

ArubaOS 6.2.1.2



Release Notes

Copyright

© 2014 Aruba Networks, Inc. Aruba Networks trademarks include , Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

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

Warranty

This hardware product is protected by an Aruba warranty. For more information, refer to the ArubaCare service and support terms and conditions.



www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Chapter 1	Release Overview	9
	Chapter Overview	9
	Release Mapping	9
	Supported Browsers.....	10
	Contacting Support	10
	10
Chapter 2	What's New in this Release	11
	Supported Channels and Country Domains.....	11
	Resolved Issues in ArubaOS 6.2.1.2	12
	AP Platform	12
	AP Wireless	13
	BaseOS Security	13
	Command Line Interface.....	13
	Control Plane Security (CPsec).....	14
	Controller Datapath.....	14
	Controller Platform	15
	Controller Software	15
	Dot1x.....	15
	Enhanced Voice-Data Optimized	16
	IPv6	16
	Mobility.....	16
	Online Certificate Status Protocol (OCSP).....	16
	RADIUS	17
	Voice SIP.....	17
	WebUI	17
	Upgrade Caveats.....	17
Chapter 3	Features Added in Previous Releases	19
	Upgrading the New Software Image Scheme	19
	AP Capacity Per Controller.....	19
	Hardware Platforms.....	20
	7200 Series Controller.....	20
	RAP-108 and RAP-109 Remote Access Points.....	20
	RAP-3WN and RAP-3WNP Remote Access Points.....	20
	Remote Nodes Feature	20
	LLDP	21
	Spectrum Analysis.....	21
	Improved Visibility in the 5 GHz Radio Band	21
	Spectrum Analysis RFPlayback Tool	21
	Increased AP Support for Spectrum Analysis.....	22
	Platform	22
	Controller Capacity Alerts	22
	ARM Scanning Enhancements	23
	Timestamps in CLI Output	23
	Support for New Version of ETSI DFS standard	24

Enabling FCC DFS channels	24
Regulatory adjustments	24
Support for Single-Chain Mode	24
L2/L3 VLAN Scalability Requirements	26
Enhancement to WMM-DSCP Mapping	26
New Wizard Enhancements	26
Controller Wizard	26
Campus Wizard	26
WebUI Profile Usability Enhancements	26
Policy Enforcement Firewall (PEF) Visibility	27
Security	27
Enabling Bandwidth Contract Support for RAPs	27
DHCP Exhaustion Prevention	28
RAP Serviceability Enhancements	28
Captive Portal Enhancements	28
Inter-Controller IP Mobility Support on L2-GRE Tunnel	29
RAP 3G/4G Backhaul Link Quality Monitoring	29
New MIB Enhancements	29
LLDP MIBs	29
RAP Instrumentation for Airwave Monitoring	29
Aruba Products sysObject IDs	30
User Idle Timeout Behavior Change	30
Changes to Hardware Support	31
651 Controller	31
3200 Controller	31

Chapter 4

Issues Fixed in Previous Releases	33
Resolved Issues in ArubaOS 6.2.1.1	33
802.1X	33
Air Management - IDS	33
AMON	33
AP Platform	34
AP Regulatory	34
AP Wireless	34
ARM	35
BaseOS Security	
Control Plane Security (CPsec)	36
Controller Platform	37
MAC-Based Authentication	37
Mesh	38
Mobility	38
Remote AP	38
Role/VLAN Derivation	39
Spectrum-Infrastructure	39
WebUI	40
Resolved Issues in ArubaOS 6.2.1.0	40
3G/4G	40
Air Management-IDS	40
AP Wireless	41
AP Platform	41
BaseOS Security	41
Dot1x	42
IPsec	42
Management Auth	42
Mesh	42
RADIUS	43

Remote AP	43
Spectrum-Infrastructure	43
Station Management	43
Switch-Platform	44
Switch-Datapath	44
UI Configuration	45
Resolved Issues in ArubaOS 6.2.0.3	46
Controller-Platform	46
Resolved Issues in ArubaOS 6.2.0.2	46
Port-Channel	46
Switch-Platform	46
Resolved Issues in ArubaOS 6.2.0.1	46
AP Regulatory	47
Base OS Security	47
Controller Platform	47
DHCP	47
Startup Wizard	47
Station Management	48
Resolved Issues in ArubaOS 6.2.0.0	48
AP Datapath	48
AP Platform	48
AP Regulatory	49
AP Wireless	49
Air Management	50
Authentication	51
Base OS Security	52
Captive Portal	53
Configuration	53
Controller-Platform	53
DataPath/Platform	54
Dot1x	54
DPA	55
Dynamic Authorization	55
IPsec	55
Mesh	56
RAP	56
Remote Access Point	56
Roles/VLAN Derivation	56
Station Management	57
STP	57
UI-Configuration	57
UI-Monitoring	58
Voice	58
WebUI	58
WMM	59

Chapter 5	Known Issues	61
	Maximum DHCP Lease Per Platform	61
	Known Issues	61
	802.1X	61
	AP Wireless	62
	AP Platform	62
	Authentication	63
	Base OS Security	63
	Controller-Platform	64
	Controller-Datapath	64
	IPsec	65

IPv6	65
Management Auth.....	66
Master-Redundancy	66
Mobility.....	66
Remote AP	67
RAP + BOAP	68
Station Management.....	68
WebUI	69
WMM.....	70
Issues Under Investigation	70
OSPF	70
Controller-Datapath	70

Chapter 6 Upgrade Procedures 71

Upgrade Caveats.....	71
Important Points to Remember and Best Practices.....	72
Memory Requirements	73
Backing up Critical Data.....	73
Back Up and Restore Compact Flash in the WebUI	74
Back Up and Restore Compact Flash in the CLI	74
Upgrading in a Multi-Controller Network.....	75
Upgrading to 6.2.x.....	75
Install using the WebUI	75
Upgrading From an Older version of ArubaOS	75
Upgrading From a Recent version of ArubaOS.....	75
Upgrading With RAP-5 and RAP-5WN APs	76
Install using the CLI	77
Upgrading From an Older version of ArubaOS	77
Upgrading From a Recent version of ArubaOS.....	77
Downgrading	79
Before you Begin.....	79
Downgrading using the WebUI.....	80
Downgrading using the CLI	80
Before You Call Technical Support	81

Chapter 7 7200 Series Migration..... 83

Migrating to the 7200 Series Controller.....	83
Important Points to Remember.....	83
Backing Up Your Data Before Upgrading to 6.2.....	84
Back Up the Flash File System in the WebUI	84
Back Up the Flash File System in the CLI	84
Upgrading Your Network	84
Backing Up Your Data After Upgrading to 6.2.....	85
Transferring Licenses	85
Installing Your New Controller	85
Installing Backed Up Controller Data.....	86
Restore the Flash File System in the WebUI	86
Restore the Flash File System in the CLI.....	86
Applying Licenses	86
Applying the Software License Key in the WebUI	86
Applying the Software License Key in the License Wizard	87
Backing Up Licenses in the WebUI	87
Backing Up Licenses in the CLI	87
Reload Your Controller.....	87
Establishing Network Connectivity	87

Connecting to the Controller	88
Verifying Controller Operation.....	88
Verifying Migration in the WebUI	88
Verifying Migration in the CLI	88

ArubaOS 6.2.1.2 is a software patch release that includes fixes to a number of known issues. For details on all of the features described in the following sections, see the *ArubaOS 6.2 User Guide*, *ArubaOS 6.2 CLI Reference Guide*, and *ArubaOS 6.2 MIB Reference Guide*.



See the [Upgrade Procedures on page 71](#) for instructions on how to upgrade your controller to this release.

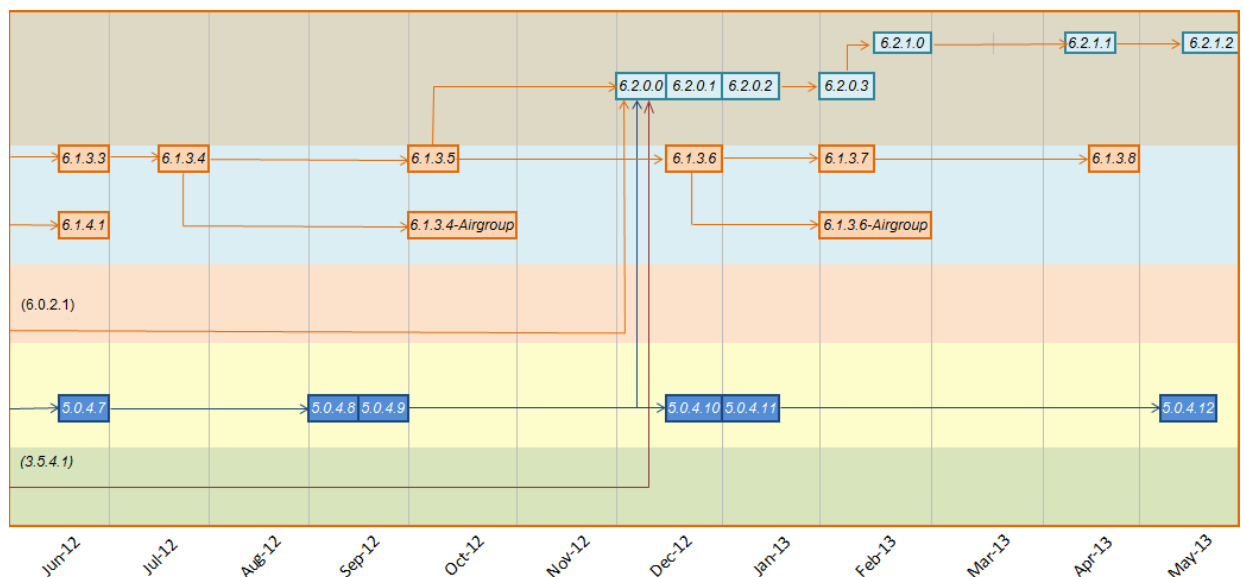
Chapter Overview

- [What's New in this Release on page 11](#) describes the fixes introduced in this release.
- [Features Added in Previous Releases on page 19](#) provides descriptions of features and enhancements added in previous 6.2.0.x releases.
- [Issues Fixed in Previous Releases on page 33](#) lists issues fixed in previous releases of 6.2.
- [Known Issues on page 61](#) provides descriptions and workarounds for outstanding issues in ArubaOS 6.2.1.2.
- [Upgrade Procedures on page 71](#) cover the procedures for upgrading your controller from any release of ArubaOS to ArubaOS 6.2.1.2.
- [7200 Series Migration on page 83](#) provides instructions for migrating your existing controllers to the new 7200 Series controller. For additional information, see support.arubanetworks.com.

Release Mapping

The following illustration shows which patches and maintenance releases are included in their entirety in ArubaOS 6.2.1.2.

Figure 1 *ArubaOS Releases and Code Stream Integration*



Supported Browsers

Beginning with ArubaOS 6.2, the following browsers are officially supported for use with the ArubaOS WebUI:

- Microsoft Internet Explorer 8.x and 9.x on Windows XP, Windows Vista, Windows 7, and MacOS
- Mozilla Firefox 14, 15, and 16 on Windows XP, Windows Vista, Windows 7, and MacOS
- Apple Safari 5.x on MacOS

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

ArubaOS 6.2.1.2 supports channel and country domain changes that impact RAP-108, RAP-109, AP-124, AP-125, AP-134 and AP-135 access points, and includes the resolved issues and upgrade caveats described in this chapter.

Supported Channels and Country Domains

The following changes impact new installations of RAP-108, RAP-109, AP-124, AP-125, AP-134 and AP-135 access points, running ArubaOS 6.2.1.2.

Table 1 *Changes in this Release*

Country Domain	Change
Changes for RAP-108/RAP-109 Access Points	
Malaysia	ArubaOS now supports this country domain.
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 and 100-140. 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.
Bermuda, 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.

Table 1 *Changes in this Release*

Country Domain	Change
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 for 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
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.

Resolved Issues in ArubaOS 6.2.1.2

AP Platform

Table 2 *AP Platform Fixed Issues*

Bug ID	Description
71978 75776	<p>Symptom: An AP model AP-68 unexpectedly rebooted due to a memory corruption. This is fixed in ArubaOS 6.2.1.2.</p> <p>Scenario: This issue was observed in an AP-68 running ArubaOS 6.2.0.0.</p>

AP Wireless

Table 3 *AP Wireless Fixed Issues*

Bug ID	Description
82493	Symptom: An AP crashed when a virtual AP configuration changed when downlink traffic from an AP to its associated the clients. Checks are added to the code to prevent and resolve this issue. Scenario: This issue is not specific to any AP model, and was identified in ArubaOS 6.1.3.7.

BaseOS Security

Table 4 *BaseOS Fixed Issues*

Bug ID	Description
68581	Symptom: When a mobile client roamed from a home agent (HA) controller to a foreign agent (FA) controller, issuing the CLI command show user-table from the FA controller incorrectly showed the client in an authenticated/derived role, whereas the output of the show datapath user command correctly showed the client in its dynamic role. The output of the show user-table command now shows correct information. Scenario: This issue was triggered when a mobile client roamed to a foreign agent controller running ArubaOS 6.2.x, and is not limited to any specific controller model.
83620 84429	Symptom: Clients using Temporal Key Integrity Protocol (TKIP) or Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) suddenly stopped receiving traffic. This issue is resolved by improvements to how ArubaOS manages counters when new keys are installed. Scenario: This issue was observed on 7200 Series controllers running ArubaOS 6.2.1.1.
81426	Symptom: A memory leak was observed in wired clients with RADIUS accounting enabled. This issue is resolved by freeing the memory allocated for RADIUS context when a user was deleted. Scenario: This issue was observed when wired clients were connected to the APs with RADIUS accounting enabled on AAA profile. This issue was not specific to any controller model.
84077	Symptom: A controller unexpectedly rebooted with a Crypto Post Failure message. This issue is resolved by enabling logs for the error message without automatically reloading the controller. Scenario: This issue is not specific to any controller model.

Command Line Interface

Table 5 *Command Line Interface Fixed Issues*

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

Control Plane Security (CPsec)

Table 6 *Control Plane Security Fixed Issue*

Bug ID	Description
66413 67875 68010	<p>Symptom: Occasionally, the Control Plane Security (CPsec) whitelist database entries did not synchronize between the master and local controller. ArubaOS 6.2.1.2 transmits smaller sized CPsec records. resolving the issue.</p> <p>Scenario: This issue was observed when the CPsec whitelist database size was large. A lossy network between the master and local controller caused some whitelist synchronization fragments to be lost. This issue was not limited to a specific controller model or release version.</p>

Controller Datapath

Table 7 *Controller Datapath Fixed Issues*

80625	<p>Symptom: A controller unexpectedly rebooted. Log files for the event listed the reason for the reboot as a Datapath timeout due to change in the tunnel MTU while processing a frame. This issue is resolved by ensuring that the same tunnel MTU is used for processing a given frame.</p> <p>Scenario: This issue was observed when tunnels were used on controllers running ArubaOS 6.1.3.x or later.</p>
83216	<p>Symptom: A controller generated proxy ARP responses out of the same trusted port from where it the controller learned the MAC address. Disabling the option bcmc-optimization in the VLAN interface resolved the issue.</p> <p>Scenario: The issue occurred when the trusted port was a port channel and the bcmc-optimization option was enabled on the VLAN interface. The issue was not specific to a controller model or a software version.</p>
83409	<p>Symptom: A controller rebooted due to missing heartbeats, and log files for the event listed the reason for the reboot as “watchdog timeout”. This issue is resolved by improvements to the communication infrastructure.</p> <p>Scenario: This issue was observed when a huge traffic hit the control plane causing loss of acknowledgements in the communication infrastructure. This is not specific to any controller model.</p>

Controller Platform

Table 8 *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 6.2.1.2. Scenario: A high amount of control traffic triggered this issue, which is not specific to any controller model.
80326 80780 81399 81462 82385 82775	Symptom: A controller failed to respond and rebooted without saving SOS crash log tar files after upgrading to ArubaOS 6.1.3.7. The log files for the event listed the reason for the reboot as “Control Processor Kernel Panic”. Internal code changes fixed this issue in ArubaOS 6.2.1.2. Scenario: This issue was first observed in ArubaOS 6.1.3.7.

Controller Software

Table 9 *Controller Software Fixed Issues*

Bug ID	Description
84622	Symptom: Bridge Protocol Data Units (BPDUs) in tagged VLANs were not flooded by the controller when spanning tree is disabled on the controller. Improvements to how process packets with a BDPU MAC address are handled resolves this issue. Scenario: This issue occurred when spanning tree was disabled on the controller and spanning tree was enabled on the uplink switch on the tagged vlan.

Dot1x

Table 10 *Dot1x Fixed Issue*

83375	Symptom: Client failed to connect to Lightweight Extensible Authentication Protocol (LEAP) SSID when operation mode was set to Dynamic-WEP and Use Session Key was enabled on the client. The issue occurred when some of the clients failed to negotiate a separate session key. Enhancements in the security protocols fixed this issue in ArubaOS 6.2.1.2. Scenario: This issue was observed in controllers running ArubaOS 6.2.1.0 and was not specific to any controller model.

Enhanced Voice-Data Optimized

Table 11 *Enhanced Voice-Data Optimized (EVDO) Fixed Issues*

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

IPv6

Table 12 *IPv6 Fixed Issues*

Bug ID	Description
76426 78962	<p>Symptom: An increase in CPU utilization by the user authentication process was observed on the controller. Creating a rule in the validuser Access Control List (ACL) to deny packets from the host source IPv6 address fe80::/128 fixed this issue in ArubaOS 6.2.1.2.</p> <p>Scenario: This issue was triggered when an HTC One X smartphone running Android version 4.1.1 generated a link-local IPv6 address fe80::/128, resulting in an increased CPU utilization on the controller. This issue was not limited to any specific version of ArubaOS.</p>
79452 77012	<p>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 6.2.1.2 updates the packets with tunnel flag so that data traffic doesn't get double encryption in an IPsec tunnel.</p> <p>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 all controller platforms running ArubaOS 6.2.x.</p>

Mobility

Table 13 *Mobility Fixed Issues*

Bug ID	Description
82673	<p>Symptom: DHCP packets from the clients at foreign agent were getting redirected through IPIP tunnel due to wrong order of the ACL. This caused a delay in allocating a valid IP address to the clients. This issue is resolved by correcting the order of the ACL.</p> <p>Scenario: This issue was observed when L3 mobility was enabled on controllers running ArubaOS 6.1.x.</p>

Online Certificate Status Protocol (OCSP)

Table 14 *OCSP Fixed Issues*

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

RADIUS

Table 15 *RADIUS Fixed Issue*

Bug ID	Description
76484	<p>Symptom: RADIUS authentication failed in networks that had different Maximum Transmission Values (MTUs).</p> <p>Scenario: The RADIUS authentication failed when the MTU value in the network between the controller and RADIUS server was different. This issue was observed in controllers running ArubaOS 6.2.1.2 or earlier and was not specific to any controller model.</p>

Voice SIP

Table 16 *Voice SIP Fixed Issue*

Bug ID	Description
81487 83707 83757 84631	<p>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.</p> <p>Scenario: This issue was observed in 7200 Series controllers running ArubaOS 6.1.3.3 or later.</p>

WebUI

Table 17 *WebUI Fixed Issues*

Bug ID	Description
76451	<p>Symptom: When guest users were imported using a .CSV file in the Configuration > Security > Authentication > Internal DB > Guest User page of the WebUI, the sponsor's email address was not imported.</p> <p>Scenario: The issue was observed in ArubaOS controllers running 6.1.3.4 and 6.2.x and was not specific to any controller model.</p>
80269	<p>Symptom: The GigabitEthernet interface 10 option was missing in the VRRP tracking Interface drop-down under Advanced Services > Redundancy > Add virtual Router > Tracking Interface table of the WebUI. ArubaOS 6.2.1.2 now includes the GigabitEthernet interface 10 option in the VRRP tracking Interface.</p> <p>Scenario: This issue was observed in M3 controller modules running ArubaOS 6.1.3.1.</p>
82959	<p>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 6.2.1.2.</p> <p>Scenario: This issue was observed in ArubaOS 6.2.x and is not specific to any controller model.</p>

Upgrade Caveats

Before upgrading to any version of ArubaOS 6.2, take note of these known caveats.

- Beginning with ArubaOS 6.2, the default **NAS-port-type** for management authentication using MSCHAPv2 is **Virtual** instead of **Wireless**. If your configuration uses the NAS-port-type in any derivation or access rules, this value will change for management user requests from the controller. This

behavior is in line with IEEE RFC 2865. There is no change in behavior for management authentication using PAP.

- Beginning with ArubaOS 6.2, you cannot create redundant firewall rules in a single ACL. ArubaOS will consider a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
 - source IP/alias
 - destination IP/alias
 - proto-port/service

If your pre-6.2 configuration contains an ACL with redundant firewall rules, upon upgrading, only the last rule will remain.

For example, in ArubaOS 6.2, in the ACL below, it is not possible to configure both of the ACE entries at the same time. Once the second ACE entry is added, the first ACE entry is overwritten.

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

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

- ArubaOS 6.2.x is supported only on the newer MIPS controllers (7200 Series, M3, 3400, 3600, 600 Series, 3200XM, and any 3200 controller with its memory upgraded using 3200-MEM-UG kit).

The PPC controllers (200, 800, 2400, SC1 and SC2) and the 3200 controller (with default memory) are *not* supported. DO NOT upgrade to 6.2.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 75](#)).

- 3200 controllers with 1GB of memory can be upgraded to ArubaOS 6.2. The 3200 controller with 512MB of memory is not supported by ArubaOS 6.2. For more information, see [“Changes to Hardware Support” on page 31](#).
- User Idle Timeout behavior has changed in ArubaOS 6.2. For more information, see [“User Idle Timeout Behavior Change” on page 30](#).
- Upon upgrade to ArubaOS 6.2, the internal AP of the 651 controller will be disabled. The controller will then operate as a 650 controller.

The following features were added in a previous release of ArubaOS 6.2.0.x:

Upgrading the New Software Image Scheme



Upgrading from ArubaOS 3.3.x, 3.4x, 5.0.x or 6.0.x to ArubaOS 6.2 may require an “upgrade hop”. Refer to [Table 18](#) for more information. Carefully follow the upgrade steps in [Upgrade Procedures on page 71](#).

[Table 18](#) provides a brief overview of the steps required to upgrade to ArubaOS 6.2.

Table 18 *ArubaOS 6.2 Upgrade Path Overview*

Version	Step 1	Step 2
3.4.x	Upgrade to the latest 3.4.5x	Upgrade to 6.2
RN-3.x	Upgrade to the latest 5.0.4.x	Upgrade to 6.2
5.0.x earlier than 5.0.3.1	Upgrade to the latest 5.0.4.x	Upgrade to 6.2
6.0.0.0 or 6.0.0.1	Upgrade to the latest 6.0.2.x	Upgrade to 6.2
6.1.x	Upgrade to 6.2	—

AP Capacity Per Controller

Starting with ArubaOS 6.2.0.0, controllers support the following number of APs. Consider the following limits when upgrading to ArubaOS 6.2 or later:

Table 19 *Controller AP Capacity*

Controller	Total AP Count	Campus APs	Remote APs
7240	2048	2048	2048
7220	1024	1024	1024
7210	512	512	512
M3	1024	512	1024
3600	512	128	512
3400	256	64	256
3200XM	128	32	128
650	16	16	16

Table 19 *Controller AP Capacity (Continued)*

Controller	Total AP Count	Campus APs	Remote APs
620	8	8	8

Hardware Platforms

7200 Series Controller



For information about migrating to the 7200 Series Controller, visit support.arubanetworks.com.

The 7200 Series controllers deliver a wide range of network services to large campus networks. The 7200 Series supports up to 32,000 users and performs stateful firewall policy enforcement at speeds up to 40 Gbps. The 7200 Series includes three models that provide varying levels of functionality.

Table 20 *Aruba 7200 Series Controller*

Model	APs Supported	Supported Users
7210	512	16,000
7220	1024	24,000
7240	2048	32,000

RAP-108 and RAP-109 Remote Access Points

The RAP-108 and RAP-109 are dual-radio, dual-band remote access points that support the IEEE 802.11n standard for high-performance WLAN.

Since the RAP-108/RAP-109 ships with Aruba Instant software, it operates, out of the box, as a Virtual Controller (VC) or an Instant AP. However, a RAP-108/RAP-109 can be converted to operate as a Remote AP (RAP).

RAP-3WN and RAP-3WNP Remote Access Points

This release of ArubaOS introduces support for RAP-3WN and RAP-3WNP access points (APs). The RAP-3WN and RAP-3WNP are single-radio, single-band wireless APs that support the IEEE 802.11n standard for high-performance WLAN.

Since the RAP-3WN and RAP-3WNP ship with Aruba Instant software, they will operate, out of the box, as a Virtual Controller (VC) or an Instant AP. However, both RAP-3WN and RAP-3WNP can be converted to operate as a Remote AP (RAP).

Remote Nodes Feature

The Remote Nodes feature is not supported in this release.



See the [LLDP MIBs on page 29](#) for MIB information specific to LLDP.

The Link Layer Discovery Protocol (LLDP) is a Layer-2 protocol that allows network devices to advertise their identity and capabilities on a LAN. Wired interfaces on Aruba APs support LLDP by periodically transmitting LLDP Protocol Data Units (PDUs) comprised of selected type-length-value (TLV) elements. For more information on the LLDP feature, refer to the Voice and Video section of the user guide.

Spectrum Analysis

Improved Visibility in the 5 GHz Radio Band

Spectrum monitor radios can now monitor the entire 5 GHz radio band at once, allowing you to view spectrum data for the upper, middle, or lower portions of the 5 GHz band using a single radio. In previous releases, a spectrum monitor radio could monitor only a portion of the 5GHz radio band at any time.

The following spectrum analysis charts now include a **Band** configuration option that allows you to change the portion of the 5GHz band you want to display for 5 GHz Spectrum Monitor radio.

- Active Devices
- Channel Metrics
- Device Duty Cycle
- Devices vs. Channel
- FFT Duty Cycle
- Interference Power
- Quality Spectrogram
- Real-Time FFT
- Swept Spectrogram

For information on Spectrum Analysis, including instructions to change these charts to display a different portion of the 5GHz radio band, refer to the Spectrum Analysis section of the user guide.

Spectrum Analysis RFPlayback Tool

Starting with ArubaOS 6.2, a spectrum recording can be played back in two ways. You can use the playback feature in the spectrum dashboard, or view recordings using the new Aruba RFPlayback tool available for download from the Aruba web site. The Aruba RFPlayback tool can play spectrum recordings created in this and earlier versions of ArubaOS. Aruba uses the Adobe AIR application to display spectrum recording information.

Follow the steps below to download and install the free Adobe AIR application and the Aruba spectrum playback tool:

1. Download the Adobe Air application from <http://get.adobe.com/air/> and install it on the client on which you want to play spectrum recordings.
2. Download the spectrum playback installation file from the Aruba web site.

3. Open the folder containing the spectrum installation file, and double-click the spectrum.air icon to install the spectrum playback tool. You will be prompted to select the folder in which you want to install this tool.



If you create a spectrum analysis recording for a 5 GHz radio using ArubaOS 6.2 or later, you can view data for any lower, middle, or upper portion of the 5 GHz radio band when you play back the recording. Spectrum recordings created using ArubaOS 6.1 or earlier capture data for only part of the 5GHz band, so these older recordings can only display data for only one portion of the 5 GHz band.

Both the spectrum dashboard and the RFPlayback tool include a playback progress bar that shows what part of the recording is being displayed. If you pause a recording, you can click and drag the red slider on this progress bar to advance to or replay any part of the current record.

Increased AP Support for Spectrum Analysis

In ArubaOS 6.2, radios on AP-104 and AP-93H devices can be configured as spectrum monitors, and AP-105 radios can be configured as either a spectrum monitor or a hybrid AP. The table below lists the AP models that support the spectrum analysis feature. Note that only radios on the AP-105 and AP-130 Series can be configured as hybrid APs.

Table 21 *Device Support for Spectrum Analysis*

Device	Configurable as a Spectrum Monitor?	Configurable as a Hybrid AP?
AP-104	Yes	No
AP-105	Yes	Yes
AP-92	Yes	No
AP-93	Yes	No
AP-93H	Yes	No
AP-120 Series	Yes	No
AP-130 Series	Yes	Yes
AP-175	Yes	No

Platform

Controller Capacity Alerts

The new controller capacity feature allows you to use the **Configuration>Management>Thresholds** page of the WebUI or the **threshold** CLI command to configure controller capacity thresholds which, when exceeded, will trigger alerts. The controller will send a **wlsxThresholdExceeded** SNMP trap and a syslog error message when the controller has exceeded a set percentage of the total capacity for that resource. A **wlsxThresholdCleared** SNMP trap and error message will be triggered if the resource usage drops below

the threshold once again. Current threshold values and limits appear in the output of the **show threshold** and **show threshold-limits** commands.

Table 22 *Threshold Descriptions*

Threshold Parameter	Description
controlpath cpu	Set an alert threshold for controlpath CPU capacity. The value of this parameter is the percentage of the total controlpath CPU capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 80%.
controlpath memory	Set an alert threshold for controlpath memory consumption. The value of this parameter is the percentage of the total memory capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 80%.
datapath cpu	Set an alert threshold for datapath CPU capacity. The value of this parameter is the percentage of the total datapath CPU capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 30%.
Total APs	The maximum number of APs that can be connected to a controller is determined by that controller's model type and installed licenses. Use this command to trigger an alert when the number of APs currently connected to the controller exceeds a specific percentage of its total AP capacity. The default threshold for this parameter is 80%.
Total local controllers	Set an alert threshold for the capacity of the master controller to support remote nodes and local controllers. A master controller can support a combined total of 256 remote nodes and local controllers. The value of this parameter is the percentage of the total master controller capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 80%.
Total tunnels	Set an alert threshold for the tunnel capacity of the controller. The value of this parameter is the percentage of the total tunnel capacity of the controller that must be exceeded before the alert is sent. The default threshold for this parameter is 80%.
Total Users	Set an alert threshold for the user capacity of the controller. The value of this parameter is the percentage of the total resource capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 80%.

ARM Scanning Enhancements

The default ARM scanning interval is determined by the **scan-interval** parameter in the ARM profile. Starting with ArubaOS 6.2, if the AP does not have any associated clients (or if most of its clients are inactive), the ARM feature will dynamically readjust this default scan interval, allowing the AP to obtain better information about its RF neighborhood, by scanning non-home channels frequently. If an AP attempts to scan a non-home channel but is unsuccessful, the AP will make additional attempts to rescan that channel, before skipping it and continuing on to other channels.

Timestamps in CLI Output

The timestamp feature can include a timestamp in the output of each show command issued in the command-line interface, indicating the date and time the command was issued. Note that the output of

show clock and **show log** do not include timestamps, even when this feature is enabled. To enable this feature, access the command-line interface in config mode and issue the command **clock append**.

Support for 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 6.2



The RAP-5WN and AP-120 Series APs can be upgraded to ArubaOS 6.2, but will become non-compliant with version 1.6.1 of the ETSI DFS standard. RAP-5WN and AP-120 Series APs already installed in a network are allowed to remain compliant with the previous version of the DFS standard, but where the ETSI rules apply, any new devices added to a network after 12/31/2012 must comply with version 1.6.1 or later of the same.

Enabling FCC DFS channels

ArubaOS 6.2 enables FCC DFS channels in the 5GHz band for the following APs:

- AP-92 and AP-93
- AP-93H
- AP-105
- AP-104
- AP-134 and AP-135

Prior to ArubaOS 6.2, FCC DFS channels were only enabled on the AP-120 Series APs.

Regulatory adjustments

Country support and EIRP transmit power levels have been updated to reflect the latest regulatory status and test results.

Support for Single-Chain Mode

Radios on all 802.11n MIMO APs can now be configured to operate in single-chain mode, allowing those APs to transmit and receive data using only legacy rates and single-stream (SISO) HT rates up to MCS 7. This feature is disabled by default.

<z_blue> below shows the antenna ports used by an AP operating in single-chain mode.

Table 23 *Antenna Interfaces for Single-Chain Mode*

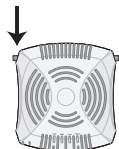

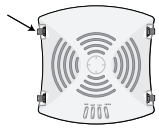



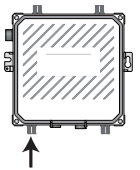
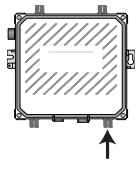
AP Model	Frequency Band	Antenna Port
AP-92	2.4GHz or 5GHz	ANT0 

Table 23 *Antenna Interfaces for Single-Chain Mode (Continued)*

AP Model	Frequency Band	Antenna Port
AP-104	2.4GHz	R1/A0 
	5GHz	R0/A0 
AP-120 and AP-124	2.4GHz	Upper Left 
	5GHz	Upper Right 
AP-134	2.4GHz or 5GHz	ANT0 
AP-175	2.4GHz	R1-1 
	5GHz	R0-1 

L2/L3 VLAN Scalability Requirements

The following table displays the supported numbers of L2 VLANs, L3 VLANs and Static Routes on each of the listed controller types:

Table 24 L2/L3 VLAN Scalability Requirements

Platform	L2 VLANs	L3 VLANs	Static Routes
620	128	128	128
650	128	128	128
3200XM	1024	512	256
3400	2048	1024	512
3600	4096	2048	1024
M3	4096	2048	2048
7200 Series	4096	4096	2048

Enhancement to WMM-DSCP Mapping

After you customize a WMM Access Class mapping and apply it to the SSID, the controller overwrites the default mapping values and uses the configured values. If a controller is upgraded to 6.2 from an older version, the default and the user configured WMM-DSCP mappings in the existing SSID profiles are retained. There are no default mappings for a newly created SSID profile and for a factory default running a 6.2 image. The maximum number of values that can be configured for WMM-DSCP is 8.

New Wizard Enhancements

Several new wizard enhancements were added to this release. These include:

Controller Wizard

You can now create a VLAN by name. After creating a new VLAN name, you can configure it for VLAN IDs, IP address, enable for NAT, add port members and configure DHCP settings.

An **Uplink** step is added that allows you to enable the **Uplink Manager**.

Campus Wizard

An **Uplink** step is added that allows you to enable the **Uplink Manager**.

WebUI Profile Usability Enhancements

Starting with ArubaOS 6.2, the various configuration profiles are divided into two tabs, **Basic** and **Advanced**. The **Basic** tab displays only those configuration settings that often need to be adjusted to suit a specific network. The **Advanced** tab shows all configuration settings, including settings that do not need frequent adjustment or should be kept at their default values.

The following profiles now appear in the WebUI with **Basic Settings** and **Advanced Settings** tabs.:

- ap system profile
- wired ap profile
- rf 802.11a profile
- rf 802.11g profile
- rf arm profile
- high-throughput radio profile
- rf event thresholds
- rf am scanning profile
- rf ssid profile
- high-throughput SSID profile
- Virtual AP profile
- LLDP profile
- LLDP-MED profile
- rf 802.1x auth profile
- VIA connection profile
- voip call admission control profile
- ids unauthorized device profile
- ids impersonation profile
- mesh-ht-ssid profile
- mesh radio profile

Policy Enforcement Firewall (PEF) Visibility

The Policy Enforcement Firewall (PEF) Visibility is a new PEF feature on the ArubaOS controller. It enables network administrators to monitor applications that are running on the controller, and the users using them in a given network.

The **Dashboard** page of the WebUI now has a new **Firewall** page. This page displays the PEF summary of all the sessions in the controller aggregated by the following:

- Users
- Devices
- Destinations
- Applications
- WLANs
- Roles



PEF Visibility is a beta feature. For troubleshooting, contact the Aruba technical support team.

Security

Enabling Bandwidth Contract Support for RAPs

This release of ArubaOS provides Bandwidth Contract support on remote APs. This is achieved by extending the Bandwidth Contract support on split-tunnel and bridge modes.

You can apply Bandwidth Contract for a RAP on a per-user or per-role basis. By default, Bandwidth Contract is applied on a per-role basis. This implies that all the users belonging to the same role will share the bandwidth pool. When Bandwidth Contract configured on the controller is attached to a user-role, it automatically gets pushed to the RAPs terminating on it.

The following show commands have been enhanced in this release to retrieve the Bandwidth Contract information from the RAP:

```
show datapath user ap-name <ap-name>
show datapath bwm ap-name <ap-name>
```

You can apply the contract on a per-role or per-user basis. Use the following commands to apply the contracts on a per-role basis for upstream and downstream:

For upstream contract of 512 Kbps:

```
(host) (config) #user-role authenticated bw-contract 512k upstream
```

For downstream contract of 256 Kbps:

```
(host) (config) #user-role authenticated bw-contract 256k downstream
```

Use the following commands to apply the contracts on a per-user basis for upstream and downstream:

For upstream contract of 512 Kbps:

```
(host) (config) #user-role authenticated bw-contract 512k per-user upstream
```

For downstream contract of 256 Kbps:

```
(host) (config) #user-role authenticated bw-contract 256k per-user downstream
```

DHCP Exhaustion Prevention

A new **Prevent DHCP Exhaustion** parameter in the Global Firewall settings checks DHCP client hardware address against the packet source MAC address. This feature checks the frame's source-MAC against the DHCPv4 client hardware address and drops the packet if it does not match. Enabling this feature prevents a client from submitting multiple DHCP requests with different hardware addresses, thereby preventing DHCP pool depletion.

RAP Serviceability Enhancements

When a remote AP (RAP) or a campus AP using control plane security fails to receive an IP address using DHCP from its ENET0 link, it keeps trying to get the address, every 35 seconds. After 10 such retries, the AP will reboot and start the process again.

Users with RAPs configured in either bridge mode or split-tunnel mode can use the RAP Console screen in the WebUI to troubleshoot connectivity issues. Access the RAP console using the URL: <http://rapconsole.arubanetworks.com>. This page also has a link to generate a support file (Generate and save support file link). These logs contains ap troubleshooting information. The output of the following firewall commands and process/mem usage commands appear in this file:

- Firewall commands - A snapshot of the bridge table, ACL table, session table, user table and ARP table in the remote AP.
- ps - reports a snapshot of the current processes.
- dmesg - Displays the kernel debug logs.
- ifconfig - Displays information on the state of the interface.
- meminfo - Displays the current total memory, free memory and the swap space of the device.
- SlabInfo - Displays kernel slab allocator statistics.

Captive Portal Enhancements

This release of ArubaOS introduces the following captive portal enhancements in tunnel and split-tunnel forwarding modes.

- When a client using captive portal authentication gets redirected to the captive portal server, the controller will send information about the AP group and name of the AP to which the client is trying to connect in the redirect URL. If the AP name is not configured, the redirect URL will contain the AP MAC address.
- A new option **redirect-url** is introduced in the Captive Portal Authentication profile which allows you to redirect the users to a specific URL after the authentication is complete.
- Captive Portal Login URL length has been increased from 256 characters to 2048 characters.
- Support for “?” (question mark) inside the Captive Portal login URL has been added.

- A new field, description has been introduced in the netdestination and netdestination6 commands to provide a description about the netdestination up to 128 characters long.
- Support for configuring Whitelist in Captive Portal has been introduced.

Inter-Controller IP Mobility Support on L2-GRE Tunnel

In the earlier implementation of IP Mobility, visitor traffic to/from the foreign agent (FA) is tunneled back to the home agent (HA) over an IPIP tunnel. The IPIP tunnel did not carry the original L2 headers from the visitor.

This release of ArubaOS replaces the IPIP tunnel with L2 GRE tunnel for the IP mobility functionality. This preserves the L2 headers in the packets from the visitor at FA to HA. The HA then bridges the traffic from the L2 GRE tunnel to the appropriate home VLAN, provided the HA knows the home VLAN of the visitor.



The L2-GRE Tunnel implementation of the IP mobility functionality is supported only on ArubaOS versions 6.2 or later and is not backward compatible with the earlier implementation. This release of ArubaOS supports only v4 mobility and does not support IPv6 L3 mobility.

RAP 3G/4G Backhaul Link Quality Monitoring

The RAP is enhanced to support link monitoring on 2G, 3G, and 4G modems to provide information about the state of USB modem and cellular network.

The USB modem has the following four states:

- Active - The USB modem is used as the primary path for connecting VPN to the controller
- Standby or Backup - The network is available but the USB modem is not used for connecting VPN to the controller
- Error - The USB modem is available but the modem is faulty
- Not Plugged - The USB modem is unavailable

New MIB Enhancements

LLDP MIBs

Two new tables have been added to the **wlsxRSMIB** (**aruba-rs.my**). These include:

- **wlsxLldpNeighborTable**: This table enumerates the LLDP neighbors discovered by the access point.
- **wlsxLldpNeighborManAddrTable**: This table enumerates the LLDP neighbor management addresses discovered by the access point.
- **wlsxRemoteWiredPortTable**: The interface name object, **remotePortName**, has been added to this table. This object specifies the name of the port.

RAP Instrumentation for Airwave Monitoring

The following objects have been added to the **wlsxWlanAPTable**:

- **wlanAPOuterIpAddress**: The outer IP address of the access point
- **wlanAPRemoteLanIpAddress**: The LAN IP address of the Remote Access Point (RAP)
- **wlanAPActiveUplink**: The uplink of the RAP (Ethernet or USB)



The following objects have been added to the **wlsxRemoteUSBTable**:

USB modem statistics are applicable only for the USB-based modems AP type Aruba RAP-5WN.

- **usbRSSI**: The USB Received Signal Strength Indicator (RSSI)
- **usbStatus**: The device status
- **usbNetworkServiceLevel**: The USB network service level and type
- **usbEsnNumber**: The USB electronic serial number (ESB)
- **usbifOperStatus**: The operational status of the USB interface
- **usbifInUcastOctets**: The received bytes
- **usbifOutUcastOctets**: The transmitted bytes
- **usbifInUcastPkts**: Received unicast packets
- **usbifOutUcastPkts**: Transmitted unicast packets
- **usbifInErrors**: The errors in the incoming interface
- **usbifOutErrors**: The errors in the outgoing interface.

Aruba Products sysObject IDs

Table 25 defines the sysObjectIds for Aruba products added to this release:

Table 25 *SNMP OIDs returned as sysObjectID for Aruba products*

SNMP MIB	OID
ap93h	1.3.6.1.4.1.14823.1.2.50
rap3wn	1.3.6.1.4.1.14823.1.2.51
rap3wnp	1.3.6.1.4.1.14823.1.2.52
ap104	1.3.6.1.4.1.14823.1.2.53
rap108	1.3.6.1.4.1.14823.1.2.56
rap109	1.3.6.1.4.1.14823.1.2.57

User Idle Timeout Behavior Change

The user idle timeout behavior for the way wireless users are aged out of the system has changed in ArubaOS 6.2.

In ArubaOS pre-6.2 versions, users were idled out if there was no IP traffic for five minutes (the default setting for **configure terminal aaa timers idle-timeout**). Now, users are idled out if there is no wireless traffic.

In ArubaOS 6.2, if the client signals that the AP it has left the BSSID, the client is aged out in the time specified by **aaa user idle-timeout**. Otherwise the client is aged out with the wireless timeout, whose default period is 1000 sec (**configure terminal wlan ssid-profile <profile name> ageout**).

Due to a change in user idle detection internal functionality, there is a possibility that VIA clients may get disconnected prematurely. This change affects non-Windows based VIA users deployed in split-tunnel mode only.

If you notice that the “Idle users due to SOS: other” counter is higher than usual, Aruba suggests that you consider changing **aaa user idle timeout** to a higher value.

```
(host) #show aaa state debug-statistics
user miss: ARP=0, 8021Q=413438, non-IP=0, zero-IP=0, loopback=0
user miss: mac mismatch=308733, spoof=0 (0), drop=379355, ncfg=0 enforce_dhcp=0
user miss: non-auth opcode=0, no-l2-user=18337, l2tp=0, vrrp=0, special mac=0, iap l3
user=0
Idled users = 26718
Idled users due to MAC mismatch = 0
Idled users due to SOS: wireless tunnel=0 wireless dtunnel=0
Idled users due to SOS: wired tunnel=16460 wired dtunnel=0
Idled users due to SOS: other=0
Idled users due STM deauth: tunnel=9883 dtunnel=0
Idled users from STM timeout: tunnel=345 dtunnel=0
Idled users from STM: other=0
Current users with STM idle flag = 6144
Idle messages: SOS=16460 STM deauth=51952 STM timeout=1
Logon lifetime iterations = 255, entries deleted = 0
SIP authentication messages received 0, dropped 0
Missing auth user deletes: 0
Captive-portal forced user deletes: 0
```

Changes to Hardware Support

651 Controller

Beginning in ArubaOS 6.2, the internal AP of the 651 controller will be disabled. For more information, see [AP Platform on page 62](#). Additionally, upon upgrade, the 651 will appear as 650-1 and the 651-8 will appear as 650-9 in ArubaOS.

3200 Controller

The 3200 controller with default memory is not supported in ArubaOS 6.2. However, ArubaOS 6.2 supports the 3200XM controller or any 3200 with its memory upgraded using 3200-MEM-UG kit.

The following issues were fixed in a previous ArubaOS 6.2.0.x release:

Resolved Issues in ArubaOS 6.2.1.1

802.1X

Table 26 802.1X Fixed Issues

Bug ID	Description
77154	<p>Symptom: If the Use Server provided Reauthentication Interval setting was enabled in an AP's 802.11X authentication profile, clients associated with that AP did not reauthenticate when the client roamed to a different AP. This issue is resolved by a change that allows the controller to store the session timeout reauthentication interval returned from the RADIUS server.</p> <p>Scenario: This issue occurred in ArubaOS 6.1.2.4, when clients authenticating with a RADIUS server roamed between APs.</p>
80841	<p>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 fix this issue in ArubaOS 6.2.1.1.</p> <p>Scenario: When MAC authentication and 802.1X is configured and an eapol-start request from the client came between MAC authentication and 802.1X authentication, the 4-way key exchange was started instead of full 802.1X authentication. This issue was observed in controllers running ArubaOS 6.1.3.5.</p>

Air Management - IDS

Table 27 Air Management - IDS Fixed Issues

Bug ID	Description
81073	<p>Symptom: An Air Monitor (AM) stopped scanning when it had been up for more than 50 days. This uptime threshold was reached when the AM's milli-tick counter, which counts the uptime in milliseconds, rolled over and the counter returned to zero.</p> <p>Scenario: This issue was identified on ArubaOS 6.1.3.2 and was not limited to a specific controller or AP model. This rollover is expected behavior and a side effect of the roll over caused the issue. A fix has been made to check for and correctly handle the rollover to avoid this issue.</p>

AMON

Table 28 AMON Fixed Issues

Bug ID	Description
81759	<p>Symptom: Upon upgrade to ArubaOS 6.2.0.2, a controller rebooted unexpectedly due to an internal process (fw_visibility) crash. This issue is resolved in ArubaOS 6.2.1.1.</p> <p>Scenario: This issue was identified on ArubaOS 6.2.0.2 and not limited to any specific controller model.</p>

AP Platform

Table 29 *AP Platform Fixed Issues*

Bug ID	Description
77236	<p>Symptom: An AP-125 configured to discover its master controller using DNS failed to connect to the controller after completing 802.1X authentication. Improvements to the master discovery process resolve this issue in ArubaOS 6.2.1.1.</p> <p>Scenario: When the AP completed 802.1X authentication, the AP selected an IP address before the master was discovered. This issue occurred on APs running ArubaOS 6.1.3.2 configured to use 802.1X authentication and dynamic master discovery.</p>

AP Regulatory

Table 30 *AP Regulatory Fixed Issue*

Bug ID	Description
79804	<p>Symptom: AP-93 APs using the Panama country code operated in air-monitor mode even though the AP's 802.11a and 802.11g radio profiles were configured in AP-mode. This issue is fixed by adding support for Panama and Puerto Rico in the PR country code on an AP-93.</p> <p>Scenario: This occurred on AP-93 access points running ArubaOS 6.1.3.x and later.</p>

AP Wireless

Table 31 *AP Wireless Fixed Issues*

Bug ID	Description
79724	<p>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 ensures that the AP sends out buffered data packets when it is notified that the Vocera client has come out of powersave mode.</p> <p>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.</p>
80334	<p>Symptom: Clients intermittently disconnected after successfully connecting to the 2.4 GHz Band of an AP-125. 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 resolves this issue in ArubaOS 6.2.1.1.</p> <p>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.</p>

ARM

Table 32 *ARM Fixed Issue*

Bug ID	Description
79204	<p>Symptom: In ArubaOS 6.2.0.0-6.2.1.0, APs without clients scan non-home channels for longer periods than APs that do have associated clients. This increase in scan times for APs without clients could prevent VoWLAN phones like the Motorola EWP1000 from considering those APs as roaming candidates. This issue is resolved by changing the default scan time for APs without clients to the same scan time as APs with clients.</p> <p>Scenario: This issue occurred in ArubaOS 6.2.0.0-6.2.1.0, and is not specific to any controller model.</p>

BaseOS Security

Table 33 *BaseOS Fixed Issues*

Bug ID	Description
76027	<p>Symptom: The configured netservices svc-papi and svc-sec-papi did not appear in the output of the show running-config CLI command. A change to how these services are added to the controller resolves this issue.</p> <p>Scenario: This issue appeared in ArubaOS 6.2.0.0, and is not limited to any specific controller model.</p>
79564	<p>Symptom: The controller's internal user authentication process crashed when a wireless client used captive portal authentication and the client user role required reauthentication. Improvements to the reauthentication timer fixed this issue in ArubaOS 6.2.1.1.</p> <p>Scenario: This issue only occurred if the wireless client had more than one IPv4/IPv6 address. When the first IP address aged out before the reauthentication timer triggered, the process crashed. This issue was observed in controllers running ArubaOS 6.x.</p>
79805	<p>Symptom: An internal controller process stopped responding, causing the controller to reboot and preventing clients from authenticating. Memory buffer improvements resolve this issue in ArubaOS 6.2.1.1.</p> <p>Scenario: In rare conditions, the error handling process incorrectly released the Extensible Authentication Protocol (EAP) memory twice, causing memory corruption. This issue occurred in an M3 controller running ArubaOS 6.1.3.7 in a master-local topology where an M3 controller acted as a local controller.</p>
80162	<p>Symptom: An error in the internal auth module on a controller caused it to stop responding. This auth module crash occurred when another controller process mistakenly told the auth module that a VPN user was ready before the user had completed the authentication process. A fix is added to ArubaOS 6.2.1.1 prevent this issue.</p> <p>Scenario: This issue was first identified in ArubaOS 6.2.0.2 and is not limited to any specific controller model.</p>
80324	<p>Symptom: An internal controller module stopped responding when the controller upgraded from ArubaOS 6.1.3.6 to ArubaOS 6.1.3.7, causing the controller to reboot. Improvements to how the controller checks for null Aruba certificates has resolved this issue in ArubaOS 6.2.1.1.</p> <p>Scenario: This issue occurred on a 620 controller in a master-local topology.</p>

Control Plane Security (CPsec)

Table 34 *Control Plane Security Fixed Issue*

Bug ID	Description
78301	<p>Symptom: A master controller stopped synchronizing its CPsec whitelist with local controllers due to an interruption in the synchronization process. Enhancements to how the synchronization process performs retry attempts fixes this issue in ArubaOS 6.2.1.1.</p> <p>Scenario: The CPsec whitelist synchronization failure on the master controller was caused by an interruption that could include any of the following:</p> <ul style="list-style-type: none">• loss of network connectivity• loss of minor frames• crash or reboot associated with the controller <p>This issue was observed in ArubaOS 6.1.2.6.</p>

Controller Platform

Table 35 *Controller Platform Fixed Issues*

Bug ID	Description
79553 77810 80328 81489	Symptom: An internal controller module failed to respond, causing the controller to reboot, when a Campus AP (CAP) was deployed behind a Remote AP (RAP). Improvements to the encapsulation process fixe this issue in ArubaOS 6.2.1.1. Scenario: This issue was triggered by packets that became corrupted after IPSEC encryption. The issue was observed in on M3 controllers running ArubaOS 6.2.0.2.
80360	Symptom: The 7200 Series controller experienced an internal process (datapath) crash and reboot when connected to and receiving data from an AMSDU-enabled client device. Scenario: AMSDU caused an internal process error that resulted in a crash and reboot of the 7200 Series controller. This issue was identified in ArubaOS 6.2.1.0 and has been fixed in this release.
80419 80523	Symptom: A feature allowed the ArubaOS DNS server to reveal its version number. This feature has been disabled in ArubaOS 6.2.1.1 as a security precaution. Scenario: This issue was identified in ArubaOS 6.2.0.0
81178	Symptom: When a 7220 controller upgraded to 6.2.1.0, an internal controller module stopped responding, causing the controller to reset. This issue was triggered by reserved source descriptor fields that were incorrectly defined in the POE buffer address info and the POE flow info packets. Changes that prevent these reserved fields from getting set resolve this issue in ArubaOS 6.2.1.1. Scenario: This issue was identified on a 7200 Series controller running ArubaOS 6.2.1.0.
81865	Symptom: When a loopback IP address is configured on a controller but the controller IP is set to the IP address of another VLAN interface, no entry appears for the loopback interface's IP address in the user table. A fix is introduced in ArubaOS 6.2.1.1 to create an entry in the user table if the controller 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.

MAC-Based Authentication

Table 36 *MAC-Based Authentication Fixed Issue*

Bug ID	Description
77491	Symptom: The Session-Timeout attribute returned from the RADIUS Server during MAC authentication was not honored in reauthentications, and the client did not revert to its initial user role when MAC authentication failed. This issue has been fixed on ArubaOS 6.2.1.1 by adding session-timeout support for MAC authentication. Scenario: This issue was identified on a controller running ArubaOS 6.1.3.5, and not specific to any controller model.

Mesh

Table 37 *Mesh Fixed Issue*

Bug ID	Description
78805	<p>Symptom: The controller process that handles AP management and user association unexpectedly stopped and restarted. This issue is fixed in ArubaOS 6.2.1.1 by blocking certain entries and events that are created when the image on an AP does not match the image on the local controller.</p> <p>Scenario: This issue was observed in M3 controllers running ArubaOS 6.1.3.6 with Mesh Portals and Points in the setup. When the image version on the AP 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.</p>

Mobility

Table 38 *Mobility Fixed Issues*

Bug ID	Description
75093	<p>Symptom: The show ip mobile host CLI command incorrectly displayed the roaming status of a client as No state instead of the expected Home Switch/Home VLAN. Changes in the mobile IP process that free the client's host entry fixed this issue in ArubaOS 6.2.1.2.</p> <p>Scenario: This issue was observed when L3-mobility was enabled in the controller. This issue was not limited to any controllers model or version of ArubaOS.</p>
78111	<p>Symptom: Roaming clients experienced traffic interruption when L3 mobility was enabled on the controller. This issue has been fixed in ArubaOS 6.2.1.1.</p> <p>Scenario: This issue occurred because duplicate ARP responses were sent from both the home agent and foreign agent for the roaming client. This issue was observed when the controllers were upgraded from ArubaOS 5.x to 6.1.x.</p>

Remote AP

Table 39 *Remote AP Fixed Issues*

Bug ID	Description
77450	<p>Symptom: Wired clients connected to a remote AP in bridge forwarding mode were unable to get an IP address when the remote AP lost connectivity to the controller, or if any of the following fields changed in the Virtual AP or SSID:</p> <ul style="list-style-type: none">• 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 <p>ArubaOS 6.2.1.1. resolves this issue with a change that prevents the uplink destination device (bond0) from being removed from the VLAN multicast table when a backup SSID is enabled and there are other wired or wireless devices present in the VLAN multicast table.</p> <p>Scenario: This issue was observed when the AP had a backup Virtual AP in the same VLAN as the wired clients, and the AP wired port profile had the Remote-AP backup option enabled. This issue was observed in APs running ArubaOS 6.1.x, and was not limited to any specific AP model.</p>

Table 39 *Remote AP Fixed Issues (Continued)*

Bug ID	Description
78656	<p>Symptom: A remote AP could not operate in L2 mode when connected to a local controller in a master-local topology or a backup controller in a redundant master topology. A change in how the source IP of the GRE tunnel is defined resolves this issue in ArubaOS 6.2.1.1.</p> <p>Scenario: This issue occurred on remote APs in L-2 mode connected to a local or backup master controller, and was not limited to any specific AP model. It was triggered because the AP did not use the "controller-ip" IP address as the source IP of the GRE tunnel, which caused the controller to respond with ICMP unreachable messages for packets sent by the AP.</p>

Role/VLAN Derivation

Table 40 *Role/VLAN Derivation Fixed Issue*

Bug ID	Description
78322	<p>Symptom: Clients connected to an AP in bridge forwarding mode derived incorrect roles when the AP was connected to a Cisco bridge VLAN. This issue has been resolved in ArubaOS 6.2.1.1, which now checks to see if the source MAC address from the L2 bridge mobility advertisement message is the AP's MAC address, then prevents the AP from deleting L2 and L3 entries if the MAC addresses are the same.</p> <p>Scenario: This issue was observed when an AP connected to a Cisco bridge VLAN received its own broadcast message over the uplink and started deleting L2 and L3 database entries. This issue is not specific to a controller model.</p>

Spectrum-Infrastructure

Table 41 *Spectrum-Infrastructure Fixed Issue*

Bug ID	Description
79144	<p>Symptom: AP-105, AP-92, and AP-93 access points running ArubaOS 6.2.x and later versions unexpectedly stopped responding and rebooted. This issue is resolved in ArubaOS 6.3.</p> <p>Scenario: This issue occurred when spectrum monitoring was enabled in the AP's 802.11a or 802.11g radio profile.</p>

Voice SIP

Table 42 *Voice SIP Fixed Issue*

Bug ID	Description
79717	<p>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 fix this issue in ArubaOS 6.2.1.1.</p> <p>Scenario: SIP ALG was not able to parse SDP (Session Description Protocol), which prevented the the traffic from being correctly prioritized. This issue was observed in ArubaOS 6.1.3.5.</p>

WebUI

Table 43 *WebUI Fixed Issues*

77548	<p>Symptom: Accessing any page of the controller's WebUI generated a Null error message. Changes to how WebUI sessions are managed fix this issue in ArubaOS 6.2.1.2.</p> <p>Scenario: This issue occurred due to an internal error in a process that affects how commands are executed in a WebUI session. This issue is not limited to any controller model or version of ArubaOS.</p>

Resolved Issues in ArubaOS 6.2.1.0

The following issues have been resolved in ArubaOS 6.2.1.0:

3G/4G

Table 44 *3G/4G Fixed Issue*

Bug ID	Description
77928	<p>Symptom: An AP failed to complete a DNS query when it was configured to use a UML290 USB modem uplink. Improvements to multicast IP address checks resolves this issue in ArubaOS 6.2.1.0</p> <p>Scenario: This issue occurred when a UML290 uplink was configured on an Instant AP that was provisioned to use a wired interface and a DNS host name for a VPN. Due to this issue, DNS host names could not be resolved on the IAP or its clients. This issue was identified on RAP-3WN, RAP-108 and RAP-109 access points running ArubaOS 6.2.0.0.</p>

Air Management-IDS

Table 45 *Air Management-IDS Fixed Issues*

Bug ID	Description
76936	<p>Symptom: Rogue APs operating in Greenfield mode were not contained by Air Monitors (AMs). Improvements to AP containment processes resolve this issue in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue was first identified in ArubaOS 6.1.3.5, and was not limited to any specific controller or AP model.</p>
76808	<p>Symptom: Some internal processes on the controller were unusually busy, while overall CPU utilization remained within expected levels. ArubaOS 6.2.1.0 introduces changes that prevent APs from sending excessive containment event messages to the controller, so these internal processes do not become overloaded.</p> <p>Scenario: This issue was triggered when the wireless containment parameter in the IDS General profile was set to tarpit all-sta or tarpit-non-valid-sta, and one or more IDS Protection features are enabled such that active containment occurred.</p>

AP Wireless

Table 46 *AP Wireless Fixed Issue*

Bug ID	Description
77946	<p>Symptom: ArubaOS did not support mixed encryption modes for static-WEP and WPA-PSK-TKIP, or for dynamic-WEP and WPA-TKIP. This issue is fixed in ArubaOS 6.2.1.0 and these combinations are now in the list of allowed modes.</p> <p>Scenario: When editing the SSID profile in the WebUI, the system displayed the error message “invalid opmode combination”, even though dynamic-WEP WPA-TKIP was available for selection in the WebUI. This issue was observed in ArubaOS 6.1 and later versions, and was not limited to any specific controller model.</p>

AP Platform

Table 47 *AP Platform Fixed Issues*

Bug ID	Description
76021	<p>Symptom: A core file from an AP with a special character in the AP name included the special character in the core file name, causing TFTP dump servers to reject that file. ArubaOS 6.2.1.0 resolves this issue by removing special characters from the core file name before it sends the file to the dump server.</p> <p>Scenario: This issue occurred when an internal process crashed on an AP, and a core file of troubleshooting data was sent to the dump server defined in the AP's system profile. This issue was seen on APs with one or more special characters in the AP name, and was not limited to a specific AP model.</p>
77183	<p>Symptom: An AP-61 associated with a 7200 Series controller running ArubaOS 6.2.0.1 unexpectedly rebooted. The log files on the controller listed the reason for the AP reboot as “watchdog timeout.” Changes to channel reuse processing resolves this issue in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue occurred when the RX Sensitivity Tuning Based Channel Reuse setting in the dot11x radio profile was set to dynamic.</p>
77645	<p>Symptom: APs associated to a 7200 Series controller rebooted, forcing clients to reassociate. Changes in how the controller manages duplicate MAC addresses resolves this issue in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue occurred on a 7200 Series controller in a master-local topology where the APs failed over between two controllers.</p>

BaseOS Security

Table 48 *BaseOS Fixed Issue*

Bug ID	Description
75754	<p>Symptom: The user table showed that some 802.1X authenticated clients managed by an external XML-API server were using Web authentication, even though there was no captive portal authentication configured for those clients. This display issue is resolved in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue occurred on a controller configured with a 802.1X default role with an ACL that sent traffic through the GRE tunnel to a SafeConnect appliance. In this scenario, L3 authentication was managed by the SafeConnect XML API, which updated the user role to an L3-authenticated role.</p>

Dot1x

Table 49 *Dot1x Fixed Issues*

Bug ID	Description
77705, 78658, 78559	Symptom: Clients using WPA-TKIP encryption were unable to complete 802.1x authentication. Changes in how TX sequence numbers are reset resolves this issue in ArubaOS 6.2.1.0. Scenario: This issue occurred on 7200 Series controllers running ArubaOS 6.2.0.2.
79546	Symptom: An internal controller module stopped responding, causing the controller to unexpectedly reboot. The log file for the event listed the reason for the reboot as “datapath exception. Memory buffer improvements resolve this issue in ArubaOS 6.2.1.0. Scenario: This issue occurred on M3 controllers running ArubaOS 6.1.3.7.

IPsec

Table 50 *IPsec Fixed Issues*

Bug ID	Description
68035	Symptom: When site-to-site VPN was enabled between two controllers, static routes were not removed from the routing table when site-to-site VPN went down. Improvements to the way controllers add and delete static routes resolves this issue in ArubaOS 6.2.1.0. Scenario: This occurred when site-to-site VPN was enabled and a static route was added to a remote subnet with an IPsec map.
76301	Symptom: An AP continually rebooted. The log files for the event listed the reason for the reboot as “Send failed in function sapd_keepalive_cb.” This issue is resolved in ArubaOS 6.2.1.0 Scenario: This issue occurred on both campus APs (CAPs) and remote APs (RAPs) with IPsec tunnel to the controller.

Management Auth

Table 51 *Management Auth Fixed Issue*

Bug ID	Description
75665, 75860	Symptom: A 3rd generation iPad running iOS 6.0.1 was incorrectly assigned to the default VLAN. Changes to how the controller manages PMKID data resolves this issue in ArubaOS 6.2.1.0. Scenario: This issue occurred in ArubaOS 6.1.3.5, when a Virtual AP was configured with both MAC authentication and 802.1x authentication, a VLAN derivation rule was configured on the MAC authentication server, and the derived VLAN was different from the default VLAN of the virtual AP.

Mesh

Table 52 *Mesh Fixed Issue*

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

RADIUS

Table 53 *RADIUS Fixed Issue*

Bug ID	Description
71836	<p>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 has resolved this issue.</p> <p>Scenario: This issue occurred when multiple users with the same MAC address tried to connect to the controller using a wired connection.</p>

Remote AP

Table 54 *Remote AP Fixed Issue*

Bug ID	Description
72454	<p>Symptom: When a UML290 USB modem was provisioned as a remote AP (RAP) uplink with the cellular_nw_preference parameter set to auto, the RSSI value for the 3G/4G uplink was not fetched dynamically. This issue is resolved by changes in ArubaOS 6.2.1.0 that enable an explicit dynamic RSSI check.</p> <p>Scenario: This issue was identified on RAPs with a UML290 modem uplink running ArubaOS 6.1.3.3.</p>

Spectrum-Infrastructure

Table 55 *Spectrum-Infrastructure Fixed Issue*

Bug ID	Description
79144	<p>Symptom: AP-105, AP-92 and AP-93 access points running ArubaOS 6.2.x and later versions unexpectedly stopped responding and rebooted. This issue is resolved in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue occurred when the spectrum monitoring option was enabled in the AP's 802.11a or 802.11g radio profile, allowing the AP to operate as a hybrid AP that both serves clients and performs spectrum analysis on a single radio channel.</p>

Station Management

Table 56 *Station Management Fixed Issue*

Bug ID	Description
74455	<p>Symptom: Incorrect information was present in the CLI help for the local-probe-req-threshold CLI command, suggesting that the local probe response feature had to be enabled before setting the local probe request threshold. This additional help string is removed in ArubaOS 6.2.1.0, as the local probe response feature is now enabled by default and this help message is no longer required.</p> <p>Scenario: This issue was not limited to any controller model, and appeared in the output of the wlan ssid-profile <profile> local-probe-req-threshold ? command.</p>

Switch-Platform

Table 57 *Switch-Platform Fixed Issues*

Bug ID	Description
62096	<p>Symptom: M3 controllers unexpectedly rebooted, and the log files for the event listed the reason as “User pushed reset”. This issue is resolved in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue was observed on an M3 controller when there was high traffic between the control plane and the datapath.</p>
75232	<p>Symptom: An internal system error occurred in the M3 controller and APs failed to connect to the controller.</p> <p>Scenario: The issue was seen 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 occurred in ArubaOS 5.0.4.6 and is not specific to any controller model.</p>
75411	<p>Symptom: 10GE ports on 7200 Series controllers report sporadic packets being dropped with CRC errors. This issue is resolved in ArubaOS 6.2.1.0.</p> <p>Scenario: This is an infrequent occurrence on these controllers.</p>
76852	<p>Symptom: The phonehome process sent incorrect user credentials to the corporate office. The issue is resolved by removing extra spaces from the user credentials sent via the command-line interface.</p> <p>Scenario: When the phonehome process was configured with SMTP credentials, it did not send the user credentials successfully to the corporate office. The issue occurred on controllers running ArubaOS 6.2.0.0 or later, and was not limited to any specific controller model.</p>
79385	<p>Symptom: A RAP-5WN associated to a 3200 controller failed to come up. The controller log files listed the reason as “AP-Group is not present in the RADIUS server.” Improvements to how remote AP route-cache entries are created resolves this issue in ArubaOS 6.2.1.0.</p> <p>Scenario: The issue by a gateway failover, and was seen on a RAP-5WN associated to a controller running ArubaOS 6.2.0.2 in a redundant (active/standby) gateway topology.</p>

Switch-Datapath

Table 58 *Switch-Datapath Fixed Issues*

Bug ID	Description
75843, 72359, 73246, 73256, 74575, 75700, 75753	<p>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. This issue is resolved in ArubaOS 6.1.3.7 and ArubaOS 6.2.1.0.</p> <p>Scenario: This issue occurred when an M3 controller experienced heavy traffic between the control plane module and the network.</p>
77535, 77537, 77024	<p>Symptom: Android, iOS, and MacOS devices were incorrectly blacklisted, and the log files for the event listed the reason as IP spoofing. Improvements to the ARP-spoofing feature resolved this issue in ArubaOS 6.1.3.6.</p> <p>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 these devices a leased out IP address, these clients were blacklisted.</p>
76307	<p>Symptom: A local controller crashed after a user added a VLAN ID in the master controller. Changes to how the controller decodes encrypted packets has resolved this issue in 6.2.1.0.</p> <p>Scenario: When a user added a VLAN ID to the master controller and executed the command <code>write-mem</code>, the local controller crashed due to an internal process failure. This issue was not specific to any controller or software version.</p>

Table 58 *Switch-Datapath Fixed Issues (Continued)*

Bug ID	Description
77484, 78181, 78667, 78873, 79682	<p>Symptom: Under very high load conditions, the controller datapath module can prevent users from associating or prevent associated users from passing traffic. In most cases, the controller will automatically reboot to recover from this scenario. Improvements to this internal controller module resolves this issue in ArubaOS 6.2.1.0.</p> <p>Scenario: This occurred on 7200 Series controllers running ArubaOS 6.2.0.x.</p>
77814	<p>Symptom: Errors in the internal control plane module caused a 3000 Series or M3 controller to unexpectedly reboot. The controller log files listed the reason for the reboot as “watchdog timeout.” Changes to CPU register access has resolved this issue in ArubaOS 6.2.1.0</p> <p>Scenario: This issue occurred on M3 or 3000 Series controllers in a master-local topology running ArubaOS 6.1.x.</p>
78326	<p>Symptom: A local M3 controller unexpectedly rebooted. The log files on the controller listed the reason for the reboot as “Datapath timeout.” Changes to unicast forwarding checks prevent this issue from occurring in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue was triggered when a controller that receives GRE-type PPP packets has a user role that enables source NAT.</p>
78593 79897	<p>Symptom: A controller running ArubaOS 6.2.0.1 stopped responding and reset. The controller crash logs lists reason for the reboot as “User Reboot.” Improvements to how in ArubaOS 6.2.1.0 manages coredumps resolves this issue.</p> <p>Scenario: This issue was observed in a 7200 Series controller in a master-local topology.</p>

UI Configuration

Table 59 *UI Configuration Fixed Issue*

76348	<p>Symptom: When an AP provisioned with a Fully Qualified Domain Name FQLN parameter using the format <code><floor>.<building>.<campus></code> was then reprovisioned, the AP provisioning page in the WebUI displayed the incorrect building value. This issue is resolved in ArubaOS 6.2.1.0.</p> <p>Scenario: This issue occurred on APs provisioned with the FQLN parameter, and was not limited to any specific controller or AP model.</p>

WebUI

Table 60 *WebUI Fixed Issues*

74227	<p>Symptom: The Monitoring tab of the WebUI and the output from the show ap active command did not match. The WebUI showed more APs than were actually up and the output of show ap active displayed the correct number. This issue is resolved in ArubaOS 6.2.1.0.</p> <p>Scenario: This occurred on master controllers running ArubaOS 6.1.3.2 or later if the bootstrap threshold in the ap system profile was set to over 40 minutes. In this instance, these APs were powered off when the controller attempted to send a configuration update. The APs failed to receive the update, and the controller marked the APs as down but did not update the AP database as well.</p>
76335	<p>Symptom: In the ArubaOS 6.2.0.x Dashboard tab the WebUI, the y-scale of the Noise Floor graph was inverted compared to previous versions of ArubaOS. This has been changed in ArubaOS 6.2.1.0, so -110 dBm is now shown at the bottom of the y-scale instead of the top.</p> <p>Scenario: This issue occurred on controllers running ArubaOS 6.2.0.x, and was not limited to a specific controller model.</p>

Resolved Issues in ArubaOS 6.2.0.3

The following issue was resolved in ArubaOS 6.2.0.3

Controller-Platform

Table 61 *Controller-Platform Fixed Issues*

Bug ID	Description
74048	Symptom: An issue was identified where a 7200 Series controller would crash due to AMSDU traffic. Scenario: This issue was observed when a client made a wireless connection to the AP-125, following which, and upon receiving the AMSDU traffic from the AP, the 7200 Series controller running ArubaOS 6.2.0.0, crashed. Changes that prevent the controller from sending zero-length message transfer descriptors in P2P messages, fixes this issue in ArubaOS 6.2.0.3.

Resolved Issues in ArubaOS 6.2.0.2

The following issues are resolved in ArubaOS 6.2.0.2:

Port-Channel

Table 62 *Port-Channel Fixed Issues*

Bug ID	Description
75044 75977	Symptom: After enabling LACP between 3200XM controllers and Juniper EX4200 switches, some of the ports did not come up. This issue has been resolved in ArubaOS 6.2.0.2. Scenario: This issue was observed on a 3200XM controller running ArubaOS 6.1.3.5.

Switch-Platform

Table 63 *Switch-Platform Fixed Issues*

Bug ID	Description
77230 77220	Symptom: An internal controller module stopped responding, corrupting data on the controller and causing the controller to become unusable. The only resolution is to replace the controller. This issue is resolved in ArubaOS 6.2.0.2. Scenario: This issue was observed on M3 and 3000 Series controllers running ArubaOS 6.2.0.0 and 6.2.0.1.

Resolved Issues in ArubaOS 6.2.0.1

The following issues were resolved in ArubaOS 6.2.0.1:

AP Regulatory

Table 64 *AP Regulatory Fixed Issues*

Bug ID	Description
76360	Scenario: The Korean (KR) regulatory domain did not support Dynamic Frequency Selection (DFS) for channels 52-64 on all AP types. ArubaOS 6.2.0.1 supports DFS for those channels for the KR domain.

Base OS Security

Table 65 *Base OS Security Fixed Issues*

Bug ID	Description
76233	Symptom: In ArubaOS 6.2.0.0, the Access Control List (ACL) limit was reduced by the number of roles defined. Roles no longer consume two ACLs per role. Scenario: This limitation occurred on a controller running ArubaOS 6.2.0.0. This limitation existed because two ACLs were created for every user role. Of these two ACLs, one was actively used for assigning user roles (stateful ACL) and the other was not used for any operation (stateless ACL).

Controller Platform

Table 66 *Controller Platform Fixed Issues*

Bug ID	Description
76592	Symptom: The phonehome module caused the controller to reboot continuously after upgrading to ArubaOS 6.2. Scenario: This issue occurred when a controller with a phonehome configuration upgraded to ArubaOS 6.2. The workaround for this issue required that you remove the phonehome smtp configuration before upgrading; this is no longer required.

DHCP

Table 67 *DHCP Fixed Issues*

Bug ID	Description
76672	Symptom: ArubaOS 6.2.0.0 did not allow a period (.) in DHCP pool names. This issue has been resolved in 6.2.0.1, and ArubaOS accepts DHCP pool names with periods, for example, 192.168.5. Scenario: This issue could occur on a controller running ArubaOS 6.2.0.0.

Startup Wizard

Table 68 *Startup Wizard Fixed Issues*

Bug ID	Description
76860	Symptom: In ArubaOS 6.2.0.0, after configuring a pre-authentication role with Captive Portal for a guest WLAN in the Startup Wizard, the configuration did not take effect. Scenario: This issue could occur on a controller running ArubaOS 6.2.0.0.

Station Management

Table 69 *Station Management Fixed Issues*

Bug ID	Description
76568 76593	Symptom: An internal process module (STM) crashed, causing the controller to restart. Scenario: This issue occurred on a network with Mesh APs and Airwave monitoring the controller. The controller attempted to send nonexistent data Airwave, causing the controller to experience a malfunction and restart. The workaround for this bug required that the command no mgmt-server type amp primary-server <server-IP> be used to remove all management server configuration from the controller. This is no longer required, and Channel Quality Metrics are now correctly shown by Airwave.

Resolved Issues in ArubaOS 6.2.0.0

The following issues were resolved in ArubaOS 6.2.0.0:

AP Datapath

Table 70 *AP Datapath Fixed Issues*

Bug ID	Description
63782	Symptom: An AP would crash and reboot randomly for unknown reasons. This issue has been fixed in ArubaOS 6.2.0.0. Scenario: This issue was observed only on legacy APs such as AP 60/61 running ArubaOS 6.1.2.x.
67214	Symptom: An AP would unexpectedly reboot. This issue was resolved by a change that allows the AP to handle an error by dropping a frame rather than rebooting. Scenario: Some occurrences of this issue impacted AP-120 Series access points configured with a 10Mb/s uplink.

AP Platform

Table 71 *AP Platform Fixed Issues*

Bug ID	Description
61604	Symptom: The option to sort the output of the show ap monitoring command did not work. Sorting can now be done by individual column name. Additionally, the user can now set the order (ascending or descending) of the output. Scenario: This issue could occur on all controller models.
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 are already existing. This issue was not specific to any controller model or software version.

AP Regulatory

Table 72 *AP Regulatory Fixed Issues*

Bug ID	Description
72390	Symptom: AP-175 access points did not come up in AP-mode in the Turkey domain. Support for the Turkey domain on AP-175 APs was introduced in ArubaOS 6.2.0.0. Scenario: This issue was identified on an AP-175 running ArubaOS 6.1.2.7.
73076	Symptom: When the RF 802.11g profile was set to channel 13 in European countries, the Invalid channel for 802.11G error message was displayed. Scenario: This issue occurred because support for the 8-12 and 9-13 High Throughput (HT) 40MHz channels for all European countries was not available. Due to this issue, the channel pairs 8-12 and 9-13 were not available in the regulatory domain profile for Germany and APs were not initialized in AP mode in the Turkey domain. This issue was found in 3000 Series controllers running ArubaOS 6.1.3.4 and later.
68431	Symptom: AP-135 access points did not support the Chile (CL) Country Domain. Scenario: This issue occurred on AP-135 APs running ArubaOS 6.1.3.5 and earlier, and now works properly.

AP Wireless

Table 73 *AP Wireless Fixed Issues*

Bug ID	Description
57624	Symptom: An AP-105 sometimes used excessive transmit power on the first transmit packet after the device reset. This issue prevented an AP-105 connected to a Cisco POE switch from getting power. This issue was resolved by a software change that defers transmission power or channel changes if any frames are pending. Scenario: This issue occurred on APs that scan outside home channels aggressively.
58361	Symptom: The noise floor reported right after an 802.11n AP reset was much higher than normal noise floor values, which sometimes resulted in client connectivity issues. This issue has been resolved. Scenario: This issue occurred when ARM scanning was enabled.
61669	Symptom: A local controller crashed due to an internal process (SAPD) error. Scenario: This issue occurred on a 651 controller running an ArubaOS version where the internal AP is enabled. The internal AP is now disabled so this issue no longer occurs.
65947	Symptom: AP-125 performance in 5GHz dropped significantly as RSSI dropped below -65 on ETSI DFS channels. The AP-125 performance in 5GHz now works properly in ArubaOS 6.2.0.0. Scenario: This issue was observed on an AP-125 running on ArubaOS 6.1.3.2.
65984	Symptom: Random AP rebootstrapping was observed along with poor WLAN performance and ping issue. This issue has been resolved in ArubaOS 6.2.0.0. Scenario: When a controller configured as default gateway in L2 network was responding to a large number of ARP requests, AP rebootstrapping was observed due to high CPU utilization. This issue was observed on controllers running ArubaOS 6.1.3.1 or earlier.
66780	Symptom: Some APs in the Turkey country code continuously rebooted when they were configured to use channels 100-140. This has been fixed by adding the missing channel definitions. Scenario: This occurred on the AP-60, AP-61, AP-65, AP-70, and AP-85 running on ArubaOS versions pre-6.2 Missing channel definitions in the driver caused the AP to crash.

Table 73 *AP Wireless Fixed Issues (Continued)*

Bug ID	Description
68347	<p>Symptom: Clients were unable to send packets on a virtual AP (VAP) if it had derived more than 32 unique VLANs. The maximum number of supported VLANs per VAP has been raised from 32 to 64.</p> <p>Scenario: This issue was not limited to any specific controller model. Clients were unable to send any packets on a VAP if that VAP had more than 32 unique VLANs. The higher limit alleviates this issue.</p>
69034	<p>Symptom: An issue was fixed where a TCP connection between a Panasonic tablet device and an Aruba 802.11n AP timed out frequently in the middle of data transmission.</p> <p>Scenario: This issue occurred when the tablet device went into power-save mode frequently during data transmission.</p>
69063 72123	<p>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 this data when the entry is not present.</p> <p>Scenario: This issue was identified on an AP terminating on a local 3000 Series controller running ArubaOS 6.1.3.2 in a master-local topology.</p>
71332	<p>Symptom: The handoff-assist feature sometimes failed to force a client off an AP when the RSSI dropped below the defined minimum threshold. Clients that exceed the maximum transmission fail threshold defined in the AP's WLAN SSID profile are now moved to a different access point by the handoff assist feature, regardless of whether they are roaming away from the AP.</p> <p>Scenario: This issue was identified in ArubaOS 6.1.3.4, and could impact any AP model.</p>
72382	<p>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 has been resolved in ArubaOS 6.2.0.0.</p> <p>Scenario: This issue occurred on 801.11n APs running on ArubaOS 6.1.3.2.</p>

Air Management

Table 74 *Air Management Fixed Issues*

Bug ID	Description
63116	<p>Symptom: The AP did not select the correct primary channel in a 40MHz channel for the Rogue-Aware assignment, and rogue containment was not effective for 40MHz rogue APs on certain channels. AP containment is now working properly on a band when a rogue AP is on a different channel than a valid AP.</p> <p>Scenario: This occurred on controllers running ArubaOS 6.1.x. AP-Mode APs are used to contain Rogue APs in other channels (rogue-aware ARM).</p>
66653	<p>Symptom: Master and local controllers were not maintaining the same suspect rogue confidence level between them. Suspect rogue confidence level is now sent from the AP to the WLAN Management System (WMS). If WMS is on the master, the local controller will use this to update its own state.</p> <p>Scenario: This issue could occur on controllers in a master-local topology, and was not limited to any specific controller model.</p>
67823	<p>Symptom: An issue was observed where a large number of BlockACK false positives appeared with the destination MAC address FF::FF::FF::FF::FF::FF. The AP channel scanning mechanism has been improved to prevent this.</p> <p>Scenario: This issue could occur on any controller with BlockACK detection enabled (this is enabled by default). A BlockACK attack is detected 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.</p>

Table 74 *Air Management Fixed Issues*

Bug ID	Description
68550	<p>Symptom: An internal module crash caused by a corrupt ProbePollResponse packet resulted in slow response of the WebUI and CLI. The controller now checks for message corruption in the ProbePollResponse packet sent from the AP to avoid this issue.</p> <p>Scenario: This issue was not limited to any specific controller or AP model and was caused by packet corruption on the network between the AP and controller.</p>
68669	<p>Symptom: When there were a large number of devices the database backup operation did not operate properly. As a result, issuing WMS CLI commands such as show wms general and show wms ge would trigger the error “Module WMS is busy. Please try later.”</p> <p>Scenario: This occurred on an M3 running ArubaOS 5.0.3.3. Database synchronization took a long time when there were a large number of entries that need updating.</p>

Authentication

Table 75 *Authentication Fixed Issues*

Bug ID	Description
61935 66647 67620 50192	<p>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 has been resolved.</p> <p>Scenario: This issue occurred in controllers running ArubaOS 6.1 or later when the SSID used 802.1X authentication.</p>
68412 74269	<p>Symptom: The controller incorrectly used MSCHAPv2 instead of Password Authentication Protocol (PAP) during management authentication. Changes in the internal management authentication process fixed this issue.</p> <p>Scenario: This issue occurred when a controller running ArubaOS 6.1.3.0 or later rebooted.</p>
72449	<p>Symptom: The AAA RADIUS attributes in the default configuration file were garbled and corrupted. This issue has been resolved in ArubaOS 6.2.0.0.</p> <p>Scenario: When custom RADIUS attributes were added and deleted multiple times with different attribute ID or vendor ID, incorrect attributes were seen in the configuration file. This issue was not limited to any specific controller model.</p>
72587 55202	<p>Symptom: When a client using MAC authentication roamed, the 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.</p> <p>Scenario: This issue occurred when MAC authentication was configured to derive a VLAN from a server followed by the 802.1X authentication.</p>
74831	<p>Symptom: When some clients were connecting in EAP-GTC mode, they experienced a token issue and failed authentication. This issue was fixed by sending EAP-Failure message along with the extended EAP-Failure message to the clients.</p> <p>Scenario: When RSA Token server sent a failure message, the controller forwarded the extended EAP-Failure message to the client. Some client application was unable to process the extended EAP-Failure message as it was expecting an EAP-Failure message. This issue was observed on controllers running ArubaOS 6.1.x or later.</p>

Base OS Security

Table 76 *Base OS Security Fixed Issues*

Bug ID	Description
55301	<p>Symptom: The starting and ending IP addresses in the default NAT pool dynamic-srcnat could not be modified on a 600 Series controller, although this setting could be modified on other controller models.</p> <p>Scenario: This issue was identified on a 600 Series controller running ArubaOS 5.0.3.3. The fix for this issue prevents users from changing this NAT pool on any controller type, as this value is dynamically created by the controller and should not be modified.</p>
68425	<p>Symptom: Editing an existing user role in the WebUI or issuing the show rights command in the CLI on a controller that has ethernet or MAC-based ACLs with more than 100 configured rules caused the controller to fail to respond properly. This issue has been resolved by a change that also divides the output of the show rights CLI command into sections that display up to 100 rules each.</p> <p>Scenario: This issue was first identified in ArubaOS 5.0.3.0, and occurred on a controller with an ACL configured with 100 rules or more.</p>
68467	<p>Symptom: The correct VLAN was assigned to a wireless client when the initial dot1x 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. Changes in ArubaOS 6.2.0.0 resolved this issue and now provides default_role and userderived_vlan information in log messages.</p> <p>Scenario: This issue that was noticed in controllers running ArubaOS 6.1.3.2.</p>
69859	<p>Symptom: A client was required to reauthenticate using captive portal authentication when roaming to a new AP. This issue was resolved in ArubaOS 6.2.0.0.</p> <p>Scenario: This issue occurred when a captive portal profile had configured both machine authentication and 802.1X authentication. When a client was momentarily assigned the machine authentication role during roaming, it was forced the user to authenticate using captive portal again.</p>
70307	<p>Symptom: A wired client behind an L-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.</p> <p>Scenario: This issue occurred when multiple wired clients were behind an L3-router. All the wired clients appeared to the controller to have the same mac-address, so after one wired client aged out, a second wired client bypassed the authentication and took over the role which associated to the first, aged-out wired client.</p>
70800	<p>Symptom: In the show user CLI command detailed output, the DHCP server IP address was not shown in certain conditions. This issue was fixed by changes to this command. Note that the DHCP server IP address no longer displays in the output.</p> <p>Scenario: The DHCP server did not send its own IP address in the siaddr field. This issue was observed in controllers running ArubaOS 6.1.x and later.</p>
73454	<p>Symptom: The internal controller module that manages authorization temporarily stopped responding, which impacted client authentication on the network. This issue was resolved with a change that ensures that when a Virtual AP (VAP) is disabled or removed, ACLs that are no longer used are not being referenced.</p> <p>Scenario: This issue occurred when a network administrator issued the write mem CLI command on controllers that are running ArubaOS 6.1.3.2 and earlier, and are configured with ap-group ACLs.</p>
73751	<p>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 has been fixed in ArubaOS 6.2.0.0.</p> <p>Scenario: This issue was identified on controllers in a master-standby topology, and occurred when a user was configuring authentication settings on the master controller, and issued the write mem command to save the configuration changes.</p>

Table 76 *Base OS Security Fixed Issues*

Bug ID	Description
74353 75343	<p>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.</p> <p>Scenario: This issue occurred on master controller running ArubaOS 6.1.3.4 with more than 255 local controllers.</p>
74537	<p>Symptom: The internal controller module that manages authorization temporarily stopped responding, which could impact client authentication on the network. This issue was resolved with a change to an internal statistics table that now bases the columns of the table on server statistics instead of server names.</p> <p>Scenario: This issue was identified in ArubaOS 6.1.3.4, and is not limited to any specific controller model.</p>

Captive Portal

Table 77 *Captive Portal Fixed Issues*

Bug ID	Description
53357 54900 74688	<p>Symptom: An issue was fixed where clicking Accept in the user agreement policy page of the captive portal, did not redirect users to the requested website. This issue was fixed by the addition of an internal check to verify if the client had accepted the acceptable user policy on the login page.</p> <p>Scenario: This issue occurred when a custom captive portal login page was configured to use an Acceptable User Policy with no user or guest logon role. This issue was found in controllers running ArubaOS 6.1.3.2 or earlier.</p>

Configuration

Table 78 *Configuration Fixed Issues*

Bug ID	Description
68197	<p>Symptom: The output of the show ip route command did not display the subnet mask information. This issue has been fixed in ArubaOS 6.2.0.0.</p> <p>Scenario: This issue occurred on controllers running ArubaOS 6.1.2.5.</p>

Controller-Platform

Table 79 *Controller-Platform Fixed Issues*

Bug ID	Description
52685, 52915, 61925, 64196, 64511, 65485, 65541, 65690, 75594, 79424	<p>Symptom: Errors in the internal datapath or control plane modules caused a M3 or 3000 Series controllers to unexpectedly reboot. Improvements to the internal datapath now prevent this error.</p> <p>Scenario: This issue occurred on M3 or 3000 Series controllers in a master-local topology</p>

Table 79 *Controller-Platform Fixed Issues*

Bug ID	Description
69595	<p>Symptom: The Monitoring section of the WebUI reported an incorrect number of controllers as up when a new controller when a new controller had the same IP address as the controller it replaced. This issue was resolved by improvements to how controller serial numbers are handled after a duplicate controller IP entry is removed.</p> <p>Scenario: This issue occurred on 3000 Series controllers running ArubaOS 6.1.2.3.</p>
70075	<p>Symptom: Multiple VLANs could not be added into a port channel using the WebUI. The WebUI is now working properly and supports port channel configurations.</p> <p>Scenario: This issue in ArubaOS versions earlier than ArubaOS 6.2.0.0, and was not limited to any specific controller model.</p>

DataPath/Platform

Table 80 *DataPath/Platform Fixed Issues*

Bug ID	Description
60854 64569	<p>Symptom: A controller experienced high CPU utilization when there was large amounts of IPv6 neighbor discovery traffic. This issue was fixed by changes to how ArubaOS manages IPv6 Router Advertisements (RAs).</p> <p>Scenario: This issue was found in M3 controllers running ArubaOS 6.1.3.2 or earlier.</p>
66798 69102 68829	<p>Symptom: Users experienced low throughput after enabling a bandwidth contract. This issue was resolved by an increase in the queue size for lower contract rates.</p> <p>Scenario: This issue occurred when contract rates less than 1 Mbps were applied to bandwidth contracts on controllers running ArubaOS 6.1.3.0.</p>

Dot1x

Table 81 *Dot1x Fixed Issues*

Bug ID	Description
71930	<p>Symptom: Client 802.1x authentication failed after a new security certificate was uploaded on a controller. This issue was the result of a rare condition where some values in a RSA private key were less than 128 bytes in length, and has been resolved by changes to how the controller manages RSA keys.</p> <p>Scenario: This issue occurred on controllers running 6.1.3.2 in a master-local topology and updated with new certificates.</p>
75545	<p>Symptom: If a Change of Authorization (CoA) request is used to assign a role to a client, the PMK cache is not updated with the CoA information. In a roaming scenario, where the PMK cache is used to bypass full authentication, CoA information is lost. This issue was resolved with a fix that ensures that the cache is updated with the correct CoA role.</p> <p>Scenario: This issue was not limited to a specific controller model, and was first identified in ArubaOS 6.1.3.5.</p>

DPA

Table 82 *DPA Fixed Issues*

Bug ID	Description
69226	<p>Symptom: A controller upgrade from ArubaOS 3.4.4.2 to ArubaOS 6.1.3.1 triggered the configuration error message Configuration Error: Unknown authentication SecureID. Changes to how the controller manages SecureID authentication has resolved this issue.</p> <p>Scenario: This issue occurred on a controller where clients used SecureID authentication and a point-to-point protocol (PPP) to log in to the network.</p>

Dynamic Authorization

Table 83 *Dynamic Authorization Fixed Issues*

Bug ID	Description
31834	<p>Symptom: The user rights of a client did not change correctly when the user roamed to an AP with an ACL based upon an AP-Group.</p> <p>Scenario: This issue occurred on a controller running ArubaOS 3.3 that used captive portal authentication and had two configured AP groups with different access roles.</p> <p>The fix for this issue removed the unnecessary ap-group option from the CLI command user-role <name> access list.</p>

IPsec

Table 84 *IPsec Fixed Issues*

Bug ID	Description
70903	<p>Symptom: The internal controller module that handles IPsec consumes an unusually high amount of CPU resources, and the output of the show crypto isakmp stats CLI command showed an unusually large number of transport reinit. This issue has been resolved in ArubaOS 6.2.0.0</p> <p>Scenario: This issue was observed in ArubaOS 5.0.2.0, but is not associated with a specific controller type.</p>
72356	<p>Symptom: Site to Site VPN between two controller only works when it is initiated from a single side. The fix for this issue allows either controller to act as the initiator.</p> <p>Scenario: This issue occurred on local controllers (a 620 and M3) configured to use a site-to-site VPN with the force-natt and pre-connect VPN features enabled. It was first identified in ArubaOS 6.1.3.3</p>
72681 72203	<p>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 be busy and fail to respond. Changes to how the controller managed stale entries in an internal hash table has resolved this issue.</p> <p>Scenario: This issue occurred on a M3 controller in a master-local topology, where the M3 master controller was running ArubaOS 6.1.3.2.</p>

Mesh

Table 85 *Mesh Fixed Issues*

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

RAP

Table 86 *RAP Fixed Issues*

Bug ID	Description
67191	Symptom: A remote AP rebooted with following error message: Module SAPM client is busy. Please try later. This issue has been resolved. Scenario: When more than 8 Virtual APs were configured with Remote-AP operation set to Always , the AP would reboot. This issue was observed on an AP-135 running ArubaOS 6.1.2.8.

Remote Access Point

Table 87 *Remote Access Point Fixed Issues*

Bug ID	Description
49070	Symptom: A Remote AP (RAP) failed to register in the controller. The fix for this issue checks if the RAP DHCP subnet is the same as the LMS or Tunnel-IP, and changes the RAP DHCP if it matches either value. Scenario: When the controller IP address was the same as that of the RAP's DHCP server, the packets were not exchanged between the RAP and the controller. Due to this, the RAP could not download any configuration from the controller. This issue was found in ArubaOS 5.0.2 and later.
75141	Symptom: Bridge mode clients do not receive an IP address from the external DHCP server. Scenario: This issue occurs due to the restart of an internal AP process (STM module) which causes disruptions to client connectivity and packet forwarding.

Roles/VLAN Derivation

Table 88 *Roles/VLAN Derivation Fixed Issues*

Bug ID	Description
51691 56746	Symptom: A client was assigned an incorrect role when using DHCP user derivation rules and captive portal authentication. The fix for this issue allows these clients to receive their correct role. Scenario: This issue occurred when a client was incorrectly assigned a derived role during DHCP-renew, and when in Captive Portal authentication mode. This issue was seen in ArubaOS 6.1.0.0.

Table 88 *Roles/VLAN Derivation Fixed Issues*

Bug ID	Description
54037 56411 57168 60866 61411 62342 62808 62244 62403 55898	<p>Symptom: The controller assigned VLAN 1 to wired and wireless users that connected over a GRE tunnel. This issue was fixed by improvements to the user authentication process.</p> <p>Scenario: This issue occurred when the users connected to a controller over a GRE tunnel, and was found in controllers running ArubaOS 6.1 or earlier.</p>

Station Management

Table 89 *Station Management*

Bug ID	Description
64452	<p>Symptom: The warning message “number of VLANs limit exceeded 32” appeared when over 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.</p> <p>Scenario: This issue occurred on any situation in which 32 VLANs are configured per VAP.</p>

STP

Table 90 *STP Fixed Issues*

Bug ID	Description
64164	<p>Symptom: The Spanning Tree port cost calculation was incorrect. The fix allows the output of the show spanning-tree interface CLI command to display the correct path cost.</p> <p>Scenario: This issue was observed on a controller with Spanning Tree enabled.</p>

UI-Configuration

Table 91 *UI Configuration Fixed Issues*

Bug ID	Description
52624	<p>Symptom: The WebUI did not allow users to add a new policy with a destination netmask in standard format (255.255.255.0). This issue has been resolved in ArubaOS 6.2.0.0.</p> <p>Scenario: While adding a new policy in the Configuration>Security>Access Control>User Roles>Add Role>Add new policy page in the WebUI, the destination mask was not accepted in dotted decimal format. This issue was not limited to any specific controller model.</p>

UI-Monitoring

Table 92 *UI Monitoring Fixed Issues*

Bug ID	Description
65323	Symptom: User IDs did not display properly in the WebUI. This issue was solved by a change that allows the user table to display only 50 rows of output at once. Scenario: The Dashboard > Clients page in the WebUI did not display the user IDs properly when special characters such as '[' were used in the user ID. This issue was not limited to a specific controller model.
66887 62519	Symptom: The WebUI displays a javascript error. This issue was fixed by changes to how javascript is loaded on the WebUI page. Scenario: When a user selected the status button on the Monitoring > Access Points page, the WebUI displayed a blank page with a javascript error. This issue was observed on controllers running 6.1.2 or earlier and was not limited to a specific controller model.

Voice

Table 93 *Voice Fixed Issues*

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

WebUI

Table 94 *WebUI Fixed Issues*

Bug ID	Description
62907	Symptom: The Access Control List (ACL) rules associated with host entries could not be deleted from the WebUI. Changes to the internal command syntax fixed this issue. Scenario: This issue occurred when a user tried to delete the ACL rules associated with netdestination host entries from the WebUI. This issue occurred because the netmask keyword was added to the command generated for the ACL instead of the host keyword. This issue was found in controllers running ArubaOS 6.1.2.6.
66388	Symptom: The WebUI displayed AAA test authentication messages in red text. WebUI updates have changed the authentication messages, so that a successful AAA test authentication on the Diagnostics>Network> AAA Test Server page of the WebUI is now displayed in green text. Scenario: This issue was found in controllers running ArubaOS 6.1.3.2 or earlier.
66516	Symptom: APs were not sorting properly by name in the Configuration > Wireless > AP Installation > Provisioning page of the WebUI and the UI sorted only the APs in the current page instead of the entire list. Scenario: When a user was sorting the APs in the Provisioning page, only the APs in the current page were sorted instead of the entire list of APs distributed in multiple pages. This issue was found in the controllers running ArubaOS 6.1.3.6 or earlier.

Table 94 *WebUI Fixed Issues (Continued)*

Bug ID	Description
67304	<p>Symptom: A user was unable to provision an AP-61 as a RAP from the WebUI of a master controller. Improvements to how the controller handles FQLN campus names with special characters fixed this issue.</p> <p>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 Fully Qualified Location Name (FQLN) campus name.</p>
70844	<p>Symptom: Firewall policies could not be deleted from the Configuration>Security>Access Control>User Roles tab in the WebUI. Changes to the internal command syntax fixed this issue.</p> <p>Scenario: When a user edited a firewall policy from the User Roles tab in the WebUI, some ACL rules that contained the host keyword could not be deleted. This issue occurred because ArubaOS considered single IP addresses in the source and destination to be a network value instead of a host value. This issue was found in controllers running ArubaOS 6.1.3.2 or later.</p>
73656	<p>Symptom: Creating a user role in the WebUI during a session that timed out caused a loop of User not logged on error messages. This issue was fixed by improvements to the internal session timeout settings.</p> <p>Scenario: This issue occurred when an administrator used Internet Explorer to add a user role and the WebUI timed out. It was observed on a 3000 Series controller running ArubaOS 6.1.3.1.</p>

WMM

Table 95 *WebUI Fixed Issues*

Bug ID	Description
65159	<p>Symptom: The Tx WMM [xx] Dropped counter in the output of the show ap debug client-stats CLI command did not accurately display dropped frames. This issue was resolved by a change that ensured the counter for dropped WMM frames incremented every time a frame is dropped.</p> <p>Scenario: This issue occurred on ArubaOS 6.1.2.7 for AP-135 and AP-105 access points.</p>

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

Maximum DHCP Lease Per Platform

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

Table 96 *Maximum DHCP Lease Per Platform*

Platform	Maximum
7200 Series	5000
M3	512
3200XM	512
3400	512
3600	512
600 Series	512

Known Issues

802.1X

Table 97 *802.1X Known Issue*

Bug ID	Description
74663	<p>Symptom: Clients are not able to reauthenticate after rebooting or logging off the network.</p> <p>Scenario: This issue is observed on a client running Windows 7 with machine authentication, and connected to a Cisco phone. This issue only occurs when the eapol-logoff feature that handles EAPOL-LOGOFF messages is enabled in the controller's 802.11X authentication profile.</p> <p>Workaround: Disable the Handle EAPOL-Logoff setting in the 802.11X authentication profile (This setting is disabled by default.)</p>

AP Wireless

Table 98 *AP Wireless Known Issues*

Bug ID	Description
74984	Symptom: Blackberry devices experience severe ping losses when connected to a high throughput SSID. Scenario: This issue occurs on AP-135 access points configured to use a high-throughput SSID and running ArubaOS 6.1.3.4. Workaround: None
75564	Symptom: An internal process in an AP-135 running ArubaOS 6.1.3.3 restarts, causing that AP to unexpectedly reboot. Scenario: This issue can occur if the Collect Stats parameter is enabled in the WMS General profile, and the Monitored Device Stats Update Interval parameter in the IDS General profile is set to a non-zero value. Workaround: Set the Monitored Device Stats Update Interval in the IDS General profile to 0, its default value.
84329	Symptom: AP-175 access points experienced significant ping losses, causing clients to disconnect. Scenario: This issue occurred on AP-175 associated to a standalone 6000 controller running ArubaOS 6.2.1.0. Workaround: None.

AP Platform

Table 99 *AP Platform Known Issues*

Bug ID	Description
58011 61100 60846 64517 66118 66128 66185 66596 64526 61539 61196 67435 67670 67671 67673 67871 67872 68875 68937 72069 74142 75366 75539 75703 75366	Symptom: A 651 controller reboots unexpectedly after enabling the internal AP. Scenario: This issue is observed in 651 controllers running ArubaOS 5.0 or later. Workaround: In ArubaOS 6.2.1.2, the internal AP is disabled in this controller.

Authentication

Table 100 *Authentication Known Issue*

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

Base OS Security

Table 101 *Base OS Security Known Issues*

Bug ID	Description
55419	<p>Symptom: An internal ArubaOS process (Certmgr) becomes busy when the OCSP server is unreachable.</p> <p>Scenario: Users are unable to authenticate because this process is busy queuing the OCSP requests. (Clients using 802.1X, IKE, and management authentication can be affected). This issue is observed in ArubaOS 6.2.</p> <p>Workaround: None</p>
75565	<p>Symptom: A wired user is incorrectly assigned to a initial user role instead of a user role derived from DHCP fingerprinting.</p> <p>Scenario: This issue is observed in ArubaOS 6.1.3.4, and is not specific to any controller platform.</p> <p>Workaround: Delete the user from the user table, and verify that the corresponding bridge entry is removed from the datapath before reconnecting the user.</p>
76291	<p>Symptom: An internal controller process (resolvwrap) crashes at random intervals when a RADIUS authentication server is configured with a host name.</p> <p>Scenario: This crash does not have any impact on the ArubaOS operation as the resolvwrap process is used only for resolving the host name configured for authentication server periodically. If host-name resolution fails due to a crash then subsequent attempts to resolve the host name are successful.</p> <p>Workaround: If this crash is observed continually, use an IP address is used instead of a host name in the server authentication profile.</p>
76424	<p>Symptom: Issuing the CLI command aaa user delete all on a 7200 Series controller managing over 14,000 users causes internal controller process modules that manage AP management, user association and user authentication to become busy and cause the controller to become unresponsive.</p> <p>Scenario: This issue occurred on a 7200 Series controller running ArubaOS 6.2.</p> <p>Workaround: Delete fewer users at a time.</p>
79467	<p>Symptom: User table entries for users that disconnect from the network are not correctly aging out and getting removed from the controller user table.</p> <p>Scenario: This issue was observed on a 7240 local controller running ArubaOS 6.2.0.2 in a master/local topology.</p> <p>Workaround: None.</p>

Table 101 *Base OS Security Known Issues (Continued)*

Bug ID	Description
81243	<p>Symptom: When an AP boots up, the controller log files display the message <i>AP-Group is not present in the RADIUS server for username=<mac address>; AP will take the ap-group as provisioned in the AP.</i></p> <p>Scenario: This message appears when an AP boots, and although it does not indicate a problem with the boot process, the current wording of the message can be confusing. The error message is not limited to any specific AP model or software version.</p> <p>Workaround: No workaround is needed since this error message does not indicate a functionality issue.</p>
82540	<p>Symptom: The internal controller module that manages handles user authentication stopped responding, preventing users from authenticating until the process automatically restarted.</p> <p>Scenario: This issue occurred on a M3 controller module running ArubaOS 6.2.0.2 in a master-local topology.</p> <p>Workaround: None</p>

Controller-Platform

Table 102 *Controller-Platform Known Issues*

Bug ID	Description
69277	<p>Symptom: The Point-to-Point Tunneling Protocol (PPTP) VPN connection is lost when a user tries to connect to the PPTP server using a Windows 7 client as the VPN client, then switches to split-tunnel forwarding mode.</p> <p>Scenario: This issue is seen in ArubaOS 6.1.3.2.</p> <p>Workaround: None.</p>
74428	<p>Symptom: On the dual-personality RJ45 ports 0/0/0 and 0/0/1, if the port speed is forced from/to 1Gbps to/from 10/100Mbps when traffic is flowing, traffic forwarding on the port can stop in an unintended manner.</p> <p>Scenario: This issue has been observed in controller models 7210, 7200 and 7240 running ArubaOS 6.2 in configurations or topologies where traffic is flowing. The trigger is unknown.</p> <p>Workaround: Change the speed on the port following these steps:</p> <ol style="list-style-type: none"> 1. Shut the port. 2. Change the speed on the port. 3. Open the port.
76220	<p>Symptom: A controller crashes due to a virtual AP configuration change.</p> <p>Scenario: In a high traffic deployment, when a virtual AP with active client associations is removed from an AP group, a race condition may trigger a controller crash.</p> <p>Workaround: Before removing a virtual AP profile from an AP group, wait for all active associated clients to disassociate or time out. Use the show ap association command to verify the virtual AP client association status.</p>

Controller-Datapath

Table 103 *Controller Datapath Known Issue*

Bug ID	Description
83029	<p>Symptom: A 7200 Series or 3000 Series controller with the firewall-visibility beta feature enabled may fail to respond if the controller has a high number of IPv6 sessions.</p> <p>Scenario: This issue occurred on a controller running ArubaOS 6.2.1.0. The datapath CPUs utilization reaches 100% and fails to return to nominal levels.</p> <p>Workaround: Issue the CLI command no firewall-visibility to disable this feature.</p>

Table 103 *Controller Datapath Known Issue (Continued)*

Bug ID	Description
84494	<p>Symptom: A controller unexpectedly rebooted. The log files for the event listed the reason for the reboot as “Nanny rebooted machine - udbserver process died.”</p> <p>Scenario: This issue occurred on a standalone master 7210 controller with one associated AP-135 access point.</p> <p>Workaround: None.</p>

IPsec

Table 104 *IPsec Known Issue*

Bug ID	Description
75891	<p>Symptom: When an idle user times out, the controller does not send a ping request before aging out the user. The user is aged out immediately. This applies to VPN and VIA-VPN users as well. When the users age out, the VPN tunnel will also go down.</p> <p>Scenario: This occurs on controllers running ArubaOS 6.2 or later, when there is no data for the user during the ageout time period. For VPN and VIA-VPN users, if the IPsec tunnel does not have any data for the configured user ageout time, the user will age out and the tunnel will be deleted.</p> <p>Workaround: Increase the value of the user ageout time. The default value is 5 minutes. This issue can also be avoided if you ensure that there is always some data sent from the user.</p>

IPv6

Table 105 *IPv6 Known Issues*

Bug ID	Description
74367	<p>Symptom: Clients using temporary IPv6 addresses are not be able to communicate as traffic is getting dropped.</p> <p>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.</p> <p>Workaround:</p> <ul style="list-style-type: none"> • 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.
77012	<p>Symptom: IPv6 clients experience poor network performance compared to IPv4 clients.</p> <p>Scenario: This issue impacts clients associated with APs in tunneled forwarding mode running ArubaOS 6.2.0.0.</p> <p>Workaround: If possible, configure AP supporting IPv6 clients to use bridge forwarding mode instead of tunnel forwarding mode.</p>

Management Auth

Table 106 *Management Auth Known Issue*

Bug ID	Description
81517	<p>Symptom: The controller log files are being flooded with the error <i>Datapath-UserRem(IPv4/L2) failed: mac=<controller-mac-addr></i>.</p> <p>Scenario: This issue occurred in ArubaOS 6.2.0.0 on an M3 controller and an AP-93 remote AP operating in split-tunnel forwarding mode and configured to support captive portal authentication.</p> <p>Workaround: None</p>

Master-Redundancy

Table 107 *Master-Redundancy Known Issues*

Bug ID	Description
70343	<p>Symptom: Custom captive portal pages are not synced between master and standby when set up to do so.</p> <p>Scenario: For all software versions, when the standby becomes the master, the custom captive portal page will no longer show up during CP authentication. The database synchronize command only copies database files and RF plan floor plan backgrounds.</p>
75367	<p>Symptom: Enabling web-server debug logging using the CLI command logging level debugging system subcat webserver does not take effect until you restart the HTTPD process.</p> <p>Scenario: This happens on all controller models running ArubaOS 3.x, 5.x and 6.x software versions when web-server debug logging mode is enabled.</p> <p>Workaround: Restart the HTTPD process in order to enable debug logging.</p>

Mobility

Table 108 *Mobility Known Issues*

Bug ID	Description
58883 60328	<p>Symptom: In a Layer-3 IP mobility enabled network, when the client moves from a Home Agent network to a Foreign Agent network, the IPv4 address of the client changes. This prevents the client from sending traffic.</p> <p>Scenario: Layer-3 IP mobility does not work when IPv6 packet processing is enabled on the controller. This issue is found in controllers running ArubaOS 6.2.1.2 or earlier.</p> <p>Workaround: Do not issue the router enable command along with the ipv6 enable command in the controller.</p>
63163	<p>Symptom: There is an increase in datapath CPU utilization in the controller.</p> <p>Scenario: This issue occurs in a Layer-3 IP mobility enabled network, where a wired 802.1X client is connected to an untrusted port and the IP address of the client changes rapidly. The Layer-3 IP mobility edits the bridge table entries for such clients. This results in an increased CPU utilization. This issue is found in controllers running ArubaOS 6.2 or earlier.</p> <p>Workaround: Do not change the IP address of the wired client at a rapid rate.</p>

Remote AP

Table 109 *Remote AP Known Issues*

Bug ID	Description
79799	<p>Symptom: A remote AP (RAP) failed to come up using a 3G uplink or failover to a 3G uplink when the signal strength of the 4G network was significantly lower than the 3G signal, or when only a 3G signal was available.</p> <p>Scenario: This issue was identified on a RAP-5WN AP connected to a 3200 controller and provisioned with both 4G and 3G parameters.</p> <p>Workaround: Rebootstrap the RAP to restore the 3G network connection.</p>
81245	<p>Symptom: The user table contains stale entries for users that aged out or disassociated from the network.</p> <p>Scenario: This issue occurs when users associated to a AP in split-tunnel forwarding mode and using captive portal authentication roam to multiple APs exhibiting the same ESSID.</p> <p>Workaround: Periodically delete the stale entries from the user table.</p>
83002	<p>Symptom: A wireless client connected to a backup virtual AP configured in bridge forwarding mode is unable to get an IP address from an assigned VLAN.</p> <p>Scenario: This issue occurred when the controller upgraded to ArubaOS 6.2.</p> <p>Workaround: Once the AP connects to the controller, remove the virtual AP profile from the ap-group/ap-name configuration, then return the virtual AP profile to the ap-group/ap-name settings.</p>
84004	<p>Symptom: In some instances calls from IP phones connected to a RAP-3WN AP fail because the AP drops packets.</p> <p>Scenario: This issue occurs on IP phones connected to an AP in tunnel forwarding mode, and was first identified in ArubaOS 6.2.0.2.</p> <p>Workaround: None.</p>

RAP + BOAP

Table 110 *RAP + BOAP*

Bug ID	Description
84752 85629 86217 86375 86452 86738 86742 86743 87690 87777 87793 87844 88139 88285 88577 88755 88828 89076 89168 89701 89719 90243 90483 90846 91096 91297 91595 92062 92088 92482 92996 93685 93864 93865	Symptom: AP-61, AP-65, AP-70, AP-93H, RAP-2WG, AP-135, AP-124 and AP-125 campus APs (CAPs) and remote (RAPs) stop responding and reboot. Scenario: This issue is triggered by insufficient memory and is not specific to any controller model.

Station Management

Table 111 *Station Management Known Issues*

Bug ID	Description
72194	Symptom: When VLAN pooling is used with the assignment type EVEN, the user VLAN changes when the client roams from AP to AP, but the IP address remains the same until a release/renew is executed on the client device. Scenario: This issue occurs on any controller model with the VLAN mobility and preserve VLAN features enabled. When these features are enabled, the bridge table of the controller keeps user entries for 12 hours. This issue occurs when the STM module (an internal process) of the controller does not find the entry in the bridge lookup result. Workaround: Disable VLAN mobility and the preserve VLAN feature.
82012	Symptom: An internal controller process kept restarting, preventing the controller from servicing clients. Scenario: This issue was identified when the controller upgraded its image, and was triggered when the controller expected IKEv2 information that was missing from the mysql global AP database. Workaround: none.

WebUI

Table 112 *WebUI Known Issue*

Bug ID	Description
55981	<p>Symptom: When a user views the Spectrum UI with saved preferences from a newer version of ArubaOS, the UI will display charts incorrectly.</p> <p>Scenario: After downgrading from a newer version of ArubaOS, such as from 6.2.x to 6.1.x with saved Spectrum preferences, will cause the Spectrum UI to display charts incorrectly. This is due to the difference between the Spectrum UI in 6.2 and previous versions.</p> <p>Workaround: Use the command ap spectrum clear-webui-view-settings on the controller to delete the saved preferences.</p>
66521	<p>Symptom: Two Apply buttons are displayed in the WebUI when adding users to the internal database.</p> <p>Scenario: While creating a new user in the WebUI, two Apply buttons appear in the Configuration > Security > Authentication > Internal DB page due to incorrect labeling of the buttons. This issue is not limited to a specific controller model.</p> <p>Workaround: Use the Apply button at the top to add a new user. Use the Apply button at the bottom to apply any user list changes.</p>
77542	<p>Symptom: Upgrading from a local file does not work on the 600 Series controller.</p> <p>Scenario: For the local file upgrade to be successful, the controller must have at least 75 MB of free memory. When upgraded to ArubaOS 6.2, the 600 Series controller has only 77 MB of free memory remaining. And when the browser UI is launched, the free memory is decreased to 75 MB. In this case, the local file upgrade will fail. It is recommended that you do not use the local file upgrade function in the controller has less than 80 MB of free memory.</p> <p>Workaround: None. Use the USB, TFTP, SCP, or CLI option to upgrade instead.</p>
80233 82724	<p>Symptom: The Monitoring>Access Points and Monitoring>Network>All Access Points pages of the controller WebUI show APs as down, even they are shown as up in the command-line interface.</p> <p>Scenario: This issue occurred on a master/local topology with one 6000 master controller and two local controller running ArubaOS 6.2.1.0.</p> <p>Workaround: none</p>
82611	<p>Symptom: The Dashboard>Access Points WebUI page of a controller running ArubaOS 6.2.0.3 does not correctly display AP information.</p> <p>Scenario: Accessing the Dashboard>Access Points page can trigger the following error in the controller log files: "An internal system error has occurred at file <i>mon_mgr.c</i> function <i>mon_mgr_proc_trend_query</i> line 4142 error <i>PAPI_Send</i> failed: Cannot allocate memory." This issue is not related to a memory allocation error.</p> <p>Workaround: None</p>
82502	<p>Symptom: A controller does not correctly display the Monitoring>Network Summary WebUI page.</p> <p>Scenario: This issue was observed on a 3600 standalone master controller running ArubaOS 6.2.1.0.</p> <p>Workaround: None.</p>

WMM

Table 113 *WMM Known Issues*

Bug ID	Description
68503	Symptom: The controller chooses an incorrect WMM priority (background instead of best-effort) in the downstream traffic. When same DSCP value is mapped to two different access categories, the lower of the two is used for the downstream traffic. Scenario: This issue is observed on controllers running ArubaOS 6.2 or lower in Tunnel and D-Tunnel modes. Workaround: None.

Issues Under Investigation

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

OSPF

Table 114 *OSPF Issues Under Investigation*

Bug ID	Description
82730	Symptom: A 7220 controller running ArubaOS 6.2.1.0 is not learning its default IP route using OSPF.

Controller-Datapath

Table 115 *Controller Datapath Issues Under Investigation*

Bug ID	Description
84105	Symptom: A local controller is unable to send packets. The controller log files include a warning message stating that “Configured Session limit reached for client.”
84718 84719 84725	Symptom: The internal controller module that manages station authentication stopped responding, temporarily preventing clients from associating to the network. This issue was identified on a 7200 Series controller running ArubaOS 6.2.1.1.
84563 84071	Symptom: A controller unexpectedly rebooted. The log files for the event listed the reason for the reboot as “Datapath exception.” This issue occurred on a 3000 Series and 7200 Series controller running ArubaOS 6.2.1.0.

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



CAUTION

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

Topics in this chapter include:

- [Upgrade Caveats on page 71](#)
- [Important Points to Remember and Best Practices on page 72](#)
- [Memory Requirements on page 73](#)
- [Backing up Critical Data on page 73](#)
- [Upgrading in a Multi-Controller Network on page 75](#)
- [Upgrading to 6.2.x on page 75](#)
- [Downgrading on page 79](#)
- [Before You Call Technical Support on page 81](#)

Upgrade Caveats

Before upgrading to any version of ArubaOS 6.2, take note of these known upgrade caveats.

- Beginning with ArubaOS 6.2, the default **NAS-port-type** for management authentication using MSCHAPv2 is **Virtual** instead of **Wireless**. If your configuration uses the NAS-port-type in any derivation or access rules, this value will change for management user requests from the controller. This behavior is in line with IEEE RFC 2865. There is no change in behavior for management authentication using PAP.
- Beginning with ArubaOS 6.2, you cannot create redundant firewall rules in a single ACL. ArubaOS will consider a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
 - source IP/alias
 - destination IP/alias
 - proto-port/service

If your pre-6.2 configuration contains an ACL with redundant firewall rules, upon upgrading, only the last rule will remain.

For example, in the below ACL, both ACE entries could not be configured in ArubaOS 6.2. Once the second ACE entry is added, the first would be over written.

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

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

- ArubaOS 6.2.x is supported only on the newer MIPS controllers (7200 Series, M3, 3400, 3600, 600 Series, 3200XM, and any 3200 controller with its memory upgraded using 3200-MEM-UG kit).

Legacy PPC controllers (200, 800, 2400, SC1 and SC2) and 3200 (default memory) are *not* supported. DO NOT upgrade to 6.2.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 75](#)).

- User Idle Timeout behavior has changed in ArubaOS 6.2. For more information, see [User Idle Timeout Behavior Change on page 30](#).
- Upon upgrade to ArubaOS 6.2, the internal AP of the 651 controller will be disabled. The controller will then operate as a 650 controller.
- 3200XM controllers with 1GB of memory can be upgraded to ArubaOS 6.2. The 3200 controller with 512MB of memory is not supported by ArubaOS 6.2. For more information, see "[Changes to Hardware Support on page 31](#)."

Important Points to Remember and Best Practices

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

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

- If possible, use FTP to load software images to the controller. FTP is faster 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 6.2.1.2, assess your software license requirements and load any new or expanded licenses you require. For a detailed description of these new license modules, refer to the “Software Licenses” chapter in the user guide.

Memory Requirements

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

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



CAUTION

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

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

- **Crash Data:** Issue the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in [Backing up Critical Data on page 73](#) 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 73](#) to back up the flash directory to a file named **flash.tar.gz**, then issue the command **tar clean flash** to delete the file from the controller.
- **Log files:** Issue the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in [Backing up Critical Data on page 73](#) to copy the **logs.tar** file to an external server, then issue the command **tar clean logs** to delete the file from the controller.

Backing up Critical Data

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

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

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

Back Up and Restore Compact Flash in the WebUI

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

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

You can later copy the backup file from the external server to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.

6. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page. Click **Restore**.

Back Up and Restore Compact Flash in the CLI

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

1. Enter enable mode in the CLI on the controller, and enter the following command:

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

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

```
(host) # backup flash
```

```
Please wait while we tar relevant files from flash...
```

```
Please wait while we compress the tar file...
```

```
Checking for free space on flash...
```

```
Copying file to flash...
```

```
File flashbackup.tar.gz created successfully on flash.
```

3. Use the **copy** command to transfer the backup flash file to an external server or storage device:

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

```
(host) copy flash: flashbackup.tar.gz usb: partition <partition-number>
```

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

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

```
(host) # copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
```

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

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

Upgrading in a Multi-Controller Network

In a multi-controller network (a network with two or more Aruba controllers), special care must be taken to upgrade all controllers based on the controller type (master or local). Be sure to back up all controllers being upgraded, as described in [Backing up Critical Data on page 73](#).



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 6.2.1.2:

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

Upgrading to 6.2.x

Install using the WebUI



Confirm that there is at least 60 MB of free memory and at least 75 MB of flash available for an upgrade using the WebUI. For details, see [Memory Requirements on page 73](#)



600 Series controllers running ArubaOS 6.2 cannot use the Local File upgrade option in the WebUI for further upgrades due to insufficient memory. Use other upgrade options in the WebUI.

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 6.2.1.2.

- For ArubaOS 3.x.versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.
- For ArubaOS RN-3.x or ArubaOS 5.0.x versions earlier than ArubaOS 5.0.3.1, download the latest version of ArubaOS 5.0.4.x.
- For ArubaOS 6.0.0.x, download the latest version of ArubaOS 6.0.2.x.

Follow [step 2–step 11](#) of the procedure described in [Upgrading From a Recent version of ArubaOS on page 75](#) to install the interim version of ArubaOS, then repeat [step 1–step 11](#) of the procedure to download and install ArubaOS 6.2.1.2.

Upgrading From a Recent version of ArubaOS

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

- ArubaOS 6.2.0.x
- ArubaOS 6.1.x
- ArubaOS 6.0.1.x

- ArubaOS 6.0.2.x
- ArubaOS 5.0.3.1 or later 5.0.x releases (If you are running ArubaOS 5.0.3.1 or a later 5.0.x release, review [Upgrading With RAP-5 and RAP-5WN APs on page 76](#) before proceeding further.)
- ArubaOS 3.4.4.1 or later 3.4.x releases.

Install the ArubaOS 6.2.1.2 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 6.2.1.2 from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Log in to the ArubaOS WebUI from the PC or workstation.
4. Navigate to the **Maintenance > Controller > Image Management** page. Select the **Upload Local File** option, then click **Browse** to navigate to the saved image file on your PC or workstation.
5. Select the downloaded image file.
6. In the **partition to upgrade** field, select the non-boot partition.
7. In the **Reboot Controller After Upgrade** option field, best practices is to select **Yes** to automatically reboot after upgrading. If you do not want the controller to reboot immediately, select **No**. Note however, that the upgrade will not take effect until you reboot the controller.
8. In **Save Current Configuration Before Reboot** field, select **Yes**.
9. Click **Upgrade**.
10. When the software image is uploaded to the controller, a popup window displays the message **Changes were written to flash successfully**. Click **OK**. If you chose to automatically reboot the controller in step 7, the reboot process starts automatically within a few seconds (unless you cancel it).
11. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > Controller > Controller Summary** page to verify the upgrade.

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

1. Log in into the WebUI to verify all your controllers are up after the reboot.
2. Navigate to **Monitoring > Network Summary** to determine if your APs are up and ready to accept clients.
3. Verify that the number of access points and clients are what you would expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a back up of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See [Backing up Critical Data on page 73](#) 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 76](#). 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 6.2.1.2 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 73](#)

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.

- 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 6.0.0.x, download the latest version of ArubaOS 6.0.2.x.

Follow [step 2 –step 7](#) of the procedure described in [Upgrading From a Recent version of ArubaOS on page 77](#) to install the interim version of ArubaOS.

Upgrading From a Recent version of ArubaOS

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

- ArubaOS 6.2.0.x
- ArubaOS 6.1.x
- ArubaOS 6.0.1.x
- ArubaOS 6.0.2.x
- ArubaOS 5.0.3.1 or later 5.0.x releases (If you are running ArubaOS 5.0.3.1 or a later 5.0.x release, review [Upgrading With RAP-5 and RAP-5WN APs on page 76](#) before proceeding further.)
- ArubaOS 3.4.4.1 or later 3.4.x releases.

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

1. Download ArubaOS 6.2.1.2 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 SCP/FTP/TFTP server:

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

or

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

or

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

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/hal)
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/hal) **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>
```

or

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

or

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

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

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

```
-----
```

```
Partition           : 0:1 (/dev/hal) **Default boot**
Software Version     : ArubaOS 6.2.1.2 (Digitally Signed - Production Build)
Build number         : 38432
Label                : 38432
Built on             : Fri May 24 00:03:14 PDT 2013
```

```
-----
```

```
Partition           : 0:1 (/dev/hal)
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 73](#) 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 6.2.1.2 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 6.2.1.2 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 73](#).
2. Verify that control plane security is disabled.
3. Set the controller to boot with the previously-saved pre-6.2 configuration file.
4. Set the controller to boot from the system partition that contains the previously running ArubaOS image.

When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next controller reload. An error message displays if system boot parameters are set for incompatible image and configuration files.
5. After downgrading the software on the controller:
 - Restore pre-6.2 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.2.1.2 flash backup file.

- You do not need to re-import the WMS database or RF Plan data. However, if you have added changes to RF Plan in ArubaOS 6.2.1.2, the changes do not appear in RF Plan in the downgraded ArubaOS version.
- If you installed any certificates while running ArubaOS 6.2.1.2, 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 6.2.1.2 image:

```
#show image version
```

```

-----
Partition           : 0:1 (/dev/hal)
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 6.2.1.2 (Digitally Signed - Production Build)
Build number         : 38432
Label                : 38432
Built on             : Fri May 24 19 00:03:14 PDT 2013

```

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

```
# boot system partition 0
```

5. Reboot the controller:

```
# reload
```

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

```
# show image version
```

Before You Call Technical Support

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

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

This chapter discusses the steps required to migrate your existing controllers to 7200 Series controllers.



For information about migrating to the 7200 Series Controller, visit support.arubanetworks.com.

Migrating to the 7200 Series Controller

You must complete the following tasks to complete the migration process:

- Back up the controller data from your existing controller.
- Upgrade your network to ArubaOS 6.2. This ensures that the image on your new controllers matches the image of the rest of the controllers in your network.
- Back up the controller data from your upgraded, existing controller.
- Transfer existing licenses to your new controller.
- Install your new controller.
- Install the backed up data on your new controller.
- Apply transferred and new licenses.
- Reload your controller.
- Update port-related configuration.
- Confirm that your new controller operates as expected.

Important Points to Remember

- The 7200 Series controllers use a different port number scheme than other controllers. Ports on the 7200 Series are numbered **slot/module/port**. Other controller ports are numbered **slot/port**.
- Not all Aruba controller models support ArubaOS 6.2. The following controllers support ArubaOS 6.2:
 - 7200 Series
 - M3
 - 3200XM , 3400, and 3600
 - 600 Series



Beginning in ArubaOS 6.2, the 651 controller's internal AP is disabled. Additionally, upon upgrade, the 651 will appear as a 650-1 and the 651-8 will appear as a 650-9 in ArubaOS.

- You can complete this migration process on a controller-by-controller basis if your replaced controllers support ArubaOS 6.2. The entire deployment does not need to be completed at the same time.
- When replacing a master controller, replace the backup master first.
- If you are migrating to a 7200 Series controller from a controller not listed above, please contact Aruba support.

Backing Up Your Data Before Upgrading to 6.2

Back up your controller data before upgrading to ArubaOS 6.2. To back up your controller data, complete the steps in the following sections:

Back Up the Flash File System in the WebUI

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 flashback.tar.gz file.
5. Click **Copy Backup** to copy the file to an external server.
6. 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.

Back Up the Flash File System in the CLI

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 flashback.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 flashback.tar.gz created successfully on flash.
```
3. Use the **copy** command to transfer the backup flash file to an external server:

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

Upgrading Your Network



CAUTION

Before attempting upgrade any of your controllers, it is recommended that you read the [Upgrade Procedures on page 71](#).



NOTE

If you are migrating from controllers that do not support ArubaOS 6.2, it is recommended that you upgrade to the latest supported build of your current version of ArubaOS before beginning the migration process.

[Table 116](#) provides a brief overview of the steps required to upgrade to ArubaOS 6.2. For more detailed information and procedures on upgrading, see [Upgrade Procedures on page 71](#).

Table 116 ArubaOS 6.2 Upgrade Path Overview

Version	Step 1	Step 2
3.x, earlier than 3.4.4.1	Upgrade to the latest 3.4.5x	Upgrade to 6.2
RN-3.x	Upgrade to the latest 5.0.4.x	Upgrade to 6.2
5.x, earlier than 5.0.3.1	Upgrade to the latest 5.0.4.x	Upgrade to 6.2

Table 116 ArubaOS 6.2 Upgrade Path Overview (Continued)

Version	Step 1	Step 2
6.0.0.x	Upgrade to the latest 6.0.2.x	Upgrade to 6.2
6.2.0.x 6.1.x 6.0.1.x 6.0.2.x 5.0.3.1 (or later 5.0.3.x) 5.0.4.x 3.4.4.1 (or later 3.4.x) 3.4.5.x	Upgrade to 6.2	—

Backing Up Your Data After Upgrading to 6.2

After completing the upgrade to ArubaOS 6.2, back up your controller data and configuration once more before continuing. It is recommended that you rename your backup file and transfer to an external storage device.

Transferring Licenses

To transfer existing licenses from one controller to another:

1. Open a browser, navigate to <https://licensing.arubanetworks.com/>, and login.
2. Navigate to **Certificate Management > Transfer certificate** and select the licenses you want to transfer.
3. All the certificates active on the controller of the license certificate you have selected will be displayed. Select all the certificates you would like to transfer.
4. Enter the serial number of the new controller and click **Transfer**. When the transfer has been completed successfully, you will receive a new set of activation keys.



The selected certificates must be compatible with your new controller. If not, you will not be able to complete the transfer. You will receive the following error message: **This certificate is not compatible with your system!**



If the destination controller does not exist, you will receive the following error message: **This system does not exist**. If you receive this error, ensure that you entered the serial number correctly. Once you have verified that the serial number you entered was correct, contact Aruba Technical Support.

Installing Your New Controller

For instructions and additional information about installing your 7200 Series controller, please refer to the *Aruba 7200 Series Controller Installation Guide* and *ArubaOS 6.2 Quick Start Guide* included with your device. For the latest version of this document, visit support.arubanetworks.com and click the **Documentation** tab.



After installing your 7200 Series, verify that it is running the latest version of ArubaOS 6.2. If not, it is recommended that you upgrade your controller. See [Upgrade Procedures on page 71](#).

Installing Backed Up Controller Data



The 7200 Series controllers use a different port numbering scheme than other controllers. Ports on the 7200 Series are numbered **slot/port/module**. Other controller ports are numbered **slot/port**. Once you've loaded your old configuration onto a 7200 Series controller, you will no longer be able to connect to the controller over the network. Additionally, all ports will become untrusted. You must connect to your new controller using a serial connection to reconfigure port settings.

To install your existing configuration and controller data onto your new controller, complete the following steps.

Restore the Flash File System in the WebUI

1. Navigate to the **Maintenance > File > Copy Files** page.
 - a. For **Source Selection**, specify the server to which the flashbackup.tar.gz file was previously copied.
 - b. For **Destination Selection**, select **Flash File System**.
 - c. Click **Apply**.
2. Navigate to the **Maintenance > File > Restore Flash** page.
3. Click **Restore** to restore the flashbackup.tar.gz file to the flash file system.



Do not reboot your controller before installing licenses.

Restore the Flash File System in the CLI

1. Enter **enable** mode in the CLI on the controller.
2. Transfer the flashbackup.tar.gz file from its external location to the controller's flash using the commands that follow according to your preferred method.

```
copy ftp: <ftphost> <srcfilename> flash: flashbackup.tar.gz
copy tftp: <tftphost> <srcfilename> flash: flashbackup.tar.gz
copy scp: <scphost> <username> <srcfilename> flash: flashbackup.tar.gz
copy usb: partition <partition-number> <srcfilename> flash: flashbackup.tar.gz

restore flash
```



Do not reboot your controller before installing licenses.



Do not modify your configuration before reloading the controller.

Applying Licenses

After you have installed your new controller and brought it up, you can apply and back up any new or transferred licenses.

Applying the Software License Key in the WebUI

1. Log in to your controller's WebUI.
2. Navigate to the **Configuration > Network > Controller** select the **License** tab.

3. Copy the software license key, from your email, and paste it into the **Add New License Key** field. Click **Add**.
4. Reboot your controller to enable the new license feature.

Applying the Software License Key in the License Wizard

1. Log in to your controller's WebUI.
2. Launch the License Wizard from the **Configuration** tab and click the **New** button.
3. The License Wizard will step you through the activation process. Click on the Help tab within the License Wizard for additional assistance.
4. Reboot your controller to enable the new license feature.

Backing Up Licenses in the WebUI

1. Log in to your controller's WebUI.
2. Navigate to the **Configuration > Network > Controller** and select the **License** tab.
3. Scroll to the bottom of the page and click **Export Database**.
4. Enter the file name of the file to export and click **OK**.
5. Copy the backup file from the external server or USB storage device to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.

Backing Up Licenses in the CLI

1. Use the license export <filename> command to create a license backup.

```
(host) #license export licensebackup.db
```

```
Successfully exported 1 licenses from the License Database to licensebackup.db
```

2. Use the **copy** command to transfer the backup flash file to an external server or USB drive:

```
(host) copy flash: licensebackup.db ftp: <ftphost> <ftpusername> <ftpuserpassword>  
<remote directory>
```

```
(host) #copy flash: licensebackup.db usb: partition <partition-number> licensebackup.db
```

Reload Your Controller

After restoring flash and transferring licenses, you must reboot your controller before continuing.

Establishing Network Connectivity

Due to the difference in port numbering schemes between the 7200 Series and older controller platforms, your 7200 Series controller will not have network connectivity and all ports will become untrusted after installing your previous controller's configuration in data. All previous controller models used a **slot/port** number scheme; the 7200 Series uses **slot/module/port**. To establish network connectivity, you must manually reconfigure your controller interfaces.



Slot and module will always be 0 and 0 on the 7200 Series controller.



The first two ports on the 7200 Series, 0/0/0 and 0/0/1 are combination ports and can be used for management, HA, and data traffic. Ports 0/0/2 through 0/0/5 can only be used for data traffic. Keep this in mind when reconfiguring your ports.

Connecting to the Controller

Since your 7200 Series controller does not have network connectivity, you must directly connect to it using a serial port connection. Once connected, you will receive a login prompt. Login using your configured credentials.

The following commands are affected by this new port numbering scheme and must be considered when reconfiguring your ports:



After restoring the flash and rebooting, all inherited port configuration will be lost. This can include, but is not limited to, trusted settings, port channel, port monitoring, and so on.

```
interface gigabitethernet <slot/port/module>
    trusted

interface range gigabitethernet <slot/port/module>

interface port-channel gigabitethernet
    add <slot/port/module>
    delete <slot/port/module>

interface gigabitethernet port monitor <slot/port/module>

interface vlan <vlan-id>
    ip igmp proxy gigabitethernet <slot/port/module>
```

Verifying Controller Operation

Once you have completed the tasks described above, verify that your controller and the expected APs come up and are active.

Verifying Migration in the WebUI

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 expect.
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.

Verifying Migration in the CLI

1. Log in into the CLI to verify all your controllers are up after the reboot.
2. Use 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. Backup all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See [Backing Up Your Data Before Upgrading to 6.2 on page 84](#).