issues currently under investigation.

Regulatory Updates

The following table describes regulatory enhancements introduced in ArubaOS 6.1.3.9.

Table 1 *Country Code Regulatory Updates*

Country	Change
European Union (EU)	Transmission power limits for AP-124, AP-125, AP-92, and AP-93 access points (AP) were changed to comply with the updated European Telecommunications Standards Institute (ETSI) standard.
China, Russia	Added support for RAP-108 and RAP-109 remote access points (RAP).
Croatia	Transmission power limits for AP-92 and AP-93 APs were changed to comply with the updated ETSI standard.
Macau	Added support for AP-130 Series and AP-175P APs.
Saudi Arabia	Transmission power limits for AP-124 and AP-125 APs were changed to comply with the updated certificate standards.

Resolved Issues

The following issues are resolved in ArubaOS 6.1.3.9:

AP—Datapath

Table 2 *AP—Datapath Fixed Issue*

Bug ID	Description
70879	**Symptom:** An AP crashed and rebooted after upgrading to ArubaOS 6.2. This issue was resolved by synchronizing the access to Rx queue during scanning of the packets. **Scenario:** The AP processes the Rx frames before switching the channels during scanning the packets. The issue was triggered by a race condition while accessing the Rx queue and was not limited to a specific controller or release version.

AP—Platform

Table 3 *AP—Platform Fixed Issues*

Bug ID	Description
69846	**Symptom:** The following issues were observed on a master controller: • APs associated with a local controller showed as down on the master controller. • The show ap database command took a long time to return output. • The MySQL server had a high CPU utilization on the master controller. This issue is fixed to ensure that the master controller ignores AP updates from expired sessions of the local controller. **Scenario:** This issue occurred when station management on the master controller had a backlog of incoming messages and turned busy. This issue is not specific to any controller model and release version.
71978 75776	**Symptom**: An AP unexpectedly rebooted due to a memory corruption. This issue is fixed in ArubaOS 6.1.3.9. **Scenario**: This issue was observed in AP-68 running ArubaOS 6.2.0.0.

AP—Wireless

Table 4 *AP-Wireless Fixed Issue*

Bug ID	Description
63762	**Symptom:** Beacons were not sent for a period of 1.6 - 2.0 seconds from an AP causing clients to disconnect. Improvements to the radio reset fixed this issue to ensure that the clients are not disconnected. **Scenario:** This issue was triggered when radio chips were operating on the Dynamic Frequency Selection (DFS) channels in HT-40 mode. This issue was observed in AP-125 models running ArubaOS 6.1.x.
72423 75470 77276 82056 82309 83555	**Symptom:** An AP crashed and rebooted and the log files for the event listed the reason for the crash as **watchdog timeout**. This issue was resolved by fixing a race condition that triggered the AP crash. **Scenario:** The issue was observed on all the 11n AP models running ArubaOS or later.
72951	**Symptom**: An AP-85 stopped responding and rebooted unexpectedly. Internal memory improvements have resolved this issue. **Scenario**: This issue was triggered by invalid memory access. This issue occurred on an AP-85 configured with virtual APs in bridge, tunnel, and decrypt-tunnel forwarding modes, where the 802.11g radio was configured as an air monitor, and the 802.11a radio was configured as a campus AP.
82493	**Symptom:** An AP crashed when a virtual AP configuration changed during any downlink traffic to the clients. A few checks are added to the code to resolve this issue. **Scenario:** This issue is not specific to any AP model or release version.

Base OS Security

Table 5 *Base OS Security Fixed Issues*

Bug ID	Description
67287	**Symptom:** The alternate home agent for a client failed and was not able to roam when Layer-3 (L3) mobility was enabled and the **auth-sta-roam** option was disabled in a network. This issue was fixed by allowing user-entry creation in the alternate home agent. **Scenario**: This issue was observed in controllers running ArubaOS 6.1.3.2 or later.
81426	**Symptom:** Memory leak was observed for wired client with radius accounting enabled. Updates to memory allocation resolved this issue in ArubaOS 6.1.3.9. **Scenario:** The memory leak occurred when wired clients tried to connect to APs having radius accounting enabled in the Authentication, Authorization, and Accounting (AAA) profile. This issue was observed in controllers running ArubaOS running 6.1.3.x.
83776	**Symptom:** The atheros clients did not support multiple relay counters using Wi-Fi Protected Access - Temporal Key Integrity Protocol (WPA-TKIP) encryption and was unable to connect to the network, after upgrading to ArubaOS 6.1.3.7. This issue is fixed by disabling use of multiple Traffic Identifier (TID) for WPA-TKIP. **Scenario:** This issue was observed when Wireless Multimedia Extensions (WMM) was enabled and the atheros clients did not support multiple relay counters.

Command Line Interface

Table 6 *Command Line Interface Fixed Issues*

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

Control Plane Security

Table 7 *Control Plane Security Fixed Issues*

Bug ID	Description
66413 67875 68010	**Symptom**: Occasionally, the Control Plane Security (CPSec) whitelist database entries did not synchronize between the master and local controller. Transmitting smaller sized CPSec record fixed the issue in ArubaOS 6.1.3.9. **Scenario**: This issue was observed when the CPSec whitelist database size was large. The lossy network between the master and local controller caused some whitelist sync fragments to be lost. This issue is not limited to a specific controller model or release version.

Controller Platform

Table 8 *Controller Platform Fixed Issues*

Bug ID	Description
80419 80523	**Symptom:** A feature allowed the ArubaOS DNS server to reveal its version number. This feature has been disabled in ArubaOS 6.1.3.9 as a security precaution. **Scenario:** This issue is not specific to any controller model and was observed in ArubaOS 6.1.3.7.

Controller Datapath

Table 9 *Controller Datapath Fixed Issues*

Bug ID	Description
80956 81555	**Symptom:** A controller crashed and rebooted after upgrading the software from ArubaOS 6.1.3.6 to 6.1.3.7. The log files for the event listed the reason for the crash as **watchdog timeout**. The interrupt handler for packet parsing was modified to ensure that CPU was not overwhelmed with the traffic packets**.** **Scenario:** In a high traffic deployment, a race condition triggered the controller crash and this issue was not specific to any controller models.
83216	**Symptom**: A controller generated proxy ARP responses out of the same trusted port from where the controller learned the MAC address. Disabling the **bcmc-optimization** option in the VLAN interface resolved the issue. **Scenario**: The issue occurred when the trusted port was a port channel and the **bcmc-optimization** option was enabled on the VLAN interface. The issue was not specific to a controller model or a release version.

Guest Provisioning

Table 10 *Guest Provisioning Fixed Issues*

Bug ID	Description
76451	**Symptom**: When guest user details were imported using a .CSV file in the **Configuration > Security > Authentication > Internal DB > Guest User** page of the WebUI, the sponsor's email address was not imported. The issue is fixed my making changes to the code to ignore the sponsor's email address when importing a .CSV file. **Scenario**: The issue was observed in controllers running 6.1.3.9 and 6.2.x and was not limited to any specific controller model.

IPsec

Table 11 *IPsec Fixed Issues*

Bug ID	Description
70627	**Symptom:** VPN tunnel could not be established for a site-to-site VPN between two controllers with Diffie-Hellman (DH) Group-1. The added software support for DH Group-1 fixed this issue in ArubaOS 6.1.3.9. **Scenario:** This issue was observed when DH Group-1 was not configured with IPSec map. Due to an error in implementing DH Group-1, the VPN tunnel could not be established for a site-to-site VPN. This issue was not specific to any controller model and release version.

Table 11 *IPsec Fixed Issues (Continued)*

Bug ID	Description
71686	**Symptom:** Site-to-site IPsec tunnel could not be established to the corporate network. The issue was resolved by handling multiple transform sets in the IPsec map, by looping through all of them. **Scenario:** The IPsec tunnel was not created successfully when multiple transform sets were configured in an IPsec map. This issue was observed on controllers running ArubaOS 6.1.x.
73823	**Symptom:** Site-to-site IPsec tunnel could not be established to the corporate network. The issue was resolved by enhancing the code to support specific hash algorithms. **Scenario:** The issue was observed on the controllers running ArubaOS 6.1.3.x.
77012 79452	**Symptom**: IPv6 traffic from L3 mobility clients sent from a foreign agent (FA) to a home agent (HA) was double encrypted and sent through an IPsec tunnel instead of a Generic Routing Encapsulation (GRE) tunnel without encryption. ArubaOS 6.1.3.9 updates the packets with tunnel flag so that data traffic does not get double encryption in an IPsec tunnel. **Scenario**: This issue was triggered by an internal flag that determines whether the packets parsed into the GRE tunnel should be encrypted. This issue was observed in ArubaOS 6.1.3.x.

Mobility

Table 12 *Mobility Fixed Issues*

Bug ID	Description
75093	**Symptom:** The **show ip mobile host** command displayed the roaming status of a client as **No** state instead of Home Switch/Home VLAN and did not release the host entry. This issue is fixed by making changes to the code to remove the users stuck in **No** state after the idle timeout. **Scenario:** This issue was observed when L3 mobility was enabled on controllers running any version of ArubaOS.
82673	**Symptom:** Clients were unable to obtain an IP address using Dynamic Host Configuration (DHCP) intermittently when a user roamed between controllers with L3 mobility enabled. Changes to the internal tunnel ACL code fixed this issue in ArubaOS 6.1.3.9. **Scenario:** DHCP packets from a client got redirected into an IP-in-IP (IPIP) tunnel due to an incorrect order of Access Control List (ACL) on the FA controller. This issue occurred when L3 mobility was enabled on the controller with clients using DHCP to obtain an IP address. This issue was not specific to any controller model and was observed in ArubaOS 6.1.x.
82971	**Symptom:** Traffic from user VLAN overflowed into management VLAN causing other controllers in the same domain to learn the user MAC address on management VLAN. Changes to the internal code fixed this issue in ArubaOS 6.1.3.9. **Scenario:** L2 broadcast/multicast packets from a client was placed into home VLAN based on route lookup on the client. When the user VLAN was an L2 VLAN, the route lookup resulted in the controller's default gateway and hence the user VLAN traffic overflowed into default gateway VLAN. This issue occurred when L3 mobility was configured and L2 user VLANs extended on the controllers. This issue was not specific to any controller model and was observed in ArubaOS 6.1.3.5 and prior releases.

Online Certificate Status Protocol (OCSP)

Table 13 *OCSP Fixed Issues*

Bug ID	Description
55419 65936 79704	**Symptom:** An internal ArubaOS process (Certmgr) became busy when the OCSP server was unreachable. The issue is fixed by making changes to the OCSP code base. **Scenario:** The users could not authenticate because certmgr was busy queuing the OCSP requests. All users using 802.1X, IKE, mgmt-auth were affected. This issue was observed in controller running ArubaOS 6.1.3.9.

RADIUS

Table 14 *RADIUS Fixed Issues*

Bug ID	Description
76484	**Symptom:** RADIUS authentication failed in networks that had different Maximum Transmission Values (MTUs). To fix this issue, the socket options are updated to allow the controller to send RADIUS requests to the RADIUS server when EAP termination is enabled. **Scenario:** The RADIUS authentication failed when the MTU value in the network between the controller and RADIUS server was different. This issue was observed in controllers running ArubaOS 6.1.3.9.

RAP+BOAP

Table 15 *RAP+BOAP Fixed Issues*

Bug ID	Description
54994 71004 81256 82340	**Symptom:** Datapath on a controller crashed due to an invalid net-destination entry. This issue is fixed by validation of names in dns-list to id mapping in Access Control List (ACL). **Scenario:** This issue was observed only if the ID present in the ACL had no corresponding entry in net-destination name table. This issue occurred when captive portal whitelist or net-destination name was configured in all controller platforms.

Role/VLAN Derivation

Table 16 *Role/VLAN Derivation Fixed Issues*

Bug ID	Description
77242	**Symptom:** Changes to the ArubaOS External Service Interface (ESI) Syslog parsing rule were not reflecting in the user-table or changes to the user-role were reflecting only in the system-table and datapath. This issue was fixed by updating the user-table with ESI role-change. **Scenario:** This issue was observed during a role-change event with ESI. This issue was observed in controllers and APs running ArubaOS 6.1.3.x.

SNMP

Table 17 *SNMP Fixed Issues*

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

Switch-Platform

Table 18 *Switch-Platform Fixed Issues*

Bug ID	Description
80419	**Symptom:** A feature allowed the ArubaOS DNS server to reveal its version number. This feature is disabled as a security precaution. **Scenario:** This issue was identified in ArubaOS 6.1.3.9.

Switch-Datapath

Table 19 *Switch-Datapath Fixed Issues*

Bug ID	Description
73256 83729 84707 84703	**Symptom:** Datapath crash and connectivity issue was observed in a controller. A reduction in the Maximum Transmission Unit (MTU) of the physical ports on M3 resolved this issue in ArubaOS 6.1.3.9. **Scenario:** Datapath crash and connectivity issue occurred in the controller when the upstream switch MTU was set to transmit large packets, received on M3 controller. This issue was observed in M3 controllers running any version of ArubaOS.
74648 74843 81126 83996	**Symptom:** Errors in the internal module (datapath) caused controllers to unexpectedly reboot. Improvements to the internal datapath now prevents this error. **Scenario:** This issue occurred on M3, 3000 Series, and 600 Series controllers running ArubaOS 6.1.3.x.
80625	**Symptom:** A controller rebooted with the reboot reason, **datapath timeout**. This issue was fixed by ensuring that the same tunnel Maximum Transmission Unit (MTU) is used for processing a given packet. **Scenario:** The tunnel MTU change can cause different MTU values to be used while processing a same packet. This incorrectly triggered asserts in code which caused the crash. This issue was observed in controllers running ArubaOS 6.1.3.x or later .
82738	**Symptom:** An Aruba 6000 controller rebooted due to an internal process (datapath) failure. An internal change in the code fixed this issue. **Scenario:** This issue was observed when there was excessive debug logging in an Aruba 6000 controller running ArubaOS 6.1.3.5.

Table 19 *Switch-Datapath Fixed Issues (Continued)*

Bug ID	Description
83409 83482 84696 84442 84298 84219 84064 83272 83788 83721	**Symptom:** Datapath timeout was observed when the controller missed a heartbeat. Corrective action on how Direct Memory Access (DMA) was handled, when out of order, resolved this issue in ArubaOS 6.1.3.9. **Scenario:** Datapath timeout occurred when there was an increase in traffic in the control plane, and the handling of DMA was out of order. This issue was observed in ArubaOS running 6.1.3.x.
84577	**Symptom:** Datapath timeout was observed as the datapath heartbeats did not transmit from the control plane. The handling of DMA was resolved so that the communication between the control plane and datapath TX is replenished with the appropriate buffer. **Scenario:** This issue was triggered due to an increase in the load between the control plane and datapath. This issue is not limited to a specific controller or release version.

UI-Configuration

Table 20 *UI-Configuration Fixed Issues*

Bug ID	Description
77548 80604	**Symptom:** Accessing any page of the controller's WebUI generated a Null error message. Changes to the WebUI session management mechanism have fixed this issue. **Scenario:** This issue occurred due to an internal process error that affects how commands are executed in a WebUI session. This issue was not limited to a specific controller model or release version.
80269	**Symptom:** The GigabitEthernet interface 10 option was missing in the Virtual Router Redundancy Protocol (VRRP) tracking Interface drop-down under the **Advanced Services > Redundancy > Add virtual Router > Tracking Interface table** page of the WebUI. ArubaOS 6.1.3.9 now includes the GigabitEthernet interface 10 option in the VRRP tracking Interface. **Scenario:** This issue was observed in M3 controller models running ArubaOS 6.1.3.1.
81450	**Symptom:** During AP provisioning, the **Configuration failed, provision-ap a-ant-gain 3.8 Invalid value** error was displayed. This issue was fixed by suggesting gain values in multiple of 0.5dB. **Scenario:** This error was observed during AP provisioning when some antennas suggested incorrect gain values (a-ant-gain and g-ant-gain) or gain values that were not in multiple of 0.5dB. This issue is not limited to a specific controller model or release version.
82959	**Symptom:** User was not able to navigate to the fields properly using the tab key in the **Configuration > Security > Authentication > Internal DB > Guest User** page of the WebUI and use the options: **create New**, **import**, **delete**, **print**, and **cancel**. Adding code to the guest provisioning page to create an appropriate tab index for new, import, and edit windows fixed this issue in ArubaOS 6.1.3.9. **Scenario:** This issue was observed in ArubaOS 6.1.x and is not specific to any controller model.

Voice

Table 21 *Voice Fixed Issues*

Bug ID	Description
81487 83707 83757 84631	**Symptom:** Voice clients registered as SIP clients were overridden with the application-level gateway (ALG) value as Vocera or New Office Environment (NOE). This issue is resolved by improvements that prevent subsequent updates to the initially configured ALG value. **Scenario:** This issue was observed in 7200 Series controllers running ArubaOS 6.1.3.3 or later.

Issues Under Investigation

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

Controller Datapath

Table 22 *Controller Datapath Observed Issues*

Bug ID	Description
81207 81208 81256 81479 82085 82232 82592 82827	**Symptom:** A controller running ArubaOS 6.1.3.7 stopped responding and rebooted. The log files for the event listed the reason for the crash as **datapath timeout**.
81369 81572 81853 82645 82707 82708	**Symptom:** A controller running ArubaOS 6.1.3.7 stopped responding and rebooted. The log files for the event listed the reason for the crash as **user pushed reset**.
82086 82672	**Symptom:** A controller running ArubaOS 6.1.3.7 stopped responding and rebooted. The log files for the event listed the reason for the crash as **kernel panic**.

Support for the New Version of ETSI DFS standard

With the exception of RAP-5WN and the AP-120 Series APs, all supported APs will comply with version 1.6.1 or later of the ETSI DFS standard EN301893, when the system is upgraded to ArubaOS 6.1.3.6.

The RAP-5WN and AP-120 Series APs can be upgraded to ArubaOS 6.1.3.6, but will not become compliant with version 1.6.1 of the standard. RAP-5WN and AP-120 Series APs already installed in a network are allowed to remain compliant with the previous version of the standard, but any new devices added to the network after 12/31/2012 must comply with version 1.6.1 or later, wherever ETSI rules apply.

Supported Channels and Country Domains

The following changes impact new installations of AP-124, AP-125, AP-134, and AP-135 APs running ArubaOS 6.1.3.9.

Table 1 *Channel/Domain Changes in this Release*

Country Domain	Change
Changes for AP-124/AP-125 Access Points	
Kazakhstan and Dominican Republic	ArubaOS now supports these country domains.
Australia and New Zealand	These country domains support all channels allowed by the FCC (including indoor, outdoor and DFS channels). In previous releases, Australia and New Zealand used ETSI channels.
UAE	Removed support for channels 149-165.
Mexico	This domain requires Dynamic Frequency Selection (DFS) in all 802.11a channels. In previous releases, all 802.11a channels were open without DFS support.
Serbia	Added DFS support for channels 52-64 and100-140. These channels were not open in previous releases.
New Zealand, Puerto Rico, Columbia	Removed support for channels 120-128, because these channels were removed from the FCC list of allowed channels.
Changes for AP-134/AP-135 Access Points	
Kazakhstan, Chile, Serbia, Dominican Republic and Nigeria	ArubaOS now supports these country domains.

Table 1 *Channel/Domain Changes in this Release*

Country Domain	Change
Bermuda, Croatia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Kenya, Pakistan, Mauritius, Panama, Qatar, Trinidad and Tobago and Uruguay:	Removed support for AP-134 and AP-135 in these country domains.
South Korea and **Taiwan**	Added support for DFS Channels 52-64, and 100-128. Previous releases did not include any support for these channels.
Singapore	Added support for DFS Channels 100-140. Previous releases did not include any support for these channels.
Israel	Channels 36-48 require DFS. In previous releases, these channels were open without DFS support.
Saudi Arabia	Removed support for channel 165.
Ireland and UAE	Removed support from Channel 149-165.
Australia, New Zealand	These country domains support all channels allowed by the FCC (including indoor, outdoor and DFS channels).
Mexico	Requires DFS in all 802.11a channels. In previous releases, all 802.11a channels were open without DFS support.
New Zealand and Puerto Rico	Added DFS channel support for channels 52-64, 100-128. Previous releases did not include any support for these channels.
Colombia and Thailand	Removed support for channels 116-128
Colombia and Thailand	Removed support for channel 132.
Russia	Removed support for channel 132.
Egypt	Removed support for channels 149-165. This country domain no longer supports 40MHz on any channel.
Ukraine	Added 40 MHz support for channels 149-161.
Peru	Removed support for channels 12-13, 52-64, 100-140, and 165. (The only supported channels for this country domain are 1-11, 36-48, and 149-161.)
Venezuela	Added 40MHz support for channels 36-48, 52-64, and 149-161.
Jordan	Added 40MHz support for channels 36-48 and 149-161.

Regulatory Adjustments

Country support and EIRP transmit power levels were updated in ArubaOS 6.1.3.6 to reflect the latest regulatory status and test results.

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.


NOTE

Use this feature with caution, as it can have a negative impact on healthy networks with low levels of interference. Best practices are to configuring this feature first 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 a 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 2 *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. Disable this

feature only if you 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 3 *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.
`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.

Table 3 *CLI Changes in ArubaOS 6.1.3.2*

Command	New Parameter add in 6.1.3.2	Description
`show ipc`	`forwarding-statistics`	Shows statistics about packets forwarded to internal processes from remote nodes.
`show datapath debug`	`opcode`	Shows datapath opcode statistics.

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

Fixed in 6.1.3.8

The following issues have been resolved in ArubaOS 6.1.3.8:

802.1X

Table 1 *802.1X Fixed Issues*

Bug ID	Description
77154	**Symptom:** If the **Use Server provided Reauthentication Interval** setting is enabled in an AP's 802.11X authentication profile, users associated with that AP do not reauthenticate when that client roams to a different AP. This issue was fixed by a change that allows the controller to store the session timeout reauthentication interval returned from the RADIUS server. **Scenario:** This issue occurred in ArubaOS 6.1.2.4, when clients authenticating using a RADIUS server roamed between APs.
79546 81111 81112 81114 81115 82247 82249	**Symptom:** An internal controller module stopped responding, causing the controller to unexpectedly reboot. Memory buffer improvements fixed this issue in ArubaOS 6.1.3.8. **Scenario:** The log file for the event listed the reason for the reboot as datapath exception. This issue occurred in ArubaOS 6.1.3.7.
80841	**Symptom:** A controller configured to use both 802.1X and MAC authentication ignored the **eapol-start** request sent by client before the completion of the MAC authentication process. Improvements to how the key cache is managed during the MAC authentication process fixed this issue. **Scenario:** When mac-auth and 802.1X is configured and an **eapol-start** request from the client came between the mac-auth and 802.1X, the 4-way key exchange was started instead of full 802.1X authentication. This issue was observed in ArubaOS 6.1.3.5.

Air Management - IDS

Table 2 *Air Management - IDS Fixed Issues*

Bug ID	Description
81073	**Symptom**: An Air Monitor (AM) stops scanning when it has been up for more than 50 days. This uptime threshold is reached when the AM's timer-milli-tick counter, which counts the uptime in milliseconds, rolls over and the count returns to zero. This issue was fixed by the accurate handling of roll-over side effect. **Scenario**: This issue was identified on ArubaOS 6.1.3.2 and was not limited to a specific controller or AP model. This roll over is expected behavior and a side effect of the roll over caused the issue.

AP Platform

Table 3 *AP Platform Fixed Issues*

Bug ID	Description
67853	**Symptom:** Master and local Virtual Router Redundancy Protocol (VRRP) controllers in an active state caused APs to rebootstrap. The changes to the bandwidth contracts logic that prioritize the bandwidth fixed this issue. **Scenario:** When a standby VRRP controller did not receive the VRRP heartbeats from the active VRRP controller, both the controllers claimed to be active VRRP controllers. The drop in VRRP heartbeats in the network triggered this issue in Aruba M3, 3000 Series, and 6000 controller models running ArubaOS 6.1.3.2.
74010 77980	**Symptom:** The Station handoff-assist feature had issues after the upgrade of ArubaOS 6.1.3.0 due to the use of outdated Received Signal Strength Indication (RSSI) information. This issue was fixed in ArubaOS 6.1.3.8 and the station handoff-assist feature now uses a more accurate measurement for RSSI to avoid redundant handoffs. **Scenario:** Due to the use of outdated RSSI, the clients showed the low RSSI levels in the `show ap association` command output than the `show ap monitor stats` command output. This issue was not specific to any AP or controller model.
77236	**Symptom:** DNS controller discovery failed when using 802.1X authentication for the AP. The AP successfully completed the 802.1X authentication but failed to connect the master controller using DNS discovery. The error message **No file found under /tmp/master** appeared when the AP came up after a reboot. This issue was resolved by making improvements to the master discovery process. **Scenario:** This issue occurred on AP models running ArubaOS 6.1.3.2 with 802.1X authentication and dynamic master discovery. The AP was selecting an IP address that could reach the master controller before the master controller was discovered.
81865	**Symptom:** When a loopback IP is configured on a controller but the controller IP is set to the IP address of another VLAN interface, there is no entry for the loopback interface's IP address in the user table. This issue was fixed by creating an entry in the user table if the controller's IP address is different from the loopback IP address. **Scenario:** This issue was identified on ArubaOS 6.1.3.5 and is not limited to any specific controller model.

AP Regulatory

Table 4 *AP Regulatory Datapath Fixed Issues*

Bug ID	Description
79119 82000	**Symptom:** Invalid Effective Isotropically Radiated Power (EIRP) was observed on AP-125 when the tx-power (Power transmitted by an AP) is set to 3 dBm or less. The enhancements to the algorithm for the antenna gain fixed this issue in ArubaOS 6.1.3.8. **Scenario:** The algorithm to calculate the actual tx-power in the driver caused this issue. This issue was observed in AP-125 associated with Aruba 3600 controllers running ArubaOS 6.2.1.0.
79804	**Symptom:** Regulatory domain approvals for AP-92 and AP-93 in Panama and Puerto Rico were not enabled in ArubaOS 6.1.3.6. The Panama and Puerto Rico country codes were enabled in the controller and the AP's regulatory domain was integrated to fix this issue in ArubaOS 6.1.3.8. **Scenario:** AP-92 and AP-93 access points did not come up in AP mode of operation in ArubaOS 6.1.3.6.

AP Wireless

Table 5 *AP Wireless Fixed Issues*

Bug ID	Description
79724	**Symptom:** An AP-70 did not deliver buffered data to a Vocera B3000 communication badge when the Vocera device came out of powersave mode, preventing the device from initiating a call. The fix for this issue ensured that the AP sends out buffered data packets when it is notified that the Vocera client has come out of powersave mode. **Scenario:** This issue occurred on AP-70 APs running ArubaOS 6.1.3.6, when the client Vocera badge receiving the call roamed to another AP, and then returned to its original AP.
80334	**Symptom:** Clients intermittently disconnected after successfully connecting to the 2.4 GHz Band of an AP-124. On rare occasions, if an AP deferred scanning, ArubaOS might keep some scan flags turned on and assume the AP to be in a scanning state, preventing the AP from transmitting data frames. Changes to how the scan flags are cleared when the AP defers scanning resolved this issue in ArubaOS 6.3.1.8. **Scenario:** This issue occurred when clients connected to an Open or Secure SSID, in a topology where the client VLAN was a L2 VLAN on the controller and an uplink Cisco switch was the default gateway for the client.

Base OS Security

Table 6 *Base OS Security Fixed Issues*

Bug ID	Description
70323	**Symptom:** Remote APs (RAP) rebootstrapped with the controller log files listed authentication failure as the reason for the rebootstrap. The improvements to the inner and outer IP entries handling process fixed this issue in ArubaOS 6.1.3.8. **Scenario:** This issue was observed when a static inner IP address was assigned to RAPs. On reboot, RAPs came up with new outer IP address but with the same inner IP address through Network Address Translation (NAT). This issue was observed in ArubaOS 6.1.3.1.
79805	**Symptom:** An internal controller process stopped responding, causing the controller to reboot and preventing new clients from authenticating. Memory buffer improvements resolved this issue in ArubaOS 6.1.3.8. **Scenario:** The error handling process incorrectly released the Extensible Authentication Protocol (EAP) memory which caused the memory corruption under rare conditions. This issue occurred in an M3 controller running ArubaOS 6.1.3.7 in a master-local topology where M3 controller acted as a local.
80324 82771 82999	**Symptom**: An internal controller module failed to respond, causing the controller to reboot. This issue was resolved in ArubaOS 6.1.3.8. **Scenario**: This issue was identified in 620 controllers upgrading from ArubaOS 6.1.3.6 to 6.1.3.7, and was triggered by an incorrect certificate.
80786 81665	**Symptom:** The internal controller process that handles user authentication crashed when the command **`show aaa xml-api statistics`** was executed from the command-line interface of a controller. This issue was fixed in ArubaOS 6.1.3.8. **Scenario:** This issue was observed in ArubaOS 6.1.3.7.

Controller Datapath

Table 7 *Controller Datapath Fixed Issues*

Bug ID	Description
74816	**Symptom:** A Backup VRRP controller erroneously became the active controller when bandwidth contracts were exceeded. The VRRP information was in a low priority queue and getting dropped. This issue was fixed in ArubaOS 6.1.3.8 to ensure that the VRRP information is in the high priority queue and will not be dropped. **Scenario:** This issue was observed in ArubaOS 6.2.0.0.

Controller Plane Security (CPSec)

Table 8 *Controller Plane Security Fixed Issues*

Bug ID	Description
67332	**Symptom:** Neighbor table overflow messages appeared in the system log of the controller. This issue was fixed in ArubaOS 6.1.3.8 by increasing the size of the neighbor table entries on the controller. **Scenario:** An increase in the packet flow through the controller caused the controller to send ARP request for the IP address. This issue was observed in ArubaOS 6.1.3.0.
72303 72854 73288 72429 78498 79470	**Symptom:** APs were unable to come up when control plane security was enabled on the controller. The output of the show AP database CLI command showed these APs stuck with the status Generating TU request. Improvements to the certificate generation process during the role change fixed this issue in ArubaOS 6.1.3.8. **Scenario:** This issue occurred when the role of the controller was changed from standalone master to cluster-root or cluster-member and the other way around. This issue was observed in ArubaOS 6.1.3.2.
78301	**Symptom:** CPSec whitelist in master controller stopped synchronizing with local controllers due to an interruption in the synchronization process. The enhancements to the retry attempts of the synchronization process on master controller fixed this issue in ArubaOS 6.1.3.8. **Scenario:** The crash of CPSec whitelist synchronization on master controller is caused by an interruption that may include any of the following: • loss of network connectivity • loss of minor frames • crash or reboot associated with the controller This issue was observed in ArubaOS 6.1.2.6.

Controller Platform

Table 9 *Controller Platform Fixed Issues*

Bug ID	Description
79719 81014 81086 81087 81181 81207 81368 81393 81479 81669 81853 82085 82232 82645 82708 82835	**Symptom:** A controller crashed and rebooted frequently after upgrading the software from ArubaOS 6.1.3.6 to ArubaOS 6.1.3.7. The improvements to packet processing fixed this issue in ArubaOS 6.1.3.8. **Scenario:** The high amount of control traffic triggered this issue and this issue is not specific to any controller models.
80326 80780 81399 81462 82385 82775	**Symptom:** An SOS datapath timeout occurred on the controller and crashed with the **Control Processor Kernel Panic** message without saving the SOS crash log tar files. The internal code changes fixed this issue in ArubaOS 6.1.3.8. **Scenario:** This issue was observed in ArubaOS 6.1.3.7.

Mobility

Table 10 *Mobility Fixed Issues*

Bug ID	Description
78111	**Symptom:** Loss of traffic was observed on roaming clients, when L3 mobility was enabled on the controller. This issue was fixed in ArubaOS 6.1.3.8. **Scenario:** This issue occurred because duplicate ARP responses were sent both from the home agent and foreign agent for the roaming client. Due to this, the bridge entry for the roaming client on the upstream switch was flipped. This issue was observed when a controller upgraded from ArubaOS 5.x to 6.1.x.

RAP+BOAP

Table 11 *RAP+BOAP Fixed Issues*

Bug ID	Description
59360	**Symptom:** Ethernet port of APs in bridge forwarding mode could not be configured in trusted mode because the support for transparent bridging on wired clients was not available. The support for transparent bridging was added in ArubaOS 6.1.3.8. **Scenario:** This issue was observed in APs configured as RAP and control plane security AP (CPSEC AP) on controllers running ArubaOS 6.2.0.0.

Table 11 *RAP+BOAP Fixed Issues (Continued)*

Bug ID	Description
77852	**Symptom:** An AP-105 crashed while decrypting an IPsec packet. Internal code changes fixed this issue in ArubaOS 6.1.3.8. **Scenario:** When an encrypted IPsec packet was received and processed by an AP for decryption, the packet data was fragmented (not IP fragmentation), and stored in more than one packet descriptor, as the OS allocated less space for the packets. This issue was observed in the AP-105, AP-93, and the AP-94 running ArubaOS 6.1.3.5.
77450	**Symptom:** Wired clients connected to a Remote AP in bridge forwarding mode were unable to get an IP address when the AP lost connectivity to the controller, or if any of the following fields changed in Virtual AP or SSID: • WLAN SSID opmode • WLAN SSID profile passphrase • probe type • Physical connection (phy) type • Forwarding mode • Remote AP operation • VLAN • ESSID • Backup Virtual AP in bridge forwarding-mode with PSK enabled This issue is fixed in ArubaOS 6.1.3.8. **Scenario:** This issue was observed when the AP has a backup Virtual AP in the same VLAN as the wired clients. This issue was observed in ArubaOS 6.1.x.

Role/VLAN Derivation

Table 12 *Role/VLAN Derivation Fixed Issues*

Bug ID	Description
78322	**Symptom:** Bridge clients were deriving incorrect roles when the AP was connected to a Cisco bridge VLAN. This issue was resolved in ArubaOS 6.1.3.8. **Scenario:** This issue was observed when an AP was connected to a Cisco bridge VLAN; the AP was receiving its own broadcast message over uplink and started deleting the L2 and L3 entries. This issue is not specific to any controller model.

Station Management

Table 13 *Station Management Fixed Issues*

Bug ID	Description
78805 75872	**Symptom:** The Station Management process terminated and restarted erratically on the controller. This issue was fixed in ArubaOS 6.1.3.8 by blocking certain entries and events that are created during an image-mismatch. **Scenario:** This issue was observed in ArubaOS 6.1.3.6 with mesh portals and mesh points in the setup. When the image version on mesh portals and mesh points was different from the image version stored on the controller, the initialization sequence for these APs was not accurate. This created some incomplete entries that caused a crash.

Voice SIP

Table 14 *Voice SIP Fixed Issues*

Bug ID	Description
79717	**Symptom:** The SIP application-level gateway (ALG) did not prioritize Real-time Transport Protocol (RTP) traffic for the Jabber application. Changes to the SIP parser fixed this issue in ArubaOS 6.1.3.8. **Scenario:** SIP ALG was not able to parse SDP (Session Description Protocol) and this resulted in the traffic was not prioritized. This issue was observed in ArubaOS 6.1.3.5.

Fixed in 6.1.3.7

The following issues were resolved in ArubaOS 6.1.3.7:

AP Platform

Table 15 *AP Platform Issues Fixed in 6.1.3.7*

Bug ID	Description
69426 75265	**Symptom:** When a certain internal AP process (SAPD) crashed, configured Virtual APs (VAPs) were not deleted from the AP. When the process restarted, the AP detected that the VAPs already existed. As a result, the following error messages were triggered: **sapd| An internal system error has occurred at file sapd_wlanconfig.c function sapd_wlanconfig_create line 86 error Error creating VAP 0:0** The AP can now recognize that the undeleted VAPs are already there. If VAP creation fails due to any pre-existing VAP on the radio, the log will show the error message at the debug level, else the message will be displayed in the log at the error level. An error message cannot be avoided if VAP creation fails for a reason other than a pre-existing VAP since it is indicative of some other problem. Since an error arising from a pre-existing VAP is a harmless error, the log level for that scenario was lowered from error to debug. **Scenario:** When the SAPD process on an AP crashes and restarts, it returns this error when it tries to bring up VAPs since the VAPs already exist. This issue was not specific to any controller model or software version.
70150 71177 73465 73602 74680	**Symptom:** APs crashed and rebooted due to lack of memory. The `show ap debug system-status` command displayed the message **Reboot caused by out of memory.** **Scenario:** This issue was observed when Virtual APs (VAPs) were enabled and later disabled repeatedly. This issue was not limited to a specific AP or controller model.

AP Wireless

Table 16 *AP Wireless Issues Fixed in 6.1.3.7*

Bug ID	Description
69063 72123	**Symptom:** An unexpected AP reboot occurred. This issue was caused by an internal reference to an empty entry in a data table, and was resolved by adding a check to prevent the access of such data when the entry was not present. **Scenario:** This issue was observed in APs terminating on local 3600 controllers running ArubaOS 6.1.3.2 in a master-local topology.

Table 16 *AP Wireless Issues Fixed in 6.1.3.7 (Continued)*

Bug ID	Description
77946	**Symptom:** Mixed encryption mode with `static-wep wpa-psk-tkip` and `dynamic-wep wpa-tkip` could not be configured. **Scenario:** When editing the SSID profile in the WebUI, the system displays the error message **`invalid opmode combination`**, even though **`dynamic-wep wpa-tkip`** is available for selection in the WebUI. This issue was observed in ArubaOS 6.1 and later versions, and is not specific to any hardware model. This issue was fixed by adding these modes to the list of allowed combinations.

BaseOS Security

Table 17 *BaseOS Security Issues Fixed in 6.1.3.7*

Bug ID	Description
68467	**Symptom:** The correct VLAN was assigned to a wireless client when the initial 802.1X authentication assigned a user a role with a role-based VLAN. However, when the same client reauthenticated using a different credential which assigned a role without a role-based VLAN, the role-based VLAN from the first authentication was incorrectly assigned. **Scenario:** This issue was observed in controllers running ArubaOS 6.1.3.2 or later. Changes introduced in ArubaOS 6.1.3.9 resolved this issue. The system now provides **default_role** and **user-derived_vlan** information in log messages.

Controller-Datapath

Table 18 *Controller-Datapath Issues Fixed in 6.1.3.7*

Bug ID	Description
75843	**Symptom:** Errors in the internal datapath module on a controller caused it to stop responding. The crash logs for this error listed the reason for the crash as **Datapath Timeout**. **Scenario:** This issue was observed when an M3 controller experienced heavy traffic between the control plane module and the network.
76307	**Symptom:** A local controller crashed after a user added a VLAN ID in the master controller. **Scenario:** When a user added a VLAN ID to the master controller and executed the command `write-mem`, the local controller crashed due to an internal process failure. This issue was not limited to any controller or software version.
77024 77535 77537	**Symptom:** The iOS, MacOS, and Android devices were blacklisted due to IP spoofing. **Scenario:** The iOS, MacOS, and Android devices sent ARP packets to receive the MAC address of the gateway to all the networks. When the previously connected networks assigned a leased out IP address to these devices and clients was blacklisted. This issue was observed in all the controller models running ArubaOS 6.1.3.6.
75428 76429 77814	**Symptom:** Errors in the control plane modules caused M3 and 3000 Series controllers to unexpectedly reboot with the message **reason: watchdog timeout**. **Scenario:** This issue was observed in M3 and 3000 Series controllers running ArubaOS 6.1.x.

Controller Platform

Table 19 *Controller Platform Issues Fixed in 6.1.3.7*

Bug ID	Description
62096	**Symptom:** M3 controllers may unexpectedly reboot with the reason `User Pushed Reset`. The issue was resolved by configuring VLAN bandwidth contracts to reduce the traffic to the control plane. **Scenario:** This issue was observed when there was high traffic between the control plane and the datapath.
72996	**Symptom:** When the ARM channel assignment was set to **maintain** mode, power changes were observed in APs after a reboot. Enhancements to the AP flash memory have resolved this issue. **Scenario:** This issue was observed in controller models running ArubaOS versions lower than 6.1.3.7.
74294	**Symptom:** The clients connected to a wired multiplexor from the same tunneled node used separate licenses, instead of using one license per tunneled node. **Scenario:** The clients connected to a wired multiplexor used one AP license per host when the number of AP licenses reached 511. The issue was observed in ArubaOS 6.1.3.4 and later versions, and was not specific to any controller model.
74842	**Symptom:** The 600 Series, 3200, and 3600 controllers reboot due to an internal fatal error in the operating system. **Scenario:** This issue was caused by a deadlock in the inter-CPU messaging system and has been resolved. This issue was observed in 600 Series, 3200, and 3600 controllers running ArubaOS 6.1.3.1.
74857	**Symptom:** The M3 and 3000 Series controllers reboot unexpectedly. **Scenario:** This issue was observed in M3 and 3000 Series controllers running ArubaOS 6.1.2.4 or later. The M3 and 3000 Series controllers reboot stating `User Pressed Reset` or `Kernel Panic` as the reboot cause.
75232	**Symptom:** An internal system error occurred in the M3 controller and APs failed to connect to the controller. **Scenario:** The issue was observed in large deployments, where the size of the config file was more than 360 KB, and there were large number of references to one profile instance. Due to this there was an internal system error, and the APs were unable to connect to the controller. This issue was observed in ArubaOS 5.0.4.6 and was not specific to any controller.

IPsec

Table 20 *IPsec Issues Fixed in 6.1.3.7*

Bug ID	Description
76301	**Symptom:** An AP continuously rebootstrapped. The output of the `show ap debug system-status` command listed the reason for the rebootstrap as **Send failed in function sapd_keepalive_cb**. **Scenario:** This issue was observed both in campus APs (CAPs) and in Remote APs (RAPs) with IPsec tunnels to the controller.

Management Authentication

Table 21 *Management Authentication Issues Fixed in 6.1.3.7*

Bug ID	Description
75466	**Symptom:** The clients were assigned incorrect roles during management authentication. **Scenario:** An upgrade from ArubaOS 6.1.2.8 to 6.1.3.5 caused the `NAS-Port-type` parameter to be set to `wireless` instead of `virtual`. Due to this, the remote policies were not applied and the clients were assigned incorrect privileges. This issue was not specific to any controller model or software version.
75665	**Symptom:** A 3rd generation iPad running iOS 6.0.1 was incorrectly assigned to the default VLAN. **Scenario:** This issue was observed in ArubaOS 6.1.3.5, when a Virtual AP was configured as follows: (1) both MAC authentication and 802.1X authentication, (2) a VLAN derivation rule was configured on the MAC authentication server, and (3) the derived VLAN was different from the default VLAN of the VAP.

Port-Channel

Table 22 *Port-Channel Issues Fixed in 6.1.3.7*

Bug ID	Description
75044 75977	**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 in all controller models running ArubaOS 6.1.3.5.

Radius

Table 23 *Radius Issues Fixed in 6.1.3.7*

Bug ID	Description
71836	**Symptom:** A controller sent incorrect class attributes to a RADIUS server, causing that server to show incorrect user statistics. Changes in how the controller sends class attributes in accounting requests have resolved this issue. **Scenario:** This issue was observed when multiple users with the same MAC address tried to connect to the controller using a wired connection.

RAP-3G (Remote APs with USB 3G wireless cards)

Table 24 *RAP-3G Issues Fixed in 6.1.3.7*

Bug ID	Description
50143	**Symptom:** A Remote AP could not set up EVDO successfully after a failover from a PPPoE link. **Scenario:** This issue was observed in Remote APs configured with EVDO and PPPoE links during a link failover. Specifically, it was observed in controllers running ArubaOS 6.1 or later.
73752	**Symptom:** A Remote AP could not failover to the 3G modem link when the PPPoE connection failed. **Scenario:** Initially the Remote AP was connected using a PPPoE connection and cellular links. When the PPPoE connection failed, the Remote AP did not failover to the 3G modem link. After some internal configuration changes, the Remote AP came up using the 3G modem. However, when the PPPoE connection was restored, the Remote AP did not switch from the 3G modem to the PPPoE connection. This issue was observed in all controller models running ArubaOS 5.0.4.5.

Role/VLAN Derivation

Table 25 *Role/VLAN Derivation Issues Fixed in 6.1.3.7*

Bug ID	Description
74705 75918	**Symptom:** Inconsistent VLAN derivation was observed when User Derivation Rules (UDR) or Server Derivation Rules (SDR) was configured. **Scenario:** When multiple UDR or SDR rules were configured, a client was assigned an incorrect VLAN. This issue was observed in controllers running ArubaOS 6.1 or later.
76428	**Symptom:** Users get reassigned to an incorrect user role. This issue was fixed by implementing a check for this scenario, and prevents the correct user role from being overwritten. **Scenario:** Users assigned a user role using DHCP fingerprinting and authenticated using an external Captive Portal may be later be assigned an incorrect user role when the client sends a DHCP renew packet. This issue was observed in ArubaOS 6.1.3.5, and is not specific to any specific controller model.

Security

Table 26 *Security Issues Fixed in 6.1.3.7*

Bug ID	Description
72843	**Symptom:** An issue has been fixed where slower network performance and response times occurred with 6000 and 3000 Series controllers. **Scenario:** The issue was observed in ArubaOS 6.1.3.2 in networks that support mostly client-to-client traffic.

XML API

Table 27 *XML API Issues Fixed in 6.1.3.7*

Bug ID	Description
67898	**Symptom:** Although the client accounts were deleted, the clients could connect to the Wireless Network. **Scenario:** Some of the P2P sessions for the account existed even after a client account was deleted. Due to this, the deleted clients were able to access the wireless network. The issue was observed in ArubaOS 6.1.3.7 and was not specific to any hardware model.

Fixed in 6.1.3.6

802.1X

Table 28 *802.1X - Fixed Issues in 6.1.3.6*

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 observed in ArubaOS 6.1.3.5.

Table 28 *802.1X - Fixed Issues in 6.1.3.6 (Continued)*

Bug ID	Description
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 observed in controllers running ArubaOS 6.1.3.2.

Air Management

Table 29 *Air Management - Fixed Issues in 6.1.3.6*

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 observed in 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 30 *AP Regulatory - Fixed Issues in 6.1.3.6*

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 observed in 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 observed in 3600 controllers running ArubaOS 6.1.3.4 or later.

AP Wireless

Table 31 *AP Wireless - Fixed Issues in 6.1.3.6*

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 fixed by a software change that defers transmission power or channel changes if any frames are pending. **Scenario:** This issue was observed in APs that aggressively scan outside home channels.

Table 31 *AP Wireless - Fixed Issues in 6.1.3.6 (Continued)*

Bug ID	Description
65984	**Symptom:** Random AP rebootstrapping was observed along with poor WLAN performance and a ping issue. This issue was fixed 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 was fixed 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 was fixed 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 fixed 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 32 *Authentication - Fixed Issues in 6.1.3.6*

Bug ID	Description
50192 61935 66647 67620	**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 was fixed. **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 was fixed 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 observed in the configuration file. This issue was not limited to any specific controller model.
72587	**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 32 *Authentication - Fixed Issues in 6.1.3.6 (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 in controllers running ArubaOS 6.1 or later.

BaseOS Security

Table 33 *BaseOS Security - Fixed Issues in 6.1.3.6*

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 fixed 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 33 *BaseOS Security - Fixed Issues in 6.1.3.6 (Continued)*

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 fixed 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 observed in ArubaOS 6.1.3.4, and is not limited to any specific controller model.
75754	**Symptom:** The user table no longer shows that some 802.1X authenticated clients managed by an external XML-API server are using Web authentication, even though there is no captive portal authentication configured for those clients. The user table now shows the correct status. **Scenario:** This issue occurred on a controller configured with an 802.1X default role with an ACL that sends traffic through the GRE tunnel to a SafeConnect appliance. In this scenario, L3 authentication is managed by the SafeConnect XML API, which updates the user role to an L3-authenticated role.

Controller-Datapath

Table 34 *Controller Datapath - Fixed Issues in 6.1.3.6*

Bug ID	Description
69102 66798 68829	**Symptom:** Users experienced low throughput after enabling a bandwidth contract. This issue was fixed by an increase in the queue size for lower contract rates. **Scenario:** This issue was observed when contract rates less than 1 Mbps were applied to bandwidth contracts on controllers running ArubaOS 6.1.3.0.
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 occurred 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 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.
75137	**Symptom:** Wireless clients could not communicate with a multicast router. **Scenario:** This issue was seen when the multicast router was using a VLAN without a configured IP address.

Controller Platform

Table 35 *Controller Platform - Fixed Issues in 6.1.3.6*

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.

IPsec

Table 36 *IPsec - Fixed Issues in 6.1.3.6*

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 have resolved this issue. **Scenario:** This issue occurred in an M3 controller in a master-local topology, where the M3 master controller was running ArubaOS 6.1.3.2.

Mesh

Table 37 *Mesh - Fixed Issues in 6.1.3.6*

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 works correctly before ENET0 becomes active. **Scenario:** This issue was observed in an AP-93H configured as a mesh point in which ENET0 is not connected.

RADIUS

Table 38 *RADIUS - Fixed Issues in 6.1.3.6*

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 39 *Remote Access Point - Fixed Issues in 6.1.3.6*

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 40 *Role/VLAN Derivation - Fixed Issues in 6.1.3.6*

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 41 *Startup Wizard - Fixed Issues in 6.1.3.6*

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 42 *Station Management - Fixed Issues in 6.1.3.6*

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.

Voice

Table 43 *Voice - Fixed Issues in 6.1.3.6*

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 observed in controllers running ArubaOS 6.1.3.0.

VPN

Table 44 *VPN - Fixed Issues in 6.1.3.6*

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 fixed 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 45 *WebUI - Fixed Issues in 6.1.3.6*

Bug ID	Description
67304	**Symptom:** A user was unable to provision an AP-61 as a RAP (Remote Access Point) 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.

Fixed in 6.1.3.5

Air Management - IDS

Table 46 *Air Management - IDS Issue Fixed in 6.1.3.5*

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 observed 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 47 *AP Issues Fixed in 6.1.3.5*

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	An 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.

Table 47 *AP Issues Fixed in 6.1.3.5*

Bug ID	Description
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 observed in ArubaOS 6.1.3.2 and 802.11n APs.

Authentication

Table 48 *Authentication Issues Fixed in 6.1.3.5*

Bug ID	Description
69840	An issue was observed where the EAP-TLS authentication failed when new certificates were used by clients to connect to a network.
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 49 *Captive Portal Issue Fixed in 6.1.3.5*

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

Configuration

Table 50 *Configuration Issue Fixed in 6.1.3.5*

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 51 *Hardware Management Issue Fixed in 6.1.3.5*

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 52 *Interface Issue Fixed in 6.1.3.5*

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 53 *IPsec Issue Fixed in 6.1.3.5*

Bug ID	Description
71991	An issue was fixed relating to memory management in a controller processing public keys. In ArubaOS 6.1.1.0, this issue created a memory leak that caused a reset of the controller process that handles IKE exchanges for remote APs, VPNs, and APs using control plane security.

IPv6

Table 54 *IPv6 Issue Fixed in 6.1.3.5*

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 was observed when the `ipv6 mld snooping` command was enabled on the VLAN interface.

Mesh

Table 55 *Mesh Issue Fixed in 6.1.3.5*

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 56 *Mobility Issue Fixed in 6.1.3.5*

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 observed in 3200 controller running ArubaOS 6.1.3.3.

M-Switch Software

Table 57 *M-Switch Issue Fixed in 6.1.3.5*

Bug ID	Description
67847	An issue was fixed relating to an unexpected reboot of an AP-125 due to a databus error.

Platform/Datapath

Table 58 *Platform/Datapath Issues Fixed in 6.1.3.5*

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 was fixed where the status of the NTPD module was busy on controllers running ArubaOS 6.1.2.4.

Port-Channel

Table 59 *Port-Channel Issue Fixed in 6.1.3.5*

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. 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 a blocked state. This issue was observed in controllers running ArubaOS 6.1 when a port-channel was configured and spanning tree was enabled.

RADIUS

Table 60 *Radius Issue Fixed in 6.1.3.5*

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 6.1.3.9, the controller re-transmits the failed STOP accounting messages to the ClearPass Guest server.

Remote AP

Table 61 *Remote AP Issues Fixed in 6.1.3.5*

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 observed 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, which is 3G/4G. This is observed 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 that is 3G/4G. This is applicable only when the remote AP is provisioned to use UML290 as an uplink connection.

Security

Table 62 *Security Issues Fixed in 6.1.3.5*

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 observed 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 802.1X 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 observed 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 fixed where a large number of `Dropping EAPOL packet` and `EAP-ID mismatched` entries were observed 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 fixed 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 63 *SNMP Issue Fixed in 6.1.3.5*

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 64 *Station Management Issues Fixed in 6.1.3.5*

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.
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 observed 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 65 *WebUI Issues Fixed in 6.1.3.5*

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 issue 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 66 *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).
66476 66477	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.

Table 66 *Access Points Issues Fixed in 6.1.3.4 (Continued)*

Bug ID	Description
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 67 *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 fix will lower the CPU utilization related to gathering certain types of information from the database. This issue was observed on all controllers for ArubaOS 5.0.x to 6.1.3.3.

DHCP

Table 68 *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. The fix allows the controller to send the user VLAN IP address as the source IP.

Guest Provisioning

Table 69 *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 70 *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 was observed in the 600 series, 3200, 3400, 3600 and M3 controllers running ArubaOS 6.1.3.4 and earlier.

Other

Table 71 *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 72 *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/M3 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.
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. 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 observed 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 occurred when there were a large number of VRRP instances.
68277	An issue where the `halt` command accidently displayed panic messages in controllers (3000 Series/M3 controllers) 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 73 *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.

RADIUS

Table 74 *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 75 *Remote AP Issues Fixed in 6.1.3.4*

Bug ID	Description
57637 57639	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. The message now correctly shows up in the debug logs and no longer appears in the error logs.
68637	An issue was fixed 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 76 *Security Issues Fixed in 6.1.3.4*

Bug ID	Description
68336	An issue was fixed 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 77 *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 78 *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*.
67737 73194	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 79 *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.
64017 69608	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 80 *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 81 *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.
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.
59611	An unexpected reboot that occurred on all 802.11n APs (except the AP-135) due to an internal process malfunction was fixed.
62110	A remote AP's power LED no longer turns off after a while when there is no Ethernet connection.
59343 62245	802.1X 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 fixed 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.

Table 81 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
64874	An issue was fixed 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	An issue was fixed that caused the AP-65/AP-61 to reboot under high-traffic scenarios due to memory corruption.
62556 65344 65973	APs no longer prematurely reboot before a TFTP transfer of ArubaOS is completed.
65593	APs do not crash and reboot occasionally when a UAPSD (Unscheduled Automatic Power Save Delivery) enabled client is connected to the AP.
65869	An issue was fixed 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	An issue was fixed where an AP-135 terminating on a local controller reboots due to a crash.
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.
66246	As issue was fixed regarding interoperability between Cisco 7921/7925 and the 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 was fixed where the packet loss rate on 802.11n APs was high and unstable. This was caused by a problem in the packet retry mechanism. **Workaround**: 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.

Table 81 *Bugs Fixed in 6.1.3.2 (Continued)*

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

Table 81 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
59375	If guest account expiry date/time is not set, then the controller honors the maximum account expiry time window setting in the internal database.
60534	Root/Admin users can now create a guest user entry with an expiration date beyond the maximum account expiry time window setting in the internal database.
54249	The 4-way 802.1X 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.
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 was fixed 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 was fixed through improved validation of OSPF Link-State Advertisements (LSAs) in traffic packet headers.
49325	An issue was fixed 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 was fixed 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	An issue was fixed where 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.
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 was fixed 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.

Table 81 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
61101	An issue was fixed where a 651 controller unexpectedly rebooted due to a memory allocation failure during a low memory state.
62484	An issue was fixed with a controller reboot that occurred when `write mem` was executed from the CLI or WebUI shortly after a license was added. Note that in some cases the controller does not reboot but experiences 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 was fixed where APs rebootstrap due to excessive ARPs in the network. Optimizations have been implemented in the controller to mitigate this.
62818	An issue was fixed where user entries were not deleted from the user table even after the clients were disconnected from the network. This caused IP spoofing issues as the DHCP server allocated IP addresses of the disconnected clients to the newly connecting clients in the network.
63386	An issue was fixed with regard to control messages between the controller and its APs, which 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.
63843	An issue was fixed 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. Practice note: 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 was fixed where the controller rebooted due to memory buffer depletion caused by heavy IPv6 and user traffic.
65349	An issue was fixed where 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.
65499	An issue was fixed 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 was fixed where the standalone master controller crashed due to malformed multicast Microsoft Network Load Balancer packets. This issue was observed in 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.

Table 81 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
63052	Clients using a PPTP-based Virtual Private Network (VPN) to connect to a controller enabled with the AAA fast-age feature are no longer incorrectly assigned a logon user role. This resolves an issue that prevented PPTP clients from authenticating and receiving their correct user role.
57005	Incorrect traffic counters reported by a RADIUS *Accounting Stop* message after a user session is terminated was fixed.
55311	An issue was fixed with aging out IPv6 entries of dual stack clients sending incorrect *RADIUS accounting stop* messages for IPv4 entries.
62337	An issue was fixed with AP-Group and AP-Location-Id fields in RADIUS requests being empty for wired users connected to a remote AP.
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.
59019	An issue was fixed where remote APs behind a firewall did not reconnect to the controller after a firewall restart.
62226	The number of IPsec retries in PPPoE remote APs are equal to number configured in the `number_ipsec_retries` field.
62733	An 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	An issue was fixed with slower upgrades and remote AP reboots 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.

Table 81 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
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.
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	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	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. See also entry for Bug ID 53218.
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.

Table 81 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
52186	Interface statistics now display 64-bit counter values when a user polls both *ifHCIn0ctets* and *ifHC0ut0ctets* OIDs on an M3 controller. This bug was due to 32-bit counters based implementation that resulted in incorrect values.
67190	An issue was fixed 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.
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 was fixed 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 was fixed 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	An issue was fixed regarding WebUI, where the configuration for mapping the access-group to the cellular interface was not saved in the **Configuration** > **Network** > **Ports** > **Cellular** page.
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	An issue was fixed where the user was not able to configure the CHAP secret along with the PAP username in the WebUI.

Table 81 *Bugs Fixed in 6.1.3.2 (Continued)*

Bug ID	Description
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	An issue was fixed where it was not possible to access the **Controller** > **AP** > **Status** page using Internet Explorer 8, due to a JavaScript error.
64566	An issue was fixed where the WebUI failed to locate rogue APs after upgrading to ArubaOS 6.1.3.0. 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 now be tested on the **Diagnostics** > **Network** > **AAA test server** page.
66230	An issue was fixed with usability issues in the WebUI with respect to the **Edit** and **Delete** buttons corresponding to the AP Groups in the **Configuration** > **WIRELESS** > **AP configuration** > **AP Group**. Click on the **ap-group name** link to edit the ap-group and the **Delete** button to delete the ap-group.
67091	Extremely long user names caused the **Dashboard** > **Client** page to display a blank page due to a JavaScript error. It is recommended that user names should not exceed 64 characters.
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 82 *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 was fixed where RX frames which were not mapped to an RX descriptor could cause an AP to unexpectedly reboot.
62391	An issue was fixed wherein an AP would unexpectedly reboot. Improvements to the RX queue access resolved this issue.
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 was fixed where clients were intermittently unable to connect to an AP-135 and once connected, experienced slow throughput.
64576	Enabling EAPOL optimization no longer reduces the number of retries of EAPOL frames.
60152	Clients sending user credentials to the AP before the “Interval between Identify requests” wait time defined in the 802.1X authentication profile could not complete 802.1X authentication after association.
64322	Users coming through a 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 an 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.

Table 82 *Bugs Fixed in 6.1.3.1 (Continued)*

Bug ID	Description
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 55123 57512	Resolved an SNMP issue triggered by internal user IP address lookup.
62455	The ifIndex value returned by the IP table during an SNMP walk on a 620 controller correctly matches the MIB value returned in the ifDescr table.
61259 61261	A new configuration setting has been added to enabled or disable Domain Pre-connect under the VIA connection profile.
63521	Audio and Video sessions with the same session ID no longer cause the STM module to stop responding after both sessions age out.

Fixed in 6.1.3.0

Table 83 *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.
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.

Table 83 *Bugs Fixed in 6.1.3.0 (Continued)*

Bug ID	Description
52825 53897 53365 55118 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.
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.

Table 83 *Bugs Fixed in 6.1.3.0 (Continued)*

Bug ID	Description
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.
55003 55202	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.
53904 53984 63277	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 62477 62468 62502	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 54231 55620 56561 56928 57302 61152 61155	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.
60373	Improvements to SOS crash dump collection allow datapath crashes to recover more quickly.
60431 63006	Issuing the CLI command show trunk no longer causes the **fpapps** module to stop responding when the controller includes a large number of non-contiguous VLANs.

Table 83 *Bugs Fixed in 6.1.3.0 (Continued)*

Bug ID	Description
46116	The TCP maximum segment size for TKIP tunnels has been reduced to better accommodate the WEPCRC length.
58502	Packets are now sent from the trunk port on the controller to a client on the trunk port behind a remote AP with a proper VLAN tag.
52845	Proxy-arp now provides support for split-tunnels.
54191 55794	FTP data transfer and reuse of a stray session no longer triggers a race condition and datapath timeout exception.
54943	Users are now able to get IP address on VMware Fusion.
52092	Client with .255 IP address can now ping across 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 62006 62102 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 an initial user role of **denyall** (any any any deny), even if the wireless adapter on the client is disabled then reenabled.
60167	If PPPoE remote APs using certificates and IKEv2 have a static inner IP addresses but then later change their outer IP address or port during rebootstrap, the inner IP route is retained when the remote APs establish a new IKE SA to the controller.
61000	Improvements to the handling of HELLO packets allow remote APs to be able to properly associate to their controller upon upgrading to ArubaOS 6.1.3.

Table 83 *Bugs Fixed in 6.1.3.0 (Continued)*

Bug ID	Description
60458	An issue was fixed where a remote AP mesh portal with wired bridging was failing. The customer required a LAN extension by using the enet port of a mesh point to locally bridge through the 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.
58895	Applying a "noe-acl" no longer causes RTP packets to be dropped for IP Touch 310/610 phones.

Table 83 *Bugs Fixed in 6.1.3.0 (Continued)*

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

Chapter 5

Known Issues observed in Previous Releases

This chapter describes the known issues and limitations observed 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 may cause 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

Authentication

Table 2 *Authentication Known Issues*

Bug ID	Description
50192 61935 66647 67620	**Symptom:** A user is not able to derive a VLAN from a user derived rule based on DHCP fingerprinting due to errors in the internal key exchange process. **Scenario:** This issue occurs in controllers running Dell Networking W-Series ArubaOS 6.1 or later when the SSID uses 802.1X authentication. **Workaround:** None.

Controller Datapath

Table 3 *Controller Datapath Known Issues*

Bug ID	Description
81082	**Symptom:** Connectivity failure occurs between the master and local controllers in a master-local topology. This failure occurs after replacing a layer-3 switch that is configured as a gateway and connected to a master controller. **Scenario:** When the gateway (layer-3 switch) is replaced, all the route cache entries update with the MAC address of the new gateway. However, the IPSec-route-cache entry shows the MAC address of the old gateway. This issue is observed in ArubaOS 6.1.3.5. **Workaround:** Use a virtual IP such as Virtual Router Redundancy Protocol (VRRP) or Hot Standby Router Protocol (HSRP) in the gateway of the controllers to avoid this issue. Execute the command `clear arp all` from the Command Line Interface (CLI) to recover if this issue is occurred.

Controller Platform

Table 4 *Controller Platform Known Issues*

Bug ID	Description
81555	**Symptom:** A controller crashes and reboots after upgrading the software from ArubaOS 6.1.3.6 to 6.1.3.7. The log files for the event listed the reason for the crash as **watchdog timeout**. **Scenario:** In a high traffic deployment, a race condition may trigger a controller crash and this issue is not specific to any controller models. **Workaround:** None.

Mobility

Table 5 *Mobility Known Issues*

Bug ID	Description
75093 81716	**Symptom:** The `show ip mobile host` command displays the roaming status of a client as **No state** instead of **Home Switch/Home VLAN** and does not release the host entry. **Scenario:** This issue occurs when L3-mobility is enabled on controllers running any version of ArubaOS. **Workaround:** None.
82673	**Symptom:** Clients are not able to obtain an IP address using Dynamic Host Configuration Protocol (DHCP) intermittently when a user roams between controllers with layer-3 (L3) mobility enabled. **Scenario:** DHCP packets from a client get redirected into an IP-in-IP (IPIP) tunnel due to an incorrect order of Access Control List (ACL) on the foreign agent controller. This issue occurs when L3 mobility is enabled on the controller with clients using DHCP to obtain an IP address. This issue was observed in ArubaOS 6.1.X and 6.2.X. **Workaround:** None.
82971	**Symptom:** Traffic from user VLAN overflows into management VLAN and this causes other switches in the same domain to learn the user MAC address on management VLAN. **Scenario:** Layer-2 (L2) broadcast/multicast packets from a client are placed into home VLAN based on route lookup on the client. When the user VLAN is an L2 VLAN, the route lookup results in the controller's default gateway and hence the user VLAN traffic is overflowing into default gateway VLAN. This issue occurs when L3 mobility is configured and L2 user VLANs are extended on the controllers. This issue was observed on ArubaOS 6.1.3.5 and earlier. **Workaround:** Configure the IP address on the user VLAN to avoid this issue.

Access Point

Table 6 *Access Point Known Issues and Limitations*

Bug ID	Description

57624	**Symptom:** AP-105 access points might not come up when connected to a Cisco PoE switch (WS-C6509-E:WS-X6148A-GE-45AF).
	Scenario: 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.`
	Workaround: None.

Table 6 *Access Point Known Issues and Limitations (Continued)*

Bug ID	Description
57925 60722 60846 61100 61196 61539 63460 64517 64526 65049 66118 66128 66136 66185 66409 66659 67435 67670 67671 67673 67871 67872 67977	**Symptom:** Aruba 651 controller might crash and result in unexpected reboot when the internal AP is enabled. **Scenario:** This issue occurs in controllers running ArubaOS 6.2.0.0. **Workaround:** Disable the radio on the internal AP of the Aruba 651 controller. To disable the radio for a specific AP, follow the instructions provided in “Aruba 651 Internal AP” on page 67.
64014	**Symptom:** When an AP rebootstraps due to loss of connection to a controller, a process on the AP crashes due to corrupted memory. **Scenario:** 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 observed in ArubaOS 6.1.3.0.
74984	**Symptom:** Blackberry devices have severe ping losses when connected to an AP configured to use a high throughput SSID. **Scenario:** This issue occurs on AP-135 running on ArubaOS 6.1.3.4 when support for a high throughput SSID is enabled in the AP's WLAN high-throughput SSID profile. **Workaround:** None.

Air Management - IDS

Table 7 *Air Management - IDS - Known Issues and Limitations*

Bug ID	Description
76558	**Symptom:** The ARM neighbor information that appears in the output of the **show ap arm neighbors** CLI command shows several unknown device BSSIDs on both radio bands. **Scenario**: This issue was observed in controllers running ArubaOS 6.0 or later with ARM enabled, and is triggered when BSSIDs used internally are mistakenly included in the ARM neighbor report. **Workaround:** None.

AP Platform

Table 8 *AP Platform - Known Issues and Limitations*

Bug ID	Description
74932	**Symptom:** Some APs are not operational and unable to receive configuration information from the controller for one hour, as both master and backup VRRP controllers are VRRP active simultaneously. **Scenario:** This happens when the VRRP heartbeats are lost due to high traffic on the VRRP VLAN. This issue was not specific to any controller or AP model or any specific software version. **Workaround:** None.
78282	**Symptom:** Clients running windows 7 clients do not connect in TKIP mode when static wep and wpa-psk-tkip are configured together in the SSID profile, but connected successfully in static wep mode. **Scenario:** This issue was observed in the windows 7 clients connecting to APs. Clients running windows XP were able to connect in both security modes. **Workaround:** None.

AP Wireless

Table 9 *AP Wireless - Known Issues and Limitations*

Bug ID	Description
76600	**Symptom:** APs disconnect because the radio stopped working. **Scenario:** This issue was observed in an AP-105 running ArubaOS 6.1.x.x. **Workaround:** Clear the **Spectrum Monitoring** check box under **RF Management > 802.11a radio** on the **Profile Details** page of the WebUI.
76629	**Symptom:** When the Wireless Multi-Media (WMM) feature is enabled, APs send encapsulated frames with an outer DSCP value of 24, even though the inner IP header has a DSCP value of 0. **Scenario:** This occurs when WMM is enabled in the SSID profile. Since WMM client traffic falls into an incorrect queue because of incorrect DSCP marking, the uplink switch restricts user traffic to policed throughput. This issue was observed in ArubaOS 6.1.3.1and was not limited to a specific AP or controller model. **Workaround:** Disable QoS policing on the uplink switch, so throughput for WMM clients returns to normal.
78872	**Symptom:** Wireless clients associated to an AP in bridge forwarding mode do not connect when dynamic-WEP and WPA-TKIP are configured together. However, the same mixed-mode combination works fine in tunnel mode. **Scenario:** This issue was observed, in both WEP and TKIP modes, in Windows 7 and Windows XP clients trying to connect to APs configured with bridge forward mode Virtual APs (VAPs). **Workaround:** None.

ARM

Table 10 *ARM Known Issues and Limitations*

Bug ID	Description
62878	**Symptom:** 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. **Scenario:** This issue occurs in controllers running ArubaOS 6.1.0.0. **Workaround:** None.

Authentication

Table 11 *Authentication Known Issues and Limitations*

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 observed 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 observed in controllers running ArubaOS 6.0.0.0 or later with 802.1X configured and machine authentication enabled. **Workaround:** Remove the VLAN from the 802.1X authenticated role and machine authentication.

Table 11 *Authentication Known Issues and Limitations (Continued)*

Bug ID	Description
70343	**Symptom:** Custom captive portal (CP) pages are not synchronized between the master and standby controllers. **Scenario:** 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. **Workaround:** None.
75832	**Symptom:** EAP-TLS authentication fails for the MAC clients connected to a Remote AP in split-tunnel mode. **Scenario:** This issue is observed in controller running ArubaOS 6.1.2.6. **Workaround:** None.
77490	**Symptom:** Phones disconnect when **band steering** is enabled for a virtual AP profile in the WebUI. **Scenario:** When band steering is enabled, devices such as Samsung GS3 phones disconnect from the network, and display an **authentication error** message in the Wi-Fi settings of the phone. **Workaround:** Clear the **Band Steering** check box under the **Virtual AP** profile on the **Profile Details** pane of the WebUI.

BaseOS Security

Table 12 *BaseOS Security Known Issues and Limitations*

Bug ID	Description
76958	**Symptom**: The user table displays incorrect information for a management user when that user completes 802.1X authentication with a RADIUS server, then logs in to the controller using the same user account. **Scenario:** This issue was observed in M3, 3000 Series, and 600 Series controllers running ArubaOS 6.1.3.6. **Workaround:** None.

Controller-Datapath

Table 13 *Controller-Datapath - Known Issues and Limitations*

Bug ID	Description
77247	**Symptom:** Upload and download rates achieved with bandwidth contracts of less than 1 Mbps are inaccurate. Accuracy improves with bandwidth contracts higher than 1 Mbps. **Scenario:** This issue was observed in a controller running ArubaOS 6.1.3.5 with a bandwidth contract limiting use to 512 kbps of bandwidth. **Workaround:** None.

Controller Platform

Table 14 *Controller Platform Known Issues and Limitations*

Bug ID	Description
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.
76673	**Symptom:** The M3 Mobility Controller keeps rebooting with the **Reboot Cause: Mobility Processor update** reboot message. **Scenario:** The M3 Mobility Controller keeps rebooting when the primary and secondary partitions are running different versions of ArubaOS (5.0.3.3 and 6.1.3.4) that support different FPGA (Field-Programmable-Gate-Array) images. When ArubaOS reboots the controller from the secondary partition due to an internal fatal error, an FPGA image mismatch is found. This causes the controller to reboot for a processor update. **Workaround:** if the controller reboots due to an internal fatal error, then use the same versions of ArubaOS on both primary and secondary partitions of the Mobility Controller to avoid FPGA image mismatch between partitions.
76447	**Symptom:** The M3 controller reboots and crashes following a Kernel Panic. **Scenario:** This issue was observed in M3 controllers running ArubaOS 6.1.3.5 topology, where the controller acts as a local controller. A corrupt pointer in the kernel is identified as the cause of this issue. **Workaround:** None.

Table 14 *Controller Platform Known Issues and Limitations (Continued)*

Bug ID	Description
77155	**Symptom:** The controller reboots and fails to complete the boot process. **Scenario:** This happens due to an NVRAM write failure while updating the reboot reason and boot partition. This issue was not specific to any controller model. **Workaround:** None.
77623	**Symptom:** The captive portal page does not open in the master controller. **Scenario:** This issue was observed when more than 250 users are connected to the captive portal SSID. The issue was not specific to any controller or software version. **Workaround:** None.

DHCP

Table 15 *DHCP Known Issues and Limitations*

Bug ID	Description
69145	**Symptom:** Starting with ArubaOS 6.1.3.2, if a controller supports clients behind a wireless bridge or virtual clients on VMware devices, you must disable the **broadcast-filter arp** setting from IPv4 Firewall Parameters to allow those clients to obtain an IP address. **Scenario:** This issue occurs on all controller platforms running ArubaOS 6.1.3.2. **Workaround:** None.

802.1X

Table 16 *802.1X Known Issues and Limitations*

Bug ID	Description
74663	**Symptom:** Clients are not able to reauthenticate after rebooting or logging off the networks. **Scenario:** This issue was observed in 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 17 *IPv6 Known Issues and Limitations*

Bug ID	Description
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.

Management Auth

Table 18 *Management Auth Known Issues and Limitations*

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 in 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.

Mobility

Table 19 *Mobility Known Issues and Limitations*

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 observed 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.
74272	**Symptom:** 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. **Scenario:** This issue is observed 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 20 *Platform/Datapath Known Issues and Limitations*

Bug ID	Description
63140	**Symptom:** 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. **Scenario:** The timeout occurred when aaa user delete was executed to change bandwidth contract and change of user role. **Workaround:** None.

RADIUS

Table 21 *RADIUS - Known Issues and Limitations*

Bug ID	Description
76336	**Symptom:** Clients get a DHCP IP even though DHCP is denied in the user role. **Scenario:** When the AAA profile is configured with MAC authentication, and if the 802.1X authentication profile is configured without a server group, the default-role (logon) is applied to the user-traffic upon failure of MAC authentication. As the default role allows DHCP, the users end up getting a DHCP IP. This issue was observed in all APs running ArubaOS 6.1.3.4. **Workaround:** If the server group is not configured, then remove the 802.1X authentication profile configuration from the AAA profile.

Security

Table 22 *Security - Known Issues and Limitations*

Bug ID	Description
76905	**Symptom:** MacBooks running 10.7 and 10.8, disconnect from the 802.1X SSID intermittently. **Scenario:** This issue was observed when a MacBook client is roaming between radios of the same AP but with a different ESSID. This results in L2/L3 user deauthentication followed by reauthentication. Upon reauthentication, the MacBook client successfully joins the correct 802.1X. This issue was observed in controllers running ArubaOS 6.1.3.5 or later. **Workaround:** Turn the radio OFF and then ON to reconnect.

SNMP

Table 23 *SNMP Known Issues and Limitations*

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

Station Management

Table 24 *Station Management Known Issues and Limitations*

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.

Table 24 *Station Management Known Issues and Limitations (Continued)*

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 controllers do not find the entry in the bridge lookup result. **Workaround:** Disable VLAN mobility and preserve VLAN.

Voice

Table 25 *Voice Known Issues and Limitations*

Bug ID	Description
71202	**Symptom:** The SIP ALG did not prioritize the SIP media ports which results in poor traffic quality and disconnections due to frame loss or delay. **Scenario:** This issue is observed in controllers running ArubaOS 6.1 with SIP clients configured to use video capability. **Workaround:** None.
77716	**Symptom:** Incompatibility issues observed between an Aruba 3600 controller and a Cisco CUCM. A Cisco phone can make and receive calls but there is no audio. **Scenario:** This issue was observed in a 3600 controller running ArubaOS 6.0 or later. The Cisco CUCM is compatible with the Skinny Client Control Protocol (SCCP) version 20, while the 3600 controller supports only up to version 16 of the SCCP. This incompatibility issue results in traffic not passing through the 3600 controller. **Workaround:** Configure the **allow-all** option for **voice-role** using the CLI. Alternatively, through the WebUI, you can configure the **allow-all** policy in **Security > Access Control > User Roles**, by changing the **voice User Role** and setting the firewall policy to **allow-all**.

WebUI

Table 26 *WebUI Known Issues and Limitations*

Bug ID	Description
66521	**Symptom:** When creating a user in the WebUI, you see two **Apply** buttons in the **Configuration > Security > Authentication > Internal DB** page. **Scenario:** 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. **Workaround:** None.
75873	**Symptom:** An error message is displayed in the WebUI after enabling or disabling the user debug option. **Scenario:** After a user debug is enabled or disabled in the **Monitoring > Clients > Debug** page of the WebUI and the user debug is successful, the **Error enabling debugging for user** error message is displayed. This issue was observed in ArubaOS 6.1.3.4 and later and is not limited to any specific controller model. **Workaround:** None.

WMM

Table 27 *WMM Known Issues and Limitations*

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 in controllers running ArubaOS 6.1.3.6 or lower in Tunnel and Decrypt-Tunnel modes. **Workaround:** None.

Table 27 *WMM Known Issues and Limitations (Continued)*

Bug ID	Description
76776	**Symptom:** Poor voice quality and interoperability issues were observed between an Alcatel 310 device and an AP. **Scenario:** This issue was observed in the ArubaOS 6.1.3.5. This issue is not specific to any network topology, and occurs when the client tries to associate with controllers. **Workaround:** Upgrade the firmware on the Alcatel 310 device to version 120.028.

Issues Under Investigation

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

AP Platform

Table 28 *AP Platform- Observed Issues*

Bug ID	Description
75564	**Symptom:** An unexpected reboot has been observed with an AP-135 terminating on a controller running ArubaOS 6.1.3.3.

BaseOS Security

Table 29 *BaseOS Security - Observed Issues*

Bug ID	Description
75082	**Symptom:** A controller failed to properly detect or report a MAC/IP spoofing event.
77227	**Symptom:** An unexpected crash in the module that handles user authentication was observed in a 3600 controller running ArubaOS 6.1.3.5.

Controller Datapath

Table 30 *Controller Datapath - Observed Issues*

Bug ID	Description
73256 74050 75700 76731	**Symptom:** An unexpected timeout in an internal datapath process caused a controller to unexpectedly reboot.

Controller-Platform

Table 31 *Controller Platform - Observed Issues*

Bug ID	Description
77402	**Symptom:** The *fpapps* process crashes on M3 controllers. This issue was observed in M3 controllers running ArubaOS 6.1.3.5 and is under investigation.
76473 77536	**Symptom:** A local controller reboots and the log files for the event listed the reason as **User pushed reset**. This issue occurs in 3000 Series and 6000 controllers running any ArubaOS 6.x version. This issue may occur under a heavy load scenario, and is under investigation.
77522	**Symptom:** Some remote clients were not routed through an IPsec tunnel to the correct subnet in IPsec due to a route-cache error. This issue was observed in an M3 controller module running ArubaOS 6.1.3.6 in a master-local topology.
77597	**Symptom:** An M3 controller running ArubaOS 6.1.3.5 unexpectedly rebooted and the log files for the event listed the reason for the reboot as **user pushed reset**. The cause has not been identified.
77633	**Symptom:** An internal process module (datapath) crash was observed in a 3600 controller running ArubaOS 6.1.3.4. This caused the controller to reboot unexpectedly.

Hardware Management

Table 32 *Hardware Management - Observed Issues*

Bug ID	Description
77091	**Symptom:** The physical link goes down in a 620 controller during an ArubaOS upgrade. This issue was observed during an upgrade of ArubaOS from version 5.0.2.0 to 6.1.3.5, while the controller is in standalone master topology.

WebUI

Table 33 *WebUI - Observed Issues*

Bug ID	Description
76149	**Symptom:** In some cases, the **Dashboard > Client** page of the WebUI does not display the details for the device type. This issue was observed in controllers running ArubaOS 6.1.3.1 or later.
77933	**Symptom:** The Firewall rule count does not display correctly in the **Configuration > Security > User Roles > Edit Role <role_name>** page of the controller WebUI. This issue was observed in M3 controllers in a master-local topology running ArubaOS 6.1.3.5.

Chapter 6

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" on page 87
- "Memory Requirements" on page 88
- "Backing up Critical Data" on page 88
- "Upgrading in a Multi-Controller Network" on page 89
- "Upgrading to 6.1.x" on page 90
- "Downgrading" on page 94
- "Before You Call Technical Support" on page 96

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. 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 than 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 6.1.3.9, 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 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 88 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 88 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 88 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 88.

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 6.1.3.9:

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


CAUTION

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 89.)

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


CAUTION

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash available for an upgrade using the WebUI. For details, see "Memory Requirements" on page 88

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 6.1.3.9.

- 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 91 to install the interim version of ArubaOS, then repeat step 1–step 11 of the procedure to download and install ArubaOS 6.1.3.9.

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 91 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 6.1.3.9 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 practice is to select **Yes** to automatically reboot after upgrading. If you do not want the controller to reboot immediately, select **No**. Note however, that the upgrade 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 88 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 91. 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 6.1.3.9 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 88

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 6.1.3.9.

- 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 92 to install the interim version of ArubaOS, then repeat step 1–step 7 of the procedure to download and install ArubaOS 6.1.3.9.

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 91 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 6.1.3.9 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 6.1.3.9 (Digitally Signed - Production Build)
   Build number            : 36462
   Label                   : 36462
   Built on                : Fri Jul 12 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 88 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 6.1.3.9 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 6.1.3.9 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 88.
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 is displayed 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 6.1.3.9 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 6.1.3.9, the changes do not appear in RF Plan in the downgraded ArubaOS version.
   - If you installed any certificates while running ArubaOS 6.1.3.9, 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 6.1.3.9 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 6.1.3.9 (Digitally Signed - Production Build)
Build number            : 36462
Built on                : 2013-07-12 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, 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), the wireless NIC make and model number, the 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 by selecting the WebUI Maintenance tab or through 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.