ArubaOS 6.1.2.8

Release Notes

Open Source Code

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

http://www.arubanetworks.com/open_source

Legal Notice

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

Warranty

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

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

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

ArubaOS 6.1.2.8 is a patch software release that introduces fixes to many previously outstanding issues. For details on all of the features described in the following sections, see the *ArubaOS 6.1 User Guide*, *ArubaOS 6.1 CLI Reference Guide*, and *ArubaOS 6.1 MIB Reference Guide*.

NOTE

See the "Upgrade Procedures" on page 47 for instructions on how to upgrade your controller to this release.

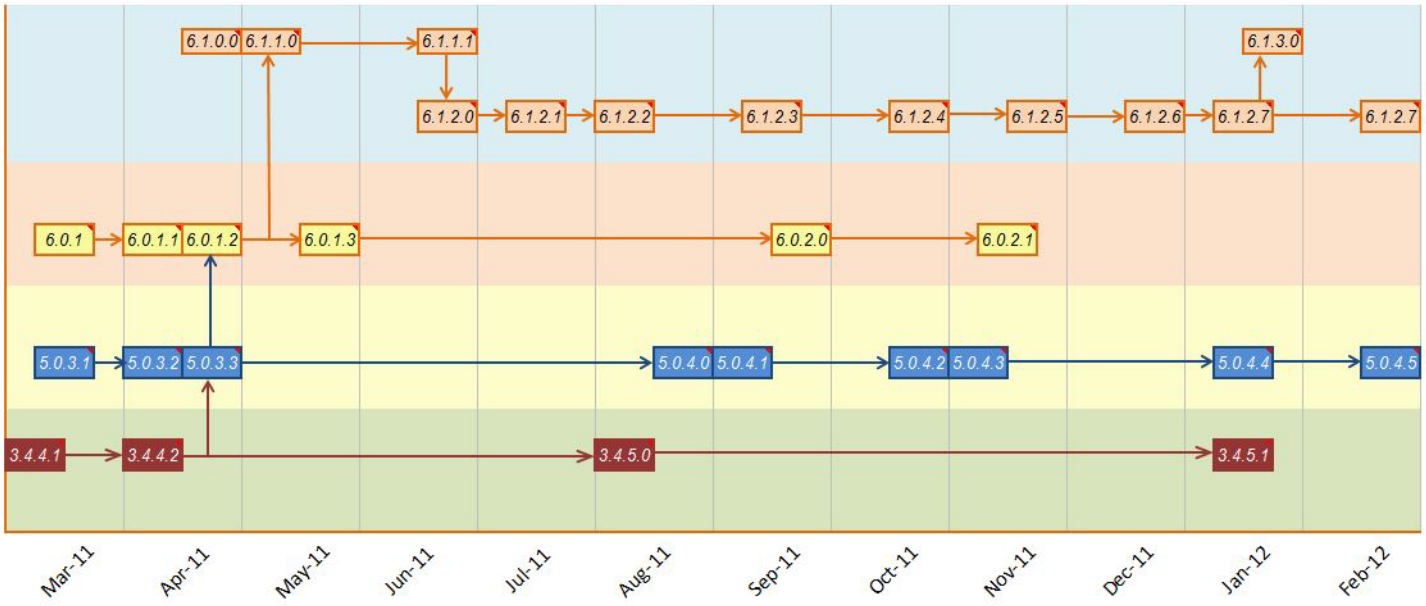
Release Note Overview

- Chapter 2, "What's New in this Release" on page 11 describes the new features and bug fixes introduced in this release, as well as new known issue that have been identified since the previous release.
- Chapter 3, "Features Added In Previous 6.1.x Releases" on page 15 provides information on features added in previous releases of ArubaOS 6.1.x.
- Chapter 4, "Fixed In Previous 6.1.x Releases" on page 17 describes the issues that have been fixed in this release.
- Chapter 5, "Known Issues Identified in Previous 6.1.x Releases" on page 35 provides descriptions and workarounds for outstanding issues in ArubaOS 6.1.
- Chapter 6, "Upgrade Procedures" on page 47 cover the procedures for upgrading your controller from any release of ArubaOS to ArubaOS 6.1.

Release Mapping

The following illustration shows which patches and maintenance releases are included in their entirety in ArubaOS 6.1.2.8.

Figure 1 *ArubaOS Releases and Code Stream Integration*



Supported Browsers

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

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

Contacting Support

Table 1 *Web Sites and Emails*

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

Table 2 *Contact Phone Numbers*

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

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

Bugs Fixed in this Release

The following issues have been fixed in ArubaOS 6.1.2.8. For a list of issues fixed in previous versions of ArubaOS 6.1.2.x, see "Fixed In Previous 6.1.2.x Releases" on page 27.

Access Points

Table 1 *Access Point Fixed Issues*

Bug ID	Description
57133, 64808, 63032	An issue in which a VAP's is unable to transmit and all its buffer become stuck in the software queue, resulting in ping anc onnectivity loss, has been fixed.
54256 54609 57659 50521 59720 59752 60176 56540 61629 63127 63120 63127 63120 63249 63240 63353	The AP no longer crashes with a datapath error.

Interface

Table 2 *Interface Fixed Issues*

Bug ID	Description
60991 62290 62909 63675 64309	On the 3400, there is no link flapping while using SFP-SX.

LDAP

Table 3 *LDAP Fixed Issues*

Bug ID	Description
64260	When the LDAP connection is idled out, error logs are no longer created with an stw_timer_destroy error.

Master Local

Table 4 *Master Local Fixed Issues*

Bug ID	Description
61908	The overloaded CFGM module no longer causes a write memory failure. The running dbbk periodic backup daemon now performs the database backup operation in the background after doing write-mem.

Platform/Datapath

Table 5 *Platform/Datapath Fixed Issues*

Bug ID	Description
62526	When there is configuration corruption during a download, the cfgm module no longer aborts; instead, it resets the master/local connection and re-downloads the configuration.
53804 53004	The FPCLI does not crash on an AP name over 64 characters long while executing the `show ap debug` command.
54588 62320	Bandwidth contracts of 1M and 2M for 10 users each can now pass the test.
62493 62390	BCMC-optimization with rap wifi and wired-ports in tunnel mode breaks connectivity. The fix changes the ingress to indicate that ARP rsp is sent from the controller so it is not dropped in the egress direction.
54191 55794	The datapath timeout exception no longer occurs due to a race condition. The race condition was triggered by FTP data transfers and the reuse of a stray session.
6333	The M3 is no longer experiencing poor performance and packet loss from punting the frame to the SP for IPv6 open system traffic that is tunneled through an AP IPv4 tunnel.
52492	The M3 controller crashes with “reboot cause: unknown.” The unknown reboots indicate that the reboot cause is not written because of a failure when writing to flash. The fix works by retrying flash writes so that the reboot cause is written to flash.
61667	The `firewall broadcast-filter arp` command no longer causes the local controller to use the incorrect route-cache entry.

Radius

Table 6 *Radius Fixed Issues*

Bug ID	Description
58094 62754	The controller no longer retransmits accounting packets even though it has received an Accounting-Response for the first packet.

RAP+BOAP

Table 7 *RAP+BOAP Fixed Issues*

Bug ID	Description
61000 63412	RAPs running 6.0.x and 5.X no longer fail to upgrade to 6.1.2.X, due to a message version mismatch between the AP and the controller.

Role/VLAN Derivation

Table 8 *Role/VLAN Derivation Fixed Issues*

Bug ID	Description
60707 61409	I-phones intermittently performing dot1x are no longer being reset to their initial-role. And the I-pad user-role is no longer reset to logon when it wakes up from sleep mode.

Security

Table 9 *Security Fixed Issues*

Bug ID	Description
63287 63207	The auth module no longer passes a stale pointer to the monitoring routine and causes it to crash.
61551 62289 61597 60310	The auth module no longer crashes on the controller.
59661 59130	The auth module no longer crashes, causing clients to get disconnected.
61461	The bandwidth contract no longer changes when the user moves from the Initial role to the final role (both roles have a different bwm-contract configured).
58098 63601 50090	The auth module no longer crashes on one of the controllers.

Station Management

Table 10 *Station Management Fixed Issues*

Bug ID	Description
60657 59574 59374 63265 60605 60657	In this multi-threaded application, the memory manager (MM) now allocates enough buffer to read all the blocks of memory.

New Known Issues

The following issues have been identified since the last release. For a list of known issues found in previous versions of ArubaOS 6.1.2.x, see "Known Issues Identified in Previous 6.1.x Releases" on page 45.

Access Points

Table 11 *Access Point Known Issues and Limitations*

Bug ID	Description
59027	Bridge user entries may not be aged out if the user has roamed to a RAP on a different management VLAN. **Workaround:** Execute the command `aaa user delete` to clear the user entry.
56707	In some cases, APs which are up and active on a local controller may show as down on the master controller. **Workaround:** None.
56678	In some cases, the client good put values may show half of the expected value. **Workaround:** None.
57802	In some cases, ESI-installed blacklist entries are incorrectly installed as "Permanent" instead of being governed by the VAP's Blacklist Timeout value. **Workaround:** None.
58380	An AP-125 may crash after repeated VAP enable/disable. **Workaround:** None.
59706	In some cases, an AP may crash unexpectedly due to an interrupt during deferred set channel. **Workaround:** None.
60458	A LAN extension created by using the ENET port of a mesh point to a locally bridge via a Remote mesh point may fail. In this case, incoming user via the mesh point does not pickup a valid user ACL and all traffic (except ARP) is blocked by the firewall on the Remote Mesh Portal. **Workaround:** None.

Table 11 *Access Point Known Issues and Limitations (Continued)*

Bug ID	Description
62267	Some AP-125s may exhibit heartbeat counting and reporting errors. This can be seen in the output of `show ap debug system status`. **Workaround:** None.
62672, 63154, 61669, 62296	An Aruba 651 controller is susceptible to continuous rebooting if its internal AP (radio) is configured in Air Monitor mode (am-mode). **Workaround:** Reconfigure the internal AP (radio) in Access Point mode (ap-mode). Alternatively, you may disable the radio if not needed.
62767, 63423	In some cases, groups of APs may rebootstrap randomly in when terminating on fully loaded or close to fully loaded controllers. **Workaround:** None.
64562	In some cases, an AP-130 Series AP may crash while experiencing heavy traffic in parallel with a voice call. **Workaround:** None
64632	In some cases, an AP-65 may unexpectedly crash and reboot due to a memory corruption. **Workaround:** None.

Arm

Table 12 *ARM Issues and Limitations*

Bug ID	Description
53389	Starting a packet capture on an AP triggers an ARM channel change with reason "INV". Also the packet capture does not work **Workaround:** None.

Captive Portal

Table 13 *Captive Portal Issues and Limitations*

Bug ID	Description
45571	Captive portal is not working on the local controllers when the guest VLAN has NAT enabled. **Workaround:** If you do not have loopback IP Addresses on your controllers, let local try establish connection with master on its VLAN IP address instead of its VRRP IP address.
58729	The command ipv6 cp-redirect-address diable does not work. **Workaround:** None.

Certificate Manager

Table 14 *Certificate Manager Known Issues and Limitations*

Bug ID	Description
63008	In some cases, after replacing an expired 802.1x certificate, clients may not be able to authenticate. **Workaround:** Restart the auth process on the controller.
63134	In some cases, a webserver may not be able to revert to the factory certificate once the custom certificate expires and is deleted. **Workaround:** None.

Configuration

Table 15 *Configuration Issues and Limitations*

Bug ID	Description
51159	In some cases, your M3 may become stuck in a bootloop due to a configuration corruption. **Workaround:** The controller must be recovered from CPboot.
48961	The speed/duplex configuration is removed when the port status changes to “down.” **Workaround:** None

802.1x

Table 16 *802.1x Known Issues and Limitations*

Bug ID	Description
54238	Clients may be put into an incorrect role after successful machine auth and user auth. **Workaround:** Configure External RADIUS server not to return attribute “Class” RADIUS attribute of value “computer” in the remote-access policy, which is responsible for machine-authentication.
43431	Client blacklisting is not working if max-authentication-failures is set to 2 or larger value. **Workaround:** Set max-authentication-failures is set to 1.
56236	A replay counter mismatch might be observed during the 4-way handshake in WPA2-AES mode with a Cisco 7921 and 7925 handsets. This usually happens after the clients come back up from power save mode. **Workaround:** None; however, this mismatch will not be seen on the next attempt.
63392	The controller might consider that authentication is “out-of-service” when an iPhone or Blackberry attempts to connect using 802.1x (PEAP+MSChap2) with the wrong password. **Workaround:** None. This is a display issue.

Table 16 *802.1x Known Issues and Limitations (Continued)*

Bug ID	Description
64096	Occasionally, a WPA mismatch error might be seen, preventing clients from associating. **Workaround:** Try to force the client to connect two to three times.
61935	A DHCP fingerprinting UDR with an action of set-vlan does not work in a an 802.1x network. **Workaround:** None.

ESI

Table 17 *ESI Issues and Limitations*

Bug ID	Description
53189	A client's user role may not change after the syslog displays and show ESI parser show that there was a user role event. **Workaround:** None.

IPSec

Table 18 *IPSec Known Issues and Limitations*

Bug ID	Description
64451	You may not be able to save a configuration on a master controller with a VRRP topology. **Workaround:** Remove the VRRP configuration and complete a `write mem` to save the configuration. After that, add VRRP configuration back and save configuration.

IPv6

Table 19 *IPv6 Issues and Limitations*

Bug ID	Description
52190	In rare cases, IPv6 link-local address does not get added to the route cache. **Workaround:** None.
56978, 63919	In some cases, local user entries are missing in the datapath for IPv6. **Workaround:** Apply firewall Captive Portal bandwidth contract to avoid burst traffic.
57059	Basic routing fails when the maximum number of IPv6 L3 interfaces are configured. **Workaround:** Do not use the maximum number of IPv6 L3 interfaces.
50648	The command `show datapath session ipv6 count` shows a maximum IPv6 session count of 524287. **Workaround:** None.

LDAP

Table 20 *LDAP Issues and Limitations*

Bug ID	Description
53218	In some cases, your controller may reboot unexpectedly due to auth crash that occurs during an LDAP auth timeout. **Workaround:** None.

Local Database

Table 21 *Local Database Issues and Limitations*

Bug ID	Description
53391	The `local-userdb-ap add` command adds an invalid entry if the remote-ip first octet is greater than 127. **Workaround:** None.

Management

Table 22 *Management Issues and Limitations*

Bug ID	Description
49504	Using the `show inventory` command on M3 on slot #1 fails to give the serial number and other data. This issue occurs when this module is booted up along with a module in slot #0. This does not occur if the module as booted separately. **Workaround:** None.
54334	The wlanAPBssidAPMacAddress OID may become corrupted after upgrading. **Workaround:** None.
61423	An old user entry in the user table is not removed even after the client is disassociated to a different network. When a new user connects to the SSID, it is getting the IP address as the old user entry in the user table, which was there for couple of days. Because of the old entry, the new client is unable to pass any traffic that also gets the same IP. **Workaround:** None.
62852, 64110	In some cases, your controller may restart unexpectedly due to wms module crash. **Workaround:** None.
63800	Some valid APs be incorrectly and randomly classified as unknown. **Workaround:** Re-classify those AP as valid.
56666	In some cases, the station table might show a large number of stale entries. **Workaround:** Use the command `aaa user delete` to clear the user entries.

Table 22 *Management Issues and Limitations (Continued)*

Bug ID	Description
62988	Wireless clients might incorrectly assigned to the wrong VLAN when VLAN mobility is enabled. **Workaround:** Set firewall bandwidth contract to default.

Mesh

Table 23 *Mesh Issues and Limitations*

Bug ID	Description
55740	Mesh points may crash in node_cleanup() when controller is downgraded. **Workaround:** None.
56642	An AP-135 configured as a mesh point will fail to upgrade if the mesh link to the AP-120 Series mesh portal is using HT mode. **Workaround:** Do no enable HT on an AP-120 Series mesh portal and change the default supported-MCS from 0-23 to 0-15.

Mobility

Table 24 *Mobility Issues and Limitations*

Bug ID	Description
63163	When mobility is enabled, datapath bridge entries are being deleted for untrusted users. This happens with a L3 mobility and wired 802.1x user combination. **Workaround:** None with this configuration.
63134	The mobileip module can crash when “no router mobile” is used with a combination of “router mobile” and heavy traffic. **Workaround:** None.

OSPF

Table 25 *OSPF Issues and Limitations*

Bug ID	Description
62839	In some cases, the OSPF process may crash on an M3 with a DHCP helper address on the same OSPF configured VLAN. **Workaround:** None. This is not service impacting.

Platform/Datapath

Table 26 *Platform/Datapath Issues and Limitations*

Bug ID	Description
54943	Users may not be able to get an IP address on VMWare Fusion when broadcast-filter ARP is enabled. **Workaround:** Diable broadcast-filter ARP.
58502	Packets sent from a trunk port on a controller to a client on a trunk port behind a RAP may not have the correct VLAN tag. **Workaround:** None.
59078	Tagged VLAN traffic received through a trunk port is sent out the egress port without a PPPoE header. **Workaround:** None.
60670	In some cases, a 620 controller may reboot unexpectedly due to a datapath exception when connected to a Bell ADSL modem. **Workaround:** None.
60431	In some cases, the fpapps module may crash on your controller from show trunk when a large number of non-contiguous VLANs are present. **Workaround:** Do not use non-contiguous VLANs in a trunk configuration.
64413	On a 650 controller, the link flap counter `DOWN` under the command `show port link-event` might not update after the port is shutdown. **Workaround:** None.
64569, 64578	In some cases, your controller may reboot unexpectedly due to a datapath exception that occurs when the controller hits an ASSERT caused by a buffer depletion. **Workaround:** None.
64637, 64638	Your controller may become frozen and unresponsive with no SSH or console access. **Workaround:** Reboot your controller.
64197	In some cases, your controller may reboot unexpectedly due to a datapath module crash caused by an ASSERT. **Workaround:** None.
64565	In some cases, your M3 controller may reboot unexpectedly due to a kernel panic. **Workaround:** None.
54194	In some cases, your controller may reboot unexpectedly due to a fpapps module crash. **Workaround:** None.

Table 26 *Platform/Datapath Issues and Limitations (Continued)*

Bug ID	Description
64392	In some cases, your controller may reboot unexpectedly due to a kernel panic. **Workaround:** None.
64635	In some cases, your controller may reboot unexpectedly due to a kernel panic. **Workaround:** None.
46116	A controller may fragment TKIP-VAP traffic causing 50-100 k/s throughput for mesh points. This is caused because TCP MSS for TKIP tunnels is unable to accommodate the WEPCRC length. **Workaround:** None.
63140	Your controller may experience a datapath timeout if 2,000 users are created from an untrusted port with upstream and downstream per-user bandwidth contracts. The timeout occurred when `aaa user delete` was executed to change bandwidth contract and change of user role. **Workaround:** None.
62838	If an AP comes up on an untrusted port where the first port rule is allow all, that AP's sessions may be denied. **Workaround:** None.
61493	In some cases, your controller may reboot due to a datapath timeout caused by an ASSERT caused by incorrect EAP handling. **Workaround:** None.
62527	In some cases, your controller may reboot unexpectedly due to a crash on the arc-cli-helper. This crash was caused by the execution of the phonehome now from the WebUI. WebUI phonehome crash. **Workaround:** None.
60792, 63291	In some cases, your controller may reboot unexpectedly due to a datapath exception that is triggered by an IGMP mcast membership delete message from the control plane. **Workaround:** None.
62818	A user may not be aged out if there is traffic being sent towards that client IP address. **Workaround:** The user entry will age out once the client is idle for the amount of time configured in aaa idle timer.
64199	In some cases, your controller may reboot unexpectedly due to a datapath module crash. **Workaround:** None.
58395	After a reboot, the controller will display the reason for the reboot as "user pushed reset" if the intent or cause of the reboot is could not be written to the flash. **Workaround:** None.
62851	In some cases, the FPAPPS module can restart unexpectedly due to a memory allocation issue. **Workaround:** None.

Table 26 *Platform/Datapath Issues and Limitations (Continued)*

Bug ID	Description
63751, 63874	In some cases, the configuration from a master controller may not be successfully pushed to the local controllers. This may due to CFGM becoming to busy with heartbeats from the local controllers to handle a `write mem`. **Workaround:** None.

Port Channel

Table 27 *PPPoE Issues and Limitations*

Bug ID	Description
63840, 62936	When the native VLAN of a trunk LACP port channel is set as untrusted, ports may go down. **Workaround:** None.

PPPoE

Table 28 *PPPoE Issues and Limitations*

Bug ID	Description
58097	A local 620 controller connected through a DSL modem using PPPoE may not be able to reach the master controller. **Workaround:** Reload the local controller to populate route cache entries again.
64254	In some cases, an 620 controller might not send LCP echo responses resulting in an interruption of PPPoE connections. **Workaround:** None.
63840	A controller might drop large (greater than 1000 bytes) frames if its uplink is PPPoE. **Workaround:** Offload PPPoE from the controller to an external device.

PPTP

Table 29 *PPTP Issues and Limitations*

Bug ID	Description
63052	PPTP client may fall into logon role if `aaa user fast-age` is enabled. **Workaround:** None.
55177	A MAC PPTP client connecting to an M3 as a PPTP server is disconnected after 10 minutes if idle. **Workaround:** None.

RADIUS

Table 30 *Radius Issues and Limitations*

Bug ID	Description
57005	In some cases, your controller may report incorrect values in the RADIUS Accounting Stop packet for Acct-Input-Octets/Acct-Output-Octets. **Workaround:** None.

RAP

Table 31 *RAP Issues and Limitations*

Bug ID	Description
59036	Clients connected to backup RAP cannot send any traffic if no PEF-NG is installed. **Workaround:** In this case, install the PEF-NG license.
59723	A client may be unable to connect to split-tunnel RAP after disable/enable of wireless adapter. **Workaround:** Clear user entry using `aaa user delete` command and try re-connect.
60167	Certificate based PPPoE RAPS may rebootstrap at regular intervals with keepalive timeout. **Workaround:** None.
53408	If VLAN ID is not set in virtual-ap profile, the VAP does not survive when connectivity to the controller is lost and the AP is rebooted. **Workaround:** None.
44973	In rare cases, the group key is absent on bridge/split VAP or mismatch with the controller auth. **Workaround:** None.
57057	Occasionally, the group key might change even when there is no reboot or rebootstrap involved when the RAP VAP is 802.1x split, bridge, or d-tunnel mode. **Workaround:** None.
63073	In some cases, RAP backup VAP save to flash may fail. This occurs with large ACLs with 500 ACE entries. **Workaround:** Reduce the number of ACE entries.
62556	In rare cases, a RAP may not move to TFTP after FTP is denied or fails. **Workaround:** Add the rule `user alias controller svc-ftp permit` in the ap-acl.

Role/VLAN Derivation

Table 32 *Role/VLAN Derivation Issues and Limitations*

Bug ID	Description
55438	In some cases, the order of the dhcp-option rules is not being honored (first rule to be processed first). **Workaround:** None.
62447	Users are falling into the initial role of the default aaa profile rather than the aaa profile configured role as the L2 station does not exist. **Workaround:** None.
55867	Clients doing machine-auth will fall into the default VLAN if an external server is used for VLAN derivation. **Workaround:** None.
51691	Client role derivation does not happen correctly when the client performs DHCP-renew after UDR and CP-auth. **Workaround:** DHCP fingerprint and captive portal cannot be used together.
63348	Logon role getting assigned to wired clients bypassing the role mentioned in the aaa profile for the VLAN. **Workaround:** None.
63645	Users connecting to RAP5WN shows in the user table with logon role and there are no AP name in the user table. **Workaround:** None.
64393	In some cases, MAC clients and Cisco phones are intermittently placed in the wrong VLAN. **Workaround:** None.

Security

Table 33 *Security Issues and Limitations*

Bug ID	Description
65047	With Mobile-IP enabled, ACE entries may reach their maximum, preventing new ACLs from being added. **Workaround:** Disable mobile-IP.
55202	MAC authentication may not happen once the user is present in the user table and the client attempts to associate again. **Workaround:** Use `aaa user delete` command to delete user entry from controller.

Table 33 *Security Issues and Limitations (Continued)*

Bug ID	Description
55519	In some cases, the auth module may crash on the controller when the auth manager is 100% busy. Since the auth manager is busy, the console and WebUI access becomes unavailable. **Workaround:** None.
56130	User may incorrectly be placed in the logon role instead of the MAC-auth role when roaming. **Workaround:** None.
51393	MIPT phones may reboot continuously with any any udp 68 deny rule in validuser ACL. **Workaround:** Do not use `any any udp 68 deny` rule at first position in "validuser acl."
62099	In some cases, user entries may become stuck in the user table. **Workaround:** Use the `aaa user delete` command to clear the expired entries.
61964	The command `show acl ace-table acl <acl>` does not return any output for ACLs with around 500 ACE entries. **Workaround:** Best practices is to use around 200 ACE entries per ACL.
47868	The `name` option under the `netdestination6 Ipv6 alias` option is not available. **Workaround:** None.
62145	The `show license-usage user` command shows no user count when the controller has many VPN users. **Workaround:** None.
62253	A controller may miss sending user account interim updates to the RADIUS server if it has a sudden burst of heavy users. **Workaround:** None; however, this issue does not impact service.
64598, 63914, 64597	In rare cases, the auth module may crash, causing the controller to reboot unexpectedly, due to a memory allocation issue. **Workaround:** None.

61690	In an ACL with the following lines:
	`ip access-list session good`
	`any any any deny blacklist log`
	The ACL has the enabled the blacklist option and the valid client is falling on the MAC auth default role. The non-valid client is falling on the Deny all, but the non-valid clients are not getting blacklisted.
	Workaround:
	None.

56424	Under heavy traffic conditions, site to site IPSec tunnels may go down and show DPD messages. **Workaround:** None.

Table 33 *Security Issues and Limitations (Continued)*

Bug ID	Description
55913	After issuing the `aaa user delete all` command, user is intermittently set to the logon role. **Workaround:** None.
55936	In some cases, Cisco 7921 and 7925 phones do not respond to key1 when using PSK. **Workaround:** Reboot the Cisco phone.
59579	Rogue clients with spoofed MAC or IP addresses are correctly being denied access to the network; however, legitimate clients are also being denied. **Workaround:** None
64322, 63348, 62447	Occasionally, users coming through a L2 GRE tunnel are incorrectly placed into the logon role instead of the role defined per the VLAN wired AAA profile. **Workaround:** Use the command `aaa user delete` and recreate the user entry.

TACACS

Table 34 *TACACS Issues and Limitations*

Bug ID	Description
60667	A TACACS accounting server might block auth when there is no response. **Workaround:** Remove stale TACACS server entries from the controller.

VLAN

Table 35 *VLAN Issues and Limitations*

Bug ID	Description
53835	AP-124 and AP-125 access points may not accept DFS channels. **Workaround:** None.
53408	If vlan ID is not set in virtual-ap profile, VAP is deleted when connectivity to controller is lost and AP is rebooted. **Workaround:** Set VLAN ID in virtual-ap-profile.
64452	The warning messages “number of VLANs limit exceeded 32” may be seen even if only 32 VLAN mapped to the VAP. **Workaround:** None.

Voice

Table 36 *Voice-Platform Issues and Limitations*

Bug ID	Description
44110	Cisco phones plugged via wire behind a RAP may reregister frequently with the Call Manager with the reason UCM-Closed TCP. The problem only occurs when we have a sccpv19 phone behind the RAP using Voice role. **Workaround:** Using authenticated role, audio works. If we have a sccpv12, audio works and we do not see any Deny sessions.
62713, 63490, 63107	Your controller might reboot unexpectedly due to an STM module crash caused by an incorrect setting of ALG in race condition. **Workaround:** None.
58554	Call status may not reset correctly for Alcatel OnmiTouch 8128 devices. **Workaround:** None.
57869	In some cases, the STM module may experience high CPU usage and AP drops due to ALG netservice configuration. **Workaround:** Remove the ALG netservice configuration.
58895	RTP packets are dropped for IP Touch 310/610pjones when noe-acl is applied. **Workaround:** None.

Web-UI

Table 37 *Web-UI Issues and Limitations*

Bug ID	Description
54467	When AP is provisioned with a white space in between the AP name (example: "AP NAME") the AP provisioning page comes up blank. **Workaround:** Do not use space in between characters of ap name.
52453	WPA-PSK Pre Shared Key not accepted in controller GUI. **Workaround:** Use CLI.
61674	You cannot create an AP provisioning profile for RAP 4G-LTE using the WebUI. **Workaround:** Use the CLI instead.

XML API

Table 38 *XML API Issues and Limitations*

Bug ID	Description
61674	Radius attributes `Aruba-Location-Id` is not filled when forward mode is Split-tunnel. **Workaround:** None

Chapter 3

Fixed In Previous 6.1.2.x Releases

The following issues were fixed in previous releases of ArubaOS 6.1.2.x:

Fixed in 6.1.2.7

Table 1 *Fixed in 6.1.2.6*

Bug ID	Description
62168, 63448	An unexpected AP reboot issue caused by a memory leak that occurs when the APs have a VAP configured in decrypt-tunnel mode has been fixed.
52758	Issue that occurs when the controller SNMPD module does not respond to the AMP's SNMP requests has been fixed.
61895, 61877, 61896, 62439	A datapth exception resulting in an unexpected controller reboot has been fixed. This datapath exception occured when a bandwidth contract was deleted while packets were being added to its queue.
62436, 60597, 62504	A datapath timeout that occured when local proxy ARP is enabled on a VLAN, resulting in a unexpected controller reboot, has been fixed.

Fixed in 6.1.2.6

Table 2 *Fixed in 6.1.2.6*

Bug ID	Description
50041, 51681, 52458, 57635, 61578	A unexpected hyrbid mode AP crash caused by change made to the phy-restart knob has been fixed.
59047	An unexpected AP crash caused by kernal page fault has been fixed.
60806	An unexpected AP crash that began with the raw trace `do_gettimeofday` has been fixed.
58358	A knob has been added under HT-SSID profile - sw-retry (type: boolean) to avoid packet drop for certain types of clients.
60860	The DHCP Offer packet is now correctly sent to the same VLAN as the DHCP Discover packet came from.
61435	An unexpected controller reboot caused by a datapath module crash due to an ASSERT condition in the SESSION_SET_MEDIA_COOKIE macro has been fixed.
61466, 61572	Bandwidth contracts are no longer incorrectly added as CP bandwidth contracts after being pushed from a master to a local controller.

Table 2 *Fixed in 6.1.2.6 (Continued)*

Bug ID	Description
53497, 56022, 58185, 57411, 59249, 61210	An unexpected controller reboot caused by an fpapps module crash due to a PAPI corruption has been fixed.
58965, 59813, 60711, 61598	An unexpected controller reboot caused by an fpapps module crash due to pointer initialization issue has been fixed.
60242, 61273, 61320	Multiple instances of datapath buffer allocation failures issues have been fixed.
58632	The Layer 3 incoming sessions that were not being accepted due to a max entry has now been fixed.
58921	An error in TLS processing is now fixed.
53494	The controller correctly processes NATed PPTP packets, allowing clients are able to establish a PPTP connection while connected to an Aruba controller.
61076	IKE is now able to rekey correctly at any time.
61229	DNS look up for FQDN master no longer incorrectly appends part of the domain information.
60448	When a client, connected to a 802.1x SSID, fails to authenticate, the controller no longer generates the message `authmgr[1542]: Error sending the trap to SNMP agent` and instead returns the proper log message.
52365	ArubaOS PVST+ now correctly interacts with and responds correctly to Cisco PVST+ topology change notification (TCN) BPDU.
59990	**User Firewall State** under **Monitoring> Clients> Status** now correctly displays traffic for bridge clients.
60808, 61375, 61124	An AP crash caused by an “unaligned access” issue while updating the multi-byte fields of some of the IEs present in beacons and probe responses has been fixed.

Fixed in 6.1.2.5

Table 3 *Fixed in 6.1.2.5*

Bug ID	Description
53443	If an AP loses power in the middle of a write operation, that APs custom environment settings may be reset to factory default values. Starting with ArubaOS 6.1.2.5, a remote AP only writes data to the flash memory when necessary, reducing the chance of AP errors if the AP loses power in the middle of a write operation.
52608, 54611	A potential AP memory leak caused by a double free issue has been fixed.

Table 3 *Fixed in 6.1.2.5 (Continued)*

Bug ID	Description
56815, 60790	An issue in which WPA2 802.1x split-tunnel user were intermittently not able to complete the connection with split-tunnel SSID until that RAP is rebooted has been fixed.
58993	When you upgrade to 6.1 from a pre-6.1 version of ArubaOS, IPv6 ACLs are now correctly carried over upon upgrading.
53904, 60036, 60049, 60293	A number of issues related to core dump decode resulting in an incomplete core file have been fixed. These issues included inability to access the user table memory from the SOS core file and a race condition that caused the intent/cause data to overwrite the SOS core dump; therefore, making it incomplete.
52536, 53302, 60009, 60406, 60477, 60354	An unexpected controller reboot caused by a datapath exception due a race condition scenario where SP can release a contract and in parallel FP may refreshing that particular contract has been fixed.
52770, 58764, 60371, 60480	An unexpected controller reboot caused by an arci-cli helper crash that due to a double free issue when the queried module is busy has been fixed.
57820, 57886, 57693, 58123, 58120, 59208, 59188	An issue in which the auth module might crash while the ccontroller is freeing a data structure in a memory management function has been fixed. This was most likely executed by an SNMP query from AMP for IP and MAC addresses by querying OIDs nUserPhyAddress and NUserIpAddress.

Fixed in 6.1.2.4

Table 4 *Fixed in 6.1.2.4*

Bug ID	Description
56747	A buffer leak caused by wi-fi encrypted jumbo frames which lead to a disruption in client connectivity and AP heartbeats has been fixed. Additionally, a new counter, called **WIFI Jumbo Denied**, has been added under `show datapath frame`.
59412, 56561	A change has been made to ArubaOS to prevent SOS crashes from incorrectly being interpreted as “User Pushed Reset.” Previously, the reason was written from sbHeartbeat process once a SOS had crashed. However, in somecases, the user process was not run because the kernel became occupied with the SOS core dump and the reason for reboot was never written. Therefore, upon reboot, the reason is interpreted as "User pushed reset." Now, the reason for reboot is written once the message that a crash has occurred is received from SOS and before the SOS core dump begins.
49034, 48995, 50733, 52040, 52995, 53669, 55788	An AP crash accompanied by a break instruction in the kernel code has been fixed.

Table 4 *Fixed in 6.1.2.4 (Continued)*

Bug ID	Description
49910, 53933, 56010, 56193, 57843, 54695	An unexpected AP reboot caused by a memory that occurred when an AP in air monitor mode was upgraded has been fixed.
46163, 55259	Improvements to the controller kernel prevent APs from performing unintended reboots.
51822	An AP reboot caused by a kernel page fault due to a corruption in mac_hash has been fixed.
52183	Uplink VLAN tagging now works with PPPoE enabled for RAPs.
52450, 54880, 54165, 54323, 58874	An issue in which APs connected to a local controller ignore association requests from clients after a reboot has been fixed.
53192	AP-120 series APs support the Kenya regulatory domain.
54847	ArubaOS no longer does DFS detection on channels 36-48 and 149-165 for Mexico and Vietnam.
54872	A performance drop observed on AP-105 with 20 MHz HT enabled when connected to Mac clients has been fixed. This performance drop was seen in the form of 10% to 13% packet loss on pings to the default gateway on the controller.
55398, 56467	Support for the AP-90 series has been added for Saudi Arabia.
55495, 46278	After failing over to a secondary controller after the primary controller goes down, APs that fall into the IL state due to a lack of licenses will move back to the primary controller when it comes back up.
56756	An AP reboot caused by a kernel panic that occurs when the AP comes out of power save and the AP tries to flush the legacy PS queue.
57740, 58379	An AP radio reset caused by beacon misses on the AP's wi-fi interface that occurred while the other interface was scanning has been fixed.
57906	An AP reboot caused by a kernel panic due to a memory corruption has been fixed.
57979	Dynamic VLAN assignments are now correctly maintained during roaming while in bridge mode.
58108	An unexpected AP reboot caused by a kernel panic that occurred while radio calibration was attempted during a radio reset has been fixed.
58132, 58105, 58333, 58334	An unexpected AP reboot has been fixed by preventing the AP from queuing new packets during a channel change.
58256	An AP-105 crash with raw call trace `asap_chrdev_tx_to_am` has been fixed.
46202, 50587, 53985	A captive portal performance slow-down issue that occurred when the webserver maxclients was configured with a value of 25 or more has been fixed.

Table 4 *Fixed in 6.1.2.4 (Continued)*

Bug ID	Description
49267, 57767, 58210, 59495, 59489, 59388, 56913, 54133	An httpd process crash that prevented user from logging onto the network using Captive Portal has been fixed. This process crash was caused large amounts of auth memory corruption resulting httpd restarting to recover that memory.
55918, 56486, 58987	When a user performs L2 authentication before captive portal authentication and logs out of the captive portal, the user's L3 role is correctly changed to the L2 authenticated role instead of the initial role. Additionally, this change is correctly reflected in the user table.
58144, 57889	Wired user from an untrusted VLAN of a port-channel are correctly redirected to the captive portal page configured on the VLAN.
53189	Improvements to the syslog process allow you to change user roles through the Extended Services Interface (ESI).
57229	All ESI server entries no longer flap when one ESI server becomes unreachable.
51965, 52714	Wireless clients now correctly receive IPv6 addresses due to changes to the way IPv6 policies are handled.

49344	If the following sequence of commands is entered on a 3000 Series controller, the Link LED no longer remains lit and solid (not blinking).
	`(config) #interface port-channel 1`
	`(config-channel)#add gigabitethernet 1/0`
	`(config-channel)#add gigabitethernet 1/1`
	`(config-channel)#shutdown`
	`(config-channel)#del gigabitethernet 1/0`
	`(config-channel)#del gigabitethernet 1/1`
	`(config-channel)#!`
	`(config) #interface gigabitethernet 1/0`
	`(config-if)#speed 1000`
	`(config-if)#duplex full`
	`(config-if)#!`
	`(config) #interface gigabitethernet 1/1`
	`(config-if)#speed 1000`
	`(config-if)#duplex full`
	`(config-if)#!`
	`(config) #interface port-channel 1`
	`(config-channel)#add gigabitethernet 1/0`
	`(config-channel)#add gigabitethernet 1/1`
	`(config-channel)#no shutdown`
	`(config-channel)#!`

51668, 51619, 52869, 53141, 53774, 54568	Unexpected controller reboot following a datapath timeout caused by a race condition has been fixed.
54001, 54076, 55528	A datapath module crash caused improper handling of duplicate netdestinations has been fixed.

Table 4 *Fixed in 6.1.2.4 (Continued)*

Bug ID	Description
54143	A controller reboot caused by a datapath module crash due to an issue with VIA SSL fallback has been fixed.
55304	The datapath route-cache now correctly refreshes and releases DHCP lease when the IP address is assigned to a new device or a clear arp all is executed.
56265	An issue in which the STM module was consuming huge amounts of memory due the amount of memory consumed by the per-AP PAPI buffers has been fixed.
56641, 58232, 58231	An unexpected M3 controller reboot due to a crash in the datapath module has been fixed.
56713	RAP-5 tunneled wired user can successfully ping the default gateway after a MAC auth VLAN change.
56802, 56803	An fpapps module crash due to tunnel entries that were not validated while an SNMP walk of the ifEntry was occurring has been fixed.
57145, 57414, 57596, 58515, 58996	An unexpected controller reboot caused by a corruption in PAPI message leading to an invalid ingress upon downloading it to the datapath has been fixed.
57251, 57253	A datapath module crash that occurred when decrypting client key exchange messages when using RSA 2048 certificates has been fixed.
57774	A datapath module crash caused by a datapath exception has been fixed.
54643	Per VLAN aaa profiles are no longer ignored if wired users are connected via untrusted port-channel.
32184, 33480	Large packets (larger than 1463 bytes) can now be passed successfully through an PPPoE connection on a controller.
56429, 56431	RAP failover is successful when switching from cellular to Ethernet for the first time when using a U600 modem.
56841, 53410	ArubaOS now dynamically adapt ACL message size when a network with a high amount of packet loss is detected between the controller and AP when pushing large ACL messages. This prevents the AP from receiving incomplete ACLs.
57406	A RAP ASSERT occurring when a wired-split-tunnel client is unplugged and plugged-in 5 or more times has been fixed.
57610	Wired clients connected to an untrusted port on the controller via a L2 switch correctly follow the user-derivation rule of the aaa profile and are no longer incorrectly placed in the initial role.
52141, 52316	The opmode Xsec now works correctly with RAPs in tunnel-mode.
56996, 56954, 57274	An auth crash due to the auth module dereferencing a NULL pointer for the AAA profile has been fixed.
57404	Special characters can be used successfully in the IKE key for RAPs.

Table 4 *Fixed in 6.1.2.4 (Continued)*

Bug ID	Description
57544, 54566	Removing a VLAN's association to a physical port no longer causes the associated VAP to become inactive.
57819	An auth module crash occurs when a client (connected to an open SSID) or AP sends deauth frames has been fixed.
57949	Prohibit IP Spoofing and Prohibit ARP Spoofing now work correctly and successfully prevent user with a spoofed MAC or IP address from passing traffic.
56167	The SVP session traffic DSCP value is correctly set on the outer GRE IP address.
57076	Dynamic ACLs are now added to the derived role instead of the default role and all ACLs are saved locally in auth and updated on the local controller after it receives a config from the master controller.

Fixed in 6.1.2.3

Table 5 *Fixed in 6.1.2.3*

Bug ID	Description
53880	802.11n is now allowed for the Russia (RU) Country Code.
54003	When spectrum devices history becomes full (256 entries) and a new device is detected, remove an older entry that has been aged-out (flag=deleted).
37469	Traffic shaping and airtime fairness are now supported in decrypt-tunnel and bridge mode.
52572	Throughput issues (i.e. excessive ping drops) with RAPs in Bridge Mode has now been fixed and throughput is now as expected
53376	A drop in throughput on the AP-105 that was observed during Iperf testing is now fixed.
55992	Video quality no longer degrades as a result of unplugging the client from a power source and switching to its internal battery.
54921	Race conditions, which appear while programming the AP key cache for D-tunnel leading to a network connectivity issue, is now fixed.
55195	In bridge mode, clients can now connect to APs configured with Mixed Mode opmodes (wpa-psk-aes, wpa2-psk-tkip only) and PSK enabled. The clients no longer displays a "waiting for keys" message and completes the first two exchanges in the 4-way handshake.
56993, 57167	An unexpected controller reload due to a STM module crash has been fixed.
52605	Per SSID bandwidth contracts now work correctly.
53301	A fix has been added to ArubaOS to improve the clean up SAs after deleting them. This fix corrects an issue in which ISAKMP SAs on a master controller showed over 10,000 even though there were no active RAPs on the controller.
53701	With DNS for AP discovery enabled, if the query for "aruba-master" is not replied with "no such name" then the AP now correctly tries to complete FQDN next as expected.

Table 5 *Fixed in 6.1.2.3 (Continued)*

Bug ID	Description
56210	When a wireless client sends a router solicitation (RS) to a router, the client receives the router advertisement (RA) from the router when a port-channel is setup between the router and the controller.
54538	The error message `WARNING!!! 10 minute CAC period as channel is a weather radar channel` is no longer used.
48933	iPad clients source NATed on a controller and connected to a Cisco VPN server (L2TP/IPSec) now successfully passes traffic and accesses the correct resources.
50302	Users connected to a decrypt-tunnel VAP are now able to stream video immediately upon association since the user correctly receives the first IGMPv2 query from the controller. This query is required to tell the client device to switch from IGMPv3 to IGMPv2.
53774	A race condition creating ICMP sessions that age out, which may cause datapath exception causing the controller to go down, is now fixed.
47806, 52928	When **no IP routing** is enabled under the switch VLAN, routing across VLANs will now work correctly.
55007, 53230	An issue in which corrupted packets caused the datapath CPU to hang has been fixed. In this case, the control plane did not complete the core dump and ended up showing as a kernel panic.
56168, 56799, 56647	A fix was added to ArubaOS to re-enable immediate freeback as the xgmac RxDesc count was going very low (under 0x10) under heavy network load of IP fragments and leading to continuous AP rebootstraps.
54075, 54567, 56479, 56277, 56037, 56632, 56663, 56784, 56997, 56998, 56818, 57158, 57237	An httpd module crash that occurred during an SSL key exchange during web login has been fixed. This crash was specific to clients using custom (Elliptical Curve) certificates for SSL instead of the default RSA certificates.
52781, 52779, 51937	A check has been added to ArubaOS to ensure that the RAP configuration information sent by the master controller is not overridden.
52902, 55698	Improvements to the user-miss counter fixes a situation where a falsely high user-miss threshold could causing IP frames to be dropped, incrementing the 'Frames dropped due to excessive user misses' counter.
53971	Large frames are bridged locally on PPPoE split-tunnel RAPs. Note that this fix is specific to PPPOE RAPs and will send an ICMP error to the client when the client packet size crosses the PPPOE MTU. The client will then send a packet with a size lower than the MTU.
53511	An issue in which Captive Portal users, after authenticating successfully, are placed in the correct role but incorrect policies are applied to them is now fixed.
53526	When a user is assigned a VLAN-based aaa profile and then moves to a VLAN that assigns that user a different aaa profile, the user no longer improperly retains the user role assigned to it by the previous VLAN.

Table 5 *Fixed in 6.1.2.3 (Continued)*

Bug ID	Description
54763, 55914	ArubaOS now allows a station entry to be created when L2 miss is generated from Aruba controller when used as L3 gateway and now prevents station entry creation when L2 miss is generated from switch's own mac addresses for any reason. This change allows per-vlan aaa profile to work correctly for wired user connected via a L3 gateway.
56063	Bridge entries in datapath of a trusted port are now cleared when a VLAN is toggled from trusted to untrusted.
54534	When static WEP is used, some clients are no longer unexpectedly deauthed while roaming due to an internal timing issue between the client's association request and the processing of any data that has already been sent.
54912	Server derivation from a RADIUS server is no longer ignored and now works correctly and clients are now placed in the correct role.
54966, 56550	An unexpected controller reboot caused by a auth module crash due to the noname flag being set for netdestinations created for h323-acl acl from STM has been fixed.

55730, 55883, 55676, 55808, 56449	An issue in which auth returns the following error messages every time a client connects has been fixed.
	`<ERRS> |authmgr|  Message to 127.0.0.1:8228(Datapath) with MsgCode 0, Msglen 0, and Msgtype 0 failed with Errno 0, Errstr Success`
	`<ERRS> |authmgr|  Message to 127.0.0.1:8359(DHCP Daemon) with MsgCode 10006, Msglen 0, and Msgtype 0 failed with Errno 0, Errstr Success`

56767	A fix has been added to cleanup cached bandwidth contracts when snapshot is received.
56774, 56827	An auth process issue due to a single MAC address, with more than one user entries (due to wired to wireless roaming), being freed multiple times has been fixed.
52901	If a user is already authenticated (authtype captive portal) and there is no captive portal profile defined for L3 role that the user is in, the user does not change role.
53328	A fix has been added to ArubaOS to ensure that `ip cp-redirect` works correctly. The correct IP address is now resolved to the controller IP as configured.
54930, 54919, 54524	Captive Portal clients are no longer incorrectly placed in the post Captive Portal auth role after changing VLANs. They are now correctly treated as new users and redirected to the Captive Portal logon page.
53081, 54983, 56620	An issue in which captive portal users are reset to the logon role after terminating on a controller being used as a gateway and the captive portal AAA profile is applied on the VLAN is now fixed.
54238, 54409, 54333, 54521	When Machine Authentication is enabled with machine derivation and user derivation, if the user derivation, the user now successfully passes machine authentication, and user authentication. The user derivation now succeeds and the users will move into the correct role.
48980	An auth module process crash that caused the controller to reboot is now fixed.
54342	The auth module crash following a datapath exception caused by a buffer overflow is now fixed.
56683	An unexpected controller reload that occurs while the controller is looking for an existing session of a recently authenticated user to enforce single session for a captive portal user has been fixed.
56695	An unexpected controller reload due to a auth crash has been fixed.

Table 5 *Fixed in 6.1.2.3 (Continued)*

Bug ID	Description
49267, 51610, 52412, 53239, 53453, 54133, 54891, 54772, 54827	An httpd module crash, which occurred during instances of high Captive Portal utilization, and accompanied by high auth memory usage that led to httpd restarting (to recover memory) is now fixed.
53772	An issue in which spectrum mode APs stopped sending spectrum data to the controller with no data seen in the spectrum WebUI page and the `spectrum_hang_detect_tasklet RESETTING` error message appearing repeatedly in the syslog is now fixed.
53819	An unexpected controller reboot caused by an STM module crash has been fixed.
54096, 54241, 55570, 56737	A controller reboot caused by “Nanny rebooted machine - low on free memory” due to voip server as voice client is allocated every time when a msg is sent from server to client is now fixed.
54703	An unexpected controller reboot caused by an STM module crash due to memory corruption from a Vocera ALG has been fixed.
54810	STM now correctly ages out association records when dos-prevention is enabled.
55266	An unexpected controller reboot caused by an STM module crash has been fixed.
56043	Multiple instances of the same BSSID no longer incorrectly appear in `show ap bss-table ap-name` and `show ap debug remote bss-table ap-name` for a specific AP.
56428	An STM module crash caused by an error in processing NOE frames has been fixed.
52380, 54193, 52794	An STM module crash occurring in the H323 message parser is now fixed. The fix increases the message buffer to accommodate larger protocol messages.
56167	The TOS in the outer GRE header for voice ALGs has been fixed.
54527, 55009, 54508, 54697	Attempting to view **Security > Authentication > Profiles > AAA Profile** or **Access control > User Roles** in the WebUI does not throw an error message a pop-up error message.

Fixed in 6.1.2.2

Table 6 *Fixed in ArubaOS 6.1.2.2*

Bug ID	Description
45481, 35246	When receiving PVST BPDUs on non-default native VLANs, while Spanning Tree Protocol is disabled, the packets are now correctly moved into the forward state from the bridging state and the flooded on the VLAN.

Table 6 *Fixed in ArubaOS 6.1.2.2 (Continued)*

Bug ID	Description
51553, 51728, 52750, 53819, 54967, 53819, 54967, 53540, 54412	An unexpected controller reboot caused by an STM module crash has been fixed.
51951, 53080	The mgmt user no longer fails RADIUS or TACACS authentication after upgrading to ArubaOS 6.1.x. This issue was caused when the auth module on the controller attempted to contact AAA before AAA had come up.
52378	An auth module crash on the M3 has been fixed. This auth module crash occurred when an empty netdestination, without any entries, was assigned to and then deleted from a session ACL.
52450, 54880, 54165, 54323	An issue in which APs connected to a local controller ignore association requests from clients after a reboot has been fixed.
54628, 54817	Syslog server configurations are no longer lost upon upgrading.
54383, 54906	WPA/TKIP clients no longer become stuck at the group key exchanges after completing the four way unicast key exchange.
54711	The configured DHCP lease time is no longer lost when upgrading to ArubaOS 6.1.x. This issue was caused because the “seconds” level of DHCP lease time was not available in previous versions. Upon upgrade, the seconds value displays 0.
55104	An unexpected controller reboot caused by a datapath timeout has been fixed.

Fixed in 6.1.2.1

Table 7 *Fixed in ArubaOS 6.1.2.1*

Bug ID	Description
51990	APs no longer reboot during LMS/BLMS Failover testing.
53548	Clients connected to the same WLAN on a campus AP are now able to ping each other.
53566	A rogue AP that was detected with an ESSID name with an apostrophe was not classified correctly in a syslog message log. This issue is now fixed.
53953	Apple MacOS X devices are now able to pass TCP traffic. This applies to Mac’s manufactured in 2011.
54039	AP classification, which did not occur after upgrading to 6.1.1.0 for any AP, is now fixed.
54141	The WebUI AP Installation page now correctly reflects the reprovisiong of USB parameters.
54233	The AP-135 now closes the channel properly.

Fixed in 6.1.2.0

Table 8 *Fixed in ArubaOS 6.1.2.0*

Bug ID	Description
36941, 48318	ICMP requests are no longer being blocked on the local controller during config synchronization with the master controller.
43341	Controllers now respond to DNS queries with their own IP addresses.
49907	Multicast now works correctly when port channeling is enabled on the master controller.
49977, 50665	An isakmpd module crash caused by VRRP flaps has been fixed.
50702	IPv6 packets are no longer dropped when “broadcast-filter all/arp” is enabled.
50094, 52277	An issue in which APs did not come up after an upgrade due to mesh causing a DSCP value to be set in PAPI packets has been fixed.
50893, 51812, 52174, 51474, 52544	An issue in which APs are not coming up with the error message `PAPI_Send failed: No buffer space available` has been fixed.
52800	This release supports 4G-WiMAX on a RAP.
52953	VRRP over L2 GRE tunnels now works correctly.
52959, 52836	A controller auth module crash has been fixed.
53041	The Max ADP Time has been increased to 60 for AP Platforms (except RAP-2WG and RAP-5WN) to allow enough time for statically provisioned APs to complete ADP/DNS master discovery.
53267	EAP-termination now works correctly on the 620 controller.
53846	Ancillary image files are not deleted during boot up so that image the integrity check will pass the next time the controller is rebooted.

Fixed in 6.1.1.0

Table 9 *Fixed Issues in ArubaOS 6.1.1.0*

Bug ID	Description
44942	Instead of displaying single bit ECC error in the error log, these errors are counted and displayed as a counter in `show memory debug`.
50863	The controller will no longer generate any USBHelper syslogs unless a NAS/Printer Server configuration has been set up.
51844	An M3 controller module, connected via dual-uplink with PVST+ running, no longer learns the src MAC address from the alternate port of PVST+.

Table 9 *Fixed Issues in ArubaOS 6.1.1.0 (Continued)*

Bug ID	Description
51953, 52114, 52294, 52619, 52792	A datapath exception causing VIA controllers to reboot regularly has been fixed.
51387, 52451, 52395, 52452	Clients are now placed into the correct user roles when from one SSID to another and back again.
52632	AAA profiles can be correctly assigned to a VLAN using the WebUI.

Fixed in 6.1.0.0

Table 10 *Fixed Issues in ArubaOS 6.1*

Bug ID	Description
31074	The SNMP fault list now correctly clears RADIUS servers from the fault list when the server comes back into service.
31783	RAPs are able to establish IPSec connections when up to 64 character isakmp key.
32807	The controller now correctly blocks H.323 calls when the H.323 Call Capacity is reached. When the call is blocked, the blocked client is automatically deauthenticated.
35928	All APs that terminate on the same controller are correctly identified as a valid AP not an interfering AP.
36123	XML query with usernames now works correctly.
37115	The time it takes for the controller to locate APs for the first time, or after the cache has expired, has been improved and no longer causes the WebUI to freeze for long periods of time.
38938	The errorlog no longer shows a missing VPN auth profile for every reboot of the controller when there is a RAP terminating on that controller.
40032	The AP-105 no longer constantly detects spurious radar when operating DFS channels (52, 56, 60, and 64).
41299, 45362	An IP pool leak that was preventing users from connecting using L2TP VPN has been fixed.
41363	APs come up successfully if their AP Group Name contains a + symbol.
42333, 42332	wlanAPSysLocation has been added to AP table, which gives the value of the syslocation provisioning parameter for the AP.
42717	RAP fail-over to the backup cellular link in a case where ethernet link is NOT down, but some intermediate (between RAP and controller) connectivity is broken now work correctly.
43026	The font size of the guest provisioning printout will the size that is configured.

Table 10 *Fixed Issues in ArubaOS 6.1 (Continued)*

Bug ID	Description
43215, 43915	Clients correctly receive a DHCP ACK not matter what broadcast flag bit is applied to the DHCP request. To allow this, shaping/policing for multicast and broadcast traffic on APs based on descriptor usage has been disabled.
43300	The issue with the pause in traffic during the Chariot throughput test has been fixed.
43802, 44696	A datapath timeout that occurred when pkt-trace global was enabled has been fixed.
43855	When a certificate on a local controller expires, it can no be overwritten and deleted to make room for a new certificate.
43948, 41351, 45266, 45689, 45002, 46391, 47928, 46486	An AP reboot issue caused when the AP runs out of memory has been fixed.
44126	Client devices equipped with an Intel 4965AGN NIC can now maintain a connection and pass traffic when connected to an AP-125 via an HT SSID.
44504	The command `show user location` now provides the correct information.
44794	An issue which many bridge mode users were listed with a 0.0.0.0 IP address and many users could be seen in the datapath user table but not in the user-table has been fixed.
44846	An issue in which APs bootstrap during a write mem on the master controller has been fixed.
45009	A connectivity issue caused by abnormally large `Available TX Buffers` counts has been fixed.
45053, 46234, 39935, 45710, 45203	Improvements have been made to the stm module to prevent the controller and APs terminating on it from experiencing unintended reboots.
45126	When a RAP is in always or backup mode, the radio LED will light up to indicate that AP is up.
45202	The minimum frame size on encrypted channel has been reduced from 16 bytes to 8 bytes. This is to ensure that EAPOL-Start packets on encrypted channel are correctly decoded.
45270, 46442, 45744	Unexpected controller behavior due to a datapath exception has been fixed.
45383, 42958	The RAP-5 no longer crashes with the message “PPP: Termination Request Received” when using a 3G modem.
45384, 46355	AMSDU is now disabled by default with a knob in the firewall command in the CLI.
45534	Clients that support PMK caching are now placed into the correct cached user role after a disconnect and reconnect. When connecting to the same BSSID, the cached user role information is used.
45606	The Handoff Assist log message has been enhanced to show the actual low RSSI of the client.

Table 10 *Fixed Issues in ArubaOS 6.1 (Continued)*

Bug ID	Description
45643	An AP-85 mesh point crashed caused when the AP attempts to process large frames has been fixed.
45669, 46617	AP coverage is now shown correctly on the RF Plan heatmap.
45694	The controller is now able to respond to ARP requests from a client when the ARP request is coming from a port-channel.
45858	The option Include Technical Support Information is not selected by default when logs are downloaded.
45866, 44712, 50392, 44934	A datapath timeout issue causing the M3 controller to continuously reboot after upgrading has been fixed.
45943	In the WebUI, you can create an SNMP password with any number of characters instead of 5 or more characters.
46027	ArubaOS now ignores transient timeouts as long as subsequent LDAP requests are seeing responses back from the LDAP server.
46095	Unexpected controller behavior in the Mobile IP module caused by a race condition has been fixed.
46204	The controller's buffer size has been increased for EAPOL packets to help prevent authmgr crashes.
46251	Wireless clients no longer incorrect get a role from the wired aaa profile after an auth restart.
46321	Users are able to establish passive FTP connections.
46340	46340 ZTE modem ttyUSB no longer changes between cold and warm boot.
46483	Improvements to the Auth and STM modules prevent the controller from failing to respond due to IPIP loops.
46624	For APs using a bridge-mode SSID, VLANs in a virtual AP profile no longer appear in the Datapath VLAN Multicast Entries table, since the VLAN is only local to the bridge.
46701	A RAP-5 crash that happens when the RAP is connected to an EVDO device has been fixed.
46747	A Mesh portal and point crash due to an assertion in ieee80211_decap() has been fixed.
46761, 51443	An SNMP walk issue that breaks at `wlsxVoiceAPBssidInfoGroup` has been fixed.
46839	An AP-125 crash in skb_over_panic has been fixed.
47032, 49982, 50528, 51329, 52043	The DNSmasq process on 600 Series controllers has been improved to allow a DNS query of a domain name longer than 51 characters.
47048	Aruba-ESSID and Aruba-Location-ID are no longer missing from RADIUS requests sent to an external server when the client is authenticated by an XML-API command.

Table 10 *Fixed Issues in ArubaOS 6.1 (Continued)*

Bug ID	Description
47074	Users no longer lose IP connectivity when using split-tunnel mobility solution.
47219, 47402	The controller no longer stops forwarding traffic to clients connected via PPTP.
47313	A controller reboot caused by udbserver module crash has been fixed.
47553	A controller STM crash caused by a control process exception has been fixed.
47614	You can now successfully delete session ACLs from a policy when using the WebUI.
48040	Legacy AP with aggressive scanning settings now scan as expected.
48107, 48802, 38376	An issue in which the error log displays the message `SNMP agent timed out when sending a request to application WMS for object (object id)` and reports the controller as down when it is not has been fixed.
48242	When a TACACS accounting message fails, the SNMP trap returned by the controller under User Authentication Failed displays the user and MAC address instead of zeros.
48243	TACACS failed/success management authentication log messages now include the user name for the failed request.
48244	The controller now sends SNMP traps for failed TACACS management authentication.
48459	APs are no longer slowly running out of memory (memory leak).
48537, 50123	Authentication issues, accompanied by RADIUS timeout stats increasing, when static-wep and VLAN derivation are enabled has been fixed.
48623	The log message 301257 has been reclassified from INFO to DEBUG and the host IP information has been added.
48660	An error log message has been added to report if ArubaOS failed to decode mppe key attributes.
48758	Clients are now able to reconnect after being removed from the blacklist table and if the Max Auth failure value is set to 0, clients are not blacklisted. Additionally, the blacklist time can be set to values less than 3600 seconds.
48838	The **Clear Session on Role Update** firewall now works correctly in the case of a RADIUS disconnect event.
49038	An auth crash caused by a memory leak due to LDAP authentication timeouts has been fixed.
49271	You can now successfully delete a Captive Portal profile and user role without needing to restart the auth and httpd processes.
49321	The RADIUS attribute for Aruba-Location-Id is now correctly filled when the forwarding mode is split-tunnel.
49418, 38174	Disabling VRRP preemption now works correctly in a master-local setup.
49576	When a server certificate is installed, controller now correctly responds to DNS query with the IP address specified by `ip cp-redirect-address` configuration.
49825	The formatting for the command `show phonehome stats` has been improved.

Table 10 *Fixed Issues in ArubaOS 6.1 (Continued)*

Bug ID	Description
49985	When using Safari, the configuration fields are now correctly displayed when configuring ports under **Configuration > Network > Ports > Port** in the WebUI.
50027, 50026	A controller ISAKMPD module crash caused by a low memory state has been fixed.
50313	In the WebUI, the client activity graph for wired clients on a campus AP now correctly displays information.
50578	An AP STM memory leak initiated by a controller deauth has been fixed.
51258	An httpd module crash that prevents the WLAN wizard from working in any browser has been fixed.
49184	Upgrading by FTP using the WebUI now works correctly.
48867, 48996	Users now correctly move to the server role with user derivation rule `vlan equals bssid` and server derivation `role equals Server-Name` with dot1x termination.
48325	RAPs over PPPoE no longer crash when the ap-group has split-VAP and a bridge mode wired-AP.
48190	The **Upload from local file** option for upgrade now works when used through the WebUI.

Chapter 4

Known Issues Identified in Previous 6.1.x Releases

The following are known issues and limitations for this release of ArubaOS. Applicable bug IDs or workarounds are included.

Access Points

Table 1 *Access Point Known Issues and Limitations*

Bug ID	Description

57624	It has been observed that AP-105s might not come up when connected to a Cisco PoE switch (WS-C6509-E:WS-X6148A-GE-45AF). The APs are not powering up despite the maximum amount of power being allocated to the port the AP is connected to. The following error messages were returned when a shutdown/no shutdown was executed on the port the AP was connected to:
	`%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEthernet9/48 (not half duplex), with SEP001BD5E87C32 Port 1 (half duplex).`
	`%C6K_POWER-SP-1-PD_HW_FAULTY: The device connected to port 3/2 has a hardware problem. Power is turned off on the port.`
	`%C6K_POWER-SP-1-PD_HW_FAULTY: The device connected to port 3/2 has a hardware problem. Power is turned off on the port.`
	Workaround:
	None.

60530	The following error message will appear if you attempt to add an already existing route to your configuration. This error has not impact on network connectivity. AP <*ap-type*>@<*ipaddress*> sapd| An internal system error has occurred at file sapd_redun.c function setup_ipsec line 1156 error setup_ipsec:ROUTE ADD ERROR. **Workaround:** None.
55186	The AP-105 and AP-90 series access points do not work properly on 2.4 GHz when located close to a cellular DAS antenna. **Workaround:** Move the cellular DAS antenna away from the AP.
56883	An issue has been identified where a client's signal-to-noise ratio (SNR) becomes 0 after completing a roam. Additionally, it can take anywhere from 10 seconds to 1 min for the clients SNR to return to a non-zero value. **Workaround:** None.
56678	In Advanced Monitoring, the client goodput value might display half of the expected value. The cause for this is currently unknown. **Workaround:** None.

ARM

Table 2 *ARM Known Issues and Limitations*

Bug ID	Description
56760	Per-ssid bandwidth contracts do not work well with de-tunnel mode with UDP traffic. For example: • the actual bandwidth allocation is around 25% off compared to the configured bandwidth allocation. With tunnel mode, the error rate is only 5-10%. • the maximum UDP throughput for a single client is only 155 Mbps, which is about 30Mbps off when compared to 183 Mbps in tunnel mode. **Workaround:** None.

Bootloader

Table 3 *Interface Issues and Limitations*

Bug ID	Description
53818, 60880, 62704, 63470	Upon upgrading, a controller may encounter an error when attempting to read the boot partition from the nvram. When this happens, the controller will enter a continuous reboot loop. **Workaround:** You must interrupt the boot process by executing the `def_part {0|1}` command and `bootf` command to get the controller to boot up.

Captive Portal

Table 4 *Captive Portal Known Issues and Limitations*

Bug ID	Description
58729	The command `ipv6 cp-redirect-address` disable does not work. **Workaround:** None.

DHCP

Table 5 *DHCP Known Issues and Limitations*

Bug ID	Description
55010	Wired clients connect to and receive an IP address from a different VLAN after the controller is rebooted instead of connecting to the VLAN they were connected to prior to the reboot. **Workaround:** The client must renew its IP address using the `ipconfig /release` and `ipconfig /renew` commands.

Interface

Table 6 *Interface Issues and Limitations*

Bug ID	Description
60991, 62298, 62909	On a 3000 Series controller, using SFP-SX transceivers, the link state will indicate going up continuously in the syslog. The actual link state itself does not flap. However due to the link up transitions internally, STP, OSPF, LACP will not converge. If you are not running any of these protocols on that port, there should be no effect. **Workaround:** Use copper ports instead.

IPSec

Table 7 *IPSec Known Issues and Limitations*

Bug ID	Description

56606	The following show commands return the error message shown below instead of returning any information in the Tech Support logs.
	`% Invalid input detected at '^' marker.`
	
	`show crypto l2tp`
	`show crypto-local pki trustpoint`
	`show poe`
	`show mux config`
	`show mux state`
	`show voice prioritization`
	Workaround:
	None.

IPv6

Table 8 *IPv6 Known Issues and Limitations*

Bug ID	Description
57067	IPv6 AP's are not coming up on controller which is connected to Untrusted port. The IPv6 APs go into the ap-role. However, since the ap-role does not have any IPv6 ACLs, the APs are not coming up on controller. **Workaround:** Add IPv6 ACLs to the ap-role.
57059	When the maximum IPv6 addresses are configured on a controller, basic routing fails. This issue only occurs in IPv6. **Workaround:** It is advised to configure only the required number of IPv6 addresses. The system can hold up to 1300 addresses in M3.
55786	IPv6 Ping fails to the controller on 600 Series controllers with `broadcast-filter all` Enabled on User-vlan. **Workaround:** Disable `broadcast-filter all`.

Table 8 *IPv6 Known Issues and Limitations (Continued)*

Bug ID	Description
57124	Neighbor Discovery does not work with bcmc-optimization enabled. Enabling bcmc-optimization could cause ping to the controller interface to fail from the Users, which internally would affect WebUI access and all over IPv6 **Workaround:** Disable 'bcmc-optimization' from the VLAN interface.
57239	Datapath Utilization might spike with multiple IPv6 user traffic coming from Android devices. **Workaround:** Reload the controller.
42724	When connected to a IPv6 router via an L2 GRE tunnel between two controllers, router advertisements (RAs) do not reach the client. However, the client is able to ping the router's link-local address. **Workaround:** None.
50648	Any IPv6 sessions greater than 420k might experience packet loss and the allocation failure counter under `show datapath session ipv6 counters` will increase. **Workaround:** None.
56645	The following CLI commands do not work in parity with regards to IPv4: • `show ap blacklist-clients` for IPv6 users does not show proper reason • `no support for global user-table` for IPv6 users (show user-table unique will not display IPv6 users) • `show log user` displays IPv6 APs in v4 format • `show log ap-debug` displays IPv6 APs in v4 format • `show datapath route` has separate command for ipv6 routes `show datapath route ipv6` • `show datapath route-cache` has separate command for ipv6 route-cache `show datapath route-cache ipv6` • `show datapath user` has separate command for ipv6 users `show datapath user ipv6` • `show datapath session` has separate command for ipv6 sessions `show datapath session ipv6` • `show datapath tunnel` has separate command for ipv6 tunnels `show datapath tunnel ipv6` • filtering users from user-table will not work for IPv6 users as is. Use corresponding `show ipv6 user-table` command filters • `show aaa state user <ipv6>` will not work. The same info can be retrieved from `show ipv6 user-table ip <addr>` The following commands do not work for IPv6 APs: • `show memory ap` • `show datapath route ip-addr <addr>` • `show datapath route-cache ip-addr <addr>` • `show datapath user ip-addr <addr>` • `show datapath frame ip-addr <addr>` • `show datapath nat ip-addr <addr>` • `show datapath port ip-addr <addr>` • `show datapath session ip-addr <addr>` • `show datapath vlan ip-addr <addr>` • `show datapath vlan-mcast ip-addr <addr>` • `show ap debug received-config ip-addr <addr>` • `show ap wired stats ip-addr <addr>` **Workaround:** None.

LDAP

Table 9 *LDAP Known Issues and Limitations*

Bug ID	Description
54239, 54240, 58384	It has been observed that the auth module may crash when one of the following actions is performed: `aaa-test server, aaa query-user,` or `any LDAP query`. These crashes are accompanied with this error message: **Auth server did not reply in time or auth module is too busy. Please make sure Auth server is alive and try again. Use 'show aaa authentication-server all' for more info.** **Workaround:** None.

Licensing

Table 10 *IPv6 Known Issues and Limitations*

Bug ID	Description
55839	When the `Available Campus AP's` shows 0, no new APs are able to come up unless some used licenses become free. **Workaround:** None.

Local DB

Table 11 *Local DB Known Issues and Limitations*

Bug ID	Description
53391	An invalid RAP whitelist entry is added when `local-userdb-ap add` is issued with the `remote-ip` parameter. Specifically, An entry with Remote-IP 0.0.0.0 is added to RAP whitelist when `local-userdb-ap add mac-address <MAC> ap-group <group> ap-name <name> remote-ip <valid IP>` is issued. **Workaround:** None.

Management

Table 12 *Management Issues and Limitations*

Bug ID	Description
62296, 62297	An Aruba 651 controller is susceptible to continuous rebooting if its internal AP (radio) is configured in Air Monitor mode (am-mode). **Workaround:** Reconfigure the internal AP (radio) in Access Point mode (ap-mode). Alternatively, you may disable the radio if not needed.
60318	In some cases, your controller auth module might restart, resulting in momentary impact on your users. **Workaround:** None.

Table 12 *Management Issues and Limitations (Continued)*

Bug ID	Description
60657	In some cases, your controller might unexpectedly reboot due to a STM module crash occurring at mmRetrieveStats, resulting in momentary impact on your users. **Workaround:** None.
54655	In a stand-alone master controller deployment, the user table may show conflicting information with that in the station-table. For example, the user table may show all that clients are connected to remote AP when in reality they are connected to a campus AP. The client table of the RAP will show that none of the clients are associated. **Workaround:** None.

Mesh

Table 13 *Mesh Known Issues and Limitations*

Bug ID	Description
56642	In some cases, an AP-135 configured as a mesh point will fail to upgrade in the mesh link to an AP-125 mesh portal is using HT and `mesh-ht-ssid-profile:supported-MCS allows 0-23` (the default). This issue only occurs in mixed-AP deployments. **Workaround:** If the supported-MCS is configured to 0-15, the issue is solved.

OCSP/CRL

Table 14 *OCSP/CRL Issues and Limitations*

Bug ID	Description
55419	The certmgr module becomes busy when a large number of OCSP requests hit the certmgr when OCSP server is not reachable. This issue will appear whenever there is misconfiguration or outage between the controller and the OCSP responder. **Workaround:** None.

OSPF

Table 15 *OSPF Issues and Limitations*

Bug ID	Description
54117	16-character OSPF authentication keys are truncated to 15 characters in the output of `show ip ospf interface`. **Workaround:** Use a 15-character or less authentication password.

Platform/Datapath

Table 16 *Platform/Datapath Known Issues and Limitations*

Bug ID	Description
54191, 55794	A datapath exception can occur due to a race condition where FTP data session is deleted due to inactivity and datapath tries to access delete/invalid entry. **Workaround:** This issue can be avoided by allowing FTP traffic on port 20. Enable traffic on port using the following: `netservice svc-ftp tcp 20 21 alg ftp`
53332, 53152, 53053,	In some cases, the datapath module might crash leading to an unexpected controller reboot. This crash is due to certain invalid/corrupted frames not being dropped after multi-level GRE decapsulation. **Workaround:** None.
54907, 55436	The controller might experience a SOS module crash at user_add_l2 when a newly connected client attempts to complete 802.1x authentication. **Workaround:** None.
63083	If a bandwidth contract is applied under the user-role, your controller might unexpectedly reboot due to a datapath exception. **Workaround:** Remove the bandwidth contract under the user-role.
61272, 60744, 60992	When upgrading a local or master controller to ArubaOS 6.1.2.6, when any APs failover to a LMS backup controller that has already been upgraded, that backup controller will crash. **Workaround:** You must reboot all master, local, and backup controllers simultaneously. See the "Upgrading in a Multi-Controller Network" on page 73 for information about upgrading a multi-controller environment.
59334	In some cases, the kernel module might restart due to a control processor kernel panic. This may lead to an unexpected controller reboot. **Workaround:** None.
59190	In some cases, a bwm-contract applied to initial role may cause a ~50% degradation on captive-portal performance. In this scenario, a bwm-contract is applied downstream on the initial role and both side on captive-portal final role. However, it is observed that the direction the bwm is applied does not matter. **Workaround:** None.
58487	In some cases, with CPSEC enabled, APs might take a long time (more than 30 minutes) to come up. This is due to CPSEC SA setup timing out because the AP is not receiving the fourth IKE packet from the controller. **Workaround:** None.
57344, 57864	In some cases, the Crypto engine may become stalled on a controller causing it to lose connection to its master controller and preventing all 802.1x clients from connecting to the network. Additionally, the number of IPSec and AESCCM encryption failures continues to go up and the controller cannot send a single IPSec or AES packet. **Workaround:** None.

Table 16 *Platform/Datapath Known Issues and Limitations (Continued)*

Bug ID	Description
54635	High datapath utilization is observed when Apple iDevices negotiate BA with AMSDU traffic. **Workaround:** Starting in 6.1.2.4, you can prevent iDevices from sending AMSDU using the knob `no ba-amsdu-enable` under `wlan ht-ssid-profile`. This prevents iDevices from setting up BA with AMSDU and reverting to MPDU-Agg.
57450	Port Channel (LACP) with PVST+ disabled might result packet loss between controllers. **Workaround:** Disable Port Channel or enable PVST+.
54869	In some cases, the kernel module might restart may lead to an unexpected controller reboot. Additionally, the reason for reboot was incorrectly reported as “Reboot Cause: User reboot.” **Workaround:** None.
55948	The error message `Unable to open system file /dev/max6657 in check_max6657, hwMon.c:2123` can randomly appear in the errorlog of the controller. The message appears when the temperature sensor in the controller is not responding. **Workaround:** Rebooting the controller can resolve the issue.
55998	When copying a software image from one partition to another on the same controller, the ancillary image is not copied along with the core image. This will cause ArubaOS to report that ancillary verification has failed. **Workaround:** Copy the image file to each partition from an external source.
54854, 54851, 54856, 54852	In some cases, the nanny module might restart due to a low memory state. This may lead to an unexpected controller reboot. **Workaround:** None.
55222	During an upgrade, 3200 and 600 Series controllers may receive the incorrect ancillary.tar files. This issue can occur in the following scenario: 1. Run 6.1.2.2 from partition 0. 2. Copy 6.1.2.2 to partition 1. 3. Copy 3.4.3.3 to partition 1. 4. Downgrade to 3.4.3.3. 5. Copy 6.1.2.2 to partition 1. 6. Upgrade to 6.1.2.2. **Workaround:** Performing an additional upgrade to 6.1.2.2 resolves this issue.
54156, 55217	ArubaOS do not support APs connected to Tunneled Node ports. **Workaround:** None.

PPTP

Table 17 *PPTP Issues and Limitations*

Bug ID	Description
55177	MacBook clients running Mac OS X 10.6.7 connected to controller configured as a PPTP server are disconnected if idle for 10 minutes. This does not affect Windows clients. **Workaround:** None.

RADIUS

Table 18 *RADIUS Issues and Limitations*

Bug ID	Description
55311	In a network where IPv6 is enabled and IPv6 traffic is not very active, the IPv6 user entry will idle-out frequently. When the IPv6 entry for a MAC address idle-out, a RADIUS accounting STOP packet is sent. At that time, the RADIUS accounting session ID for all L3 user entries belonging to the same MAC address will be cleared out. This includes IPv4 entries. **Workaround:** If IPv6 is not required, you can disable IPv6 on the client side. Otherwise, there is no workaround.
57005	A controller might report incorrect values in the Radius Accounting Stop packet for Acct-Input-Octets/Acct-Output-Octets attribute. **Workaround:** None.

Remote Access Points

Table 19 *Remote Access Point Issues and Limitations*

Bug ID	Description
51546	3G to wired failover might cause interruptions in packet flow and leaves the USB-connected 3G modem in a hung state. **Workaround:** None.
59433	When wireless clients in a split-tunnel role roam from one RAP to another RAP, TCP based sessions fail. The TCP connection continues for a few seconds after the roam is complete but, shortly after, the file transfer stops. **Workaround:** None.

57196	The following commands cannot be executed on a controller where is RAP behind RAP is terminating. Note that this issue appears only when the RAP's uplink is EVDO/3G modem.
	`show ap monitor ap-list  ap-name <ap-name>`
	`show ap debug system-status ap-name <ap-name>`
	`show ap debug radio-stats ap-name <ap-name> radio 0 advanced`
	`show ap debug radio-stats ap-name <ap-name> radio 1 advanced`
	Workaround:
	None.

Table 19 *Remote Access Point Issues and Limitations (Continued)*

Bug ID	Description
56661	Split DNS functionality (resolving internal domains from DNS server behind controller and using ISP DNS for all other queries) does not work if RAP is using 3G uplink. **Workaround:** Remove dns-domain below ap-system-profile, let internal DNS server resolve all, whether they are internal or external.

56875	A RAP cannot roll back from a secondary Cellular connection to the primary Ethernet when validuser ACL does not permit svc-natt.
	Workaround:
	Modify the validuser ACL by adding the following:
	`any host <public IP of controller> svc-natt permit`
	Also, in cases where a RAP is deployed in an MPLS network and the master is configured as FQDN, make sure to add the following to 'validuser' ACL:
	`any host <MPLS IP of controller> svc-natt permit`

53755	It may take longer for a RAP to dial a 4G call when the 4G signal strength is too low (lower than -70 dBm). **Workaround:** None.
55088	IP addresses for bridge and split-tunnel mode wireless clients do not appear in the ID page of the WebUI. **Workaround:** None.
53946	RAP 4G diagnostics features such as ping, nslookup, routetrace do not display properly on the LD page. **Workaround:** None.

Role and VLAN Derivation

Table 20 *Role and VLAN Derivation Known Issues and Limitations*

Bug ID	Description
55438	In some cases, the priority with in a user derivation rule set may not be followed when a DHCP packet matches several rules. Additionally, in this situation, every DHCP discover packet triggers the UDR. **Workaround:** None.
51691, 56746	DHCP Fingerprinting & Captive Portal cannot be used together. **Workaround:** None.
52733	MDAC is being used to identify smartphones by DHCP fingerprint. While matching fingerprints, the client (smartphone) will be put into another user role (e.g device-role). Device-role binds a vlan rather than default vlan of VAP. However `show user-table verbose` displays the wrong vlan. **Workaround:** None.

Table 20 *Role and VLAN Derivation Known Issues and Limitations (Continued)*

Bug ID	Description
54037	In some cases, the maximum number of supported stations (8k entries) is being reached on the controller because idle user entries are not being released. Once the controller reaches this stage, some of the new user entries are placed in VLAN1. **Workaround:** None.
55438	In a dot1x VAP deployment with user derivation involving multiple DHCP-option rules, a number of issues have been identified. After successful dot1x authentication and the client getting placed in the default dot1x role, the dhcp-option user derivation rules (UDRs) take effect. However, the order in which the rules are being checked is out of order and every DHCP discover/request triggers the UDR. **Workaround:** None.
55867	Clients doing Machine-auth will fall into the default VLAN if an external server is used for VLAN derivation. **Workaround:** None.
54037	In some cases, the maximum number of supported stations (8k entries) is being reached on the controller because idle user entries are not being released. Once the controller reaches this stage, some of the new user entries are placed in VLAN1. **Workaround:** None.

Security

Table 21 *Security Known Issues and Limitations*

Bug ID	Description
47868	The name option under the netdestination6 alias option is not available. **Workaround:** Provide the host/network IP address instead of a name.
50396	`Deny-inter-user-bridging` does not block the IPv6 traffic between the untrust clients on same VLAN. **Workaround:** None.
57618, 57632, 56912	In some cases, your controller's auth module might restart, resulting in momentary impact on your users. **Workaround:** None.
59925	The command `show user` incorrectly displays wired users coming from a port channel or GRE tunnel as wireless users. **Workaround:** None.
55629	RAPs are not able to associate with dot1x clients if the username entry in the local DB has more than 31 characters. **Workaround:** Change the username to have 31 characters or less.

Table 21 *Security Known Issues and Limitations (Continued)*

Bug ID	Description

56932	You cannot add a single netdestination for all multicast addresses using 240.0.0.0 as netmask. The CLI will return will read 240.0.0.0 as an invalid input. For example:
	`(config-test) #network 224.0.0.0 240.0.0.0`
	`                                          ^`
	`% Invalid input detected at '^' marker.`
	Workaround:
	None.

54413, 55132	The following error messages appear in the syslog while SNMP is trying to obtain that user's user entry: `snmp_handle_new_user_request:550: Failed to get SOS user entry for SNMP.` **Workaround:** None.
56588	Per-vlan aaa profiles do not work if station-table entry exists with the same MAC address as a client but with different aaa profile assigned when the client's traffic first hit the controller's untrusted port. **Workaround:** None.
55023	Split Tunnel ACLs are not hit when an AP-Group (Location) is mapped to the Firewall policy. When a user associates to the RAP (which is connected to a switch) and gets the correct role which has the Split-Tunnel policy that has the AP-Group mapped, if they attempt to ping the switch interface where the AP is terminating, the ping fails and the split-tunnel policy is not invoked. **Workaround:** None.
56599	An error message stating that termination must be enabled appears when a Internal DB Server is added to an existing Server Group even though termination is enabled with eap-peap and mschapv2. **Workaround:** None.
55003	After failing MAC authentication and falling into the Initial-Role of the AAA profile, if the user attempts to reconnect, MAC authentication will not happen again. **Workaround:** Make sure that initial-role is logon and logon-user-idle-timeout is set to zero, so that user-entry is deleted every time a client disconnects. And when client reconnects back MAC-AUTH is performed.
54224	With tunnel mode WPA2 SSIDs and CPSec enabled on those SSIDs, after times of very low traffic, the controller blocks users from associating. Additionally, WPA2 key exchange failures are seen in the syslog. **Workaround:** Rebooting the controller solves the issue temporarily, disabling CPSec solves it permanently.
54478	Wired Captive Portal authentication can be bypassed if the wired client moves to another VLAN. For example, if a client has successfully completed Captive Portal authentication on a particular VLAN and then moves to another VLAN on the same controller, the client is placed in the authenticated role. **Workaround:** None.
55898	The command `show user` does not display the correct information for captive portal users when those users are connected through an L3 gateway. **Workaround:** None.

Table 21 *Security Known Issues and Limitations (Continued)*

Bug ID	Description
56503	The username shown in the user table is the client's dot1x username instead of the captive portal username when the client disconnects and then reassociates. **Workaround:** None.
56782	Split-tunnel captive portal does not work in RAP behind RAP configuration. In tunnel mode, a client is able to reach the captive portal logon page and authenticate while, in split-tunnel mode, the client is unable to reach the logon page. **Workaround:** None.
57500	Custom captive portal login pages do not work when guest logon is enabled. The guest logon field is not displyed on the custom login page. This issue does not occur with the default Aruba login page. **Workaround:** Use the default captive portal page or use user logon.
55375	In rare cases, RAPs are not able to communicate with the controller. The RAP stays in the down state as seen in AP database on the controller. **Workaround:** Manually reboot the AP.

SNMP

Table 22 *SNMP Known Issues and Limitations*

Bug ID	Description
52186	The IfHCInOctets and ifHCOutOctets 64 bit counters rolls over at 32-bit boundary on M3 if the packet counters (octets) exceed 32 bits. **Workaround:** None.

TACACS

Table 23 *TACACS Known Issues and Limitations*

Bug ID	Description
56927	In some cases, management user might be unable to complete authentication against TACACS. The security logs reports that the authentication protocol was invalid. **Workaround:** None.

Voice

Table 24 *Voice Known Issues and Limitations*

Bug ID	Description
56506	SIP ALG might generate an additional CDR with invalid data when DELTS is received while terminating the call. Additionally, an invalid entry is added to the voice call quality table as well. This is a CLI issue and does not impact functionality. **Workaround:** None.
55058	Sometimes, the CLI output doesn't show the Lync clients getting tagged with the high priority ToS value. This is a CLI display issue and doesn't affect the functionality. It has been seen with Lync clients taking part in conference calls. This issue does not occur with peer-to-peer calls. **Workaround:** None.
56522	Voice call connectivity fails between Avaya phones and Descr failures are seen under `show ap debug system-status ap-name <ap-name>` and `show datapath frame ap-name <ap-name>` commands. **Workaround:** None.

VRRP

Table 25 *VRRP Known Issues and Limitations*

Bug ID	Description
55764	VRRP instances on a standby master controller are not placed in the backup state by default. This may create active instances on standby and the local will try to establish connection with standby master, which will fail. **Workaround:** None.

WebUI

Table 26 *WebUI Known Issues and Limitations*

Bug ID	Description
55040	On the WebUI, the modem U600 in 4G option is missing from the **Wireless > AP Installation > Provisioning Profile** preventing you from creating a provisioning profile for the U600 in 4G. **Workaround:** Either create a provisioning profile with 4G parameters (i.e. usb_type = "beceem-wimax") from the command line and apply that profile to the ap-group. OR, Choose the correct device type in the USB settings of the AP Installation page through WebUI.
52351, 54879	DHCP lease time cannot be configured in seconds through the WebUI. **Workaround:** If the DHCP lease time must be configured in seconds, configure it using the CLI. If the DHCP lease time is configured in seconds using the CLI, the WebUI will not display the configuration correctly.

Chapter 5

Upgrade Procedures

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

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

Topics in this chapter include:

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

Important Points to Remember

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

- Best practice recommends upgrading during a maintenance window. This will limit the troubleshooting variables.
- Please check the available memory and free disk space requirements prior to upgrading the controller using the WebUI (Install ArubaOS 6.1.2.8 using the WebUI) or using the CLI (Install ArubaOS 6.1.2.8 using the CLI).
- Verify your current ArubaOS version (execute the **show version, show image version,** or the **show switches** command).
- Verify which services you are using for each controller (for example, Employee Wireless, Guest Access, Remote AP, Wireless Voice).

- Verify the exact number of access points (APs) you have assigned to each controller.
- List which method each AP uses to discover each controller (DNS, DHCP Option, broadcast), and verify that those methods are operating as expected.
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- List the devices in your infrastructure that are used to provide your wireless users with connectivity (Core switches, radius servers, DHCP servers, firewall, for example).

Technical Upgrading Best Practices

- Know your topology. The most important path is the connectivity between your APs and their controllers. Connectivity issues will interfere with a successful upgrade. You must have the ability to test and make connectivity changes (routing, switching, DHCP, authentication) to ensure your traffic path is functioning.
- Avoid combining a software upgrade with other upgrades; this will limit your troubleshooting variables.
- Avoid making configuration changes during your upgrade.
- Notify your community, well in advance, of your intention to upgrade.
- Verify that all of your controllers are running the same software version in a master-local relationship. The same software version assures consistent behavior in a multi-controller environment.
- Use FTP to upload software images to the controller. FTP is much faster then TFTP and also offers more resilience over slower links.

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

- Always upgrade the non-boot partition first. If something happens during upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.

WIP Configuration Changes in Version 6.0

New configuration parameters were added in ArubaOS 6.0. When you upgrade from an ArubaOS version prior to 6.0 to ArubaOS 6.1, new parameters will automatically be added to their respective profiles and given their default value.

If the default value of an existing parameter changed in versions prior to ArubaOS 6.0, profiles using the default value will automatically be changed to use the new default value. If your configuration uses a non-default value prior to upgrade, the value will not be modified during the upgrade process. The following default values were changed:

Detect AP Impersonation—changed from **True** to **False**

Detect Adhoc Network— changed from **True** to **False**

Detect Wireless Bridge—changed from **True** to **False**

Detect 40MHz Intol—changed from **True** to **False**

Detect Active Greenfield mode—changed from **True** to **False**

WIP Predefined Profiles

Except for predefined profiles IDS Rate Thresholds and IDS Signature, all IDS predefined profiles were deprecated in ArubaOS 6.0. Mapping the deprecated profiles are handled as follows:

- If a predefined profile is referenced by default from another profile, the reference will point to the new default instance of the profile
- If a predefined profile is referenced explicitly (that is, you changed from the default value so that it points to a predefined profile), after the upgrade the reference will point to a profile which is an editable clone of the predefined profile. That profile is named similarly to the predefined profile, except the word “transitional” is inserted after “ids-“

Wireless Containment Parameter

The wireless-containment parameter in the ids-general-profile went from an enabled/disabled knob to an enumeration (none, deauth-only, tarpit-non-valid-sta, tartip-all-sta).

- If the parameter was set to *enabled* (its default value), the upgrade will render the value as *deauth-only* (the new default value)
- If the parameter was set to *disabled*, the upgrade will render the value as *none*

Signature Matching profile Default Instance

The default instance of the signature matching profile in ArubaOS contain references to 2 predefined signatures: Deauth-Broadcast and Disassoc-Broadcast (a new signature in 6.0). The default instance of this profile was empty prior to 6.0.

- If the profile was empty, the upgrade will render the profile with both predefined signatures.
- If the profile was not empty, the upgrade will add references to the 2 predefined signatures, if they are not already there.

WIP Logging Changes

In ArubaOS 6.0, all WIP logs related to intrusion detection and protection are in the ‘security’ logging category. Previously, most WIP logs were generated under the Wireless Logging category. Many of the logs that were previously generated at the Error level have been moved to the Warning level. In the security logging category, two new subcategories are added:

- The ‘ids’ subcategory contains ‘correlated’ WIP logs.
- The ‘ids-ap’ subcategory contains WIP logs generated by the APs (uncorrelated).

Both of these new WIP logging subcategories: ‘ids’ and ‘ids-ap’ are enabled at the Warning level by the upgrade. However, by default, AP logging of WIP events is disabled and correlation of WIP logs is enabled.

Basic Upgrade Sequence

Testing your clients and ensuring performance and connectivity is probably the most time-consuming part of the upgrade. Best practices recommends that you enlist users in different locations to assist with the validation before you begin the upgrade. The list below is an overview of the upgrade and validation procedures.

If you manage your controllers via the AirWave Wireless Management Suite, the AirWave upgrade process automates most of these steps.

1. Upload the same version of the new software image onto all controllers.
2. Reboot all controllers simultaneously.
3. Execute the **ping -t** command to verify all your controllers are up after the reboot.
4. Open a Secure Shell session (SSH) on your Master Controller.
5. Execute the **show ap database** command to determine if your APs are up and ready to accept clients.

6. Execute the **show ap active** to view the up and running APs.
7. Cycle between step 5 and step 6 until a sufficient amount of APs are confirmed up and running.

   The **show ap database** command displays all of the APs, up or down. If some access points are down, execute the **show datapath session table** <*access point ip address*> command and verify traffic is passing. If not, attempt to ping them. If they still do not respond, execute a **show ap database long** command to view the wired mac address of the AP; locate it in your infrastructure.
8. Verify that the number of access points and clients are what you would expect.
9. Test a different type of client for each access method (802.1x, VPN, Remote AP, Captive Portal, Voice) and in different locations when possible.

Managing Flash Memory

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

- Do not exceed the size of the flash file system. For example, loading multiple large building JPEGs for RF Plan or VisualRF Plan can consume flash space quickly.

  Warning messages alert you that the file system is running out of space if there is a write attempt to flash and 5 Mbytes or less of space remains.

Other tasks which are sensitive to insufficient flash file system space include:

- DHCP lease and renew information is stored in flash. If the file system is full, DHCP addresses can not be distributed or renewed.
- If a controller encounters a problem and it needs to write a log file, it will not be able to do so if the file system is full and critical troubleshooting information will be lost

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

Before you upgrade

You should ensure the following before installing a new image on the controller:

- Make sure you have at least 85 MB of free compact flash space (**show storage** command).
- Run the **tar crash** command to ensure there are no “process died” files clogging up memory and FTP/TFTP the files to another storage device.
- Remove all unnecessary saved files from flash (**delete filename** command).

Backing up Critical Data

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

- Configuration data
- WMS database
- Local user database
- Licensing database
- Floor plan JPEGs

- Customer captive portal pages
- Customer x.509 certificates

Backup and Restore Compact Flash in the WebUI

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

1. Navigate to the **Maintenance > File > Backup Flash** page.
2. Click **Create Backup** to back up the contents of the Compact Flash file system to the file flashbackup.tar.gz.
3. Click **Copy Backup** to copy the file to an external server.

   You can later copy the backup file from the external server to the Compact Flash file system by navigating to the **Maintenance > File > Copy Files** page.
4. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page. Click **Restore**.

Backup and Restore Compact Flash in the CLI

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

1. Enter **enable** mode in the CLI on the controller. Use the **backup** command to back up the contents of the Compact Flash file system to the file flashbackup.tar.gz:

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

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

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

   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   ```
3. Use the **restore** command to untar and extract the *flashbackup.tar.gz* file to the Compact Flash file system:

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

Licensing Change History and Mapping

License consolidation and even renaming of licenses occur over time. The following changes and/or consolidations were made to the ArubaOS licensing.

ArubaOS 6.1

- The VIA feature now requires a PEFV license (Policy Enforcement Firewall Virtual Private Network).
- The Walled Garden feature requires the PEFNG or PEFV license.

- Advanced Cryptography License (ACR) is introduced—the ACR license is required for the Suite B Cryptography in IPsec and 802.11 modes. License enforcement behavior controls the total number of concurrent connections (IPsec or 802.11) using Suite B Cryptography.

ACR Interaction

- On a platform that supports 2048 IPsec tunnels, the maximum number of Suite B IPsec tunnels supported is 2048, even if a larger capacity license is installed.
- An evaluation ACR license is available (EVL-ACR-8192). You can install the ACR evaluation license with a higher capacity than the platform maximum.
- On a platform that supports 2048 IPsec tunnels, with a LIC-ACR-512 installed, only 512 IPsec tunnels can be terminated using Suite B encryption. An additional 1536 IPsec tunnels, using non-Suite B modes (e.g. AES-CBC), can still be supported.
- On a platform with LIC-ACR-512 installed, a mixture of IPsec and 802.11i Suite B connections can be supported. The combined number of these sessions may not exceed 512.
- A single client using both 802.11i Suite B and IPsec Suite B simultaneously will consume two ACR licenses.

ArubaOS 6.0

- WIP license is changed to RFprotect and includes the WIP and Spectrum Analysis features.

ArubaOS 5.0

Figure 1 is an up-to-date illustration of the consolidated licenses effective with this release.

- MAP was merged into base ArubaOS
- VPN was merged into base ArubaOS
- RAP was merged into AP license
- PEF (user basis) was converted to PEFNG (AP basis) with ArubaOS 5.0

ArubaOS 3.4.1

- VOC was merged into PEF. This merge happened with ArubaOS 3.4.1
- IMP was merged into base ArubaOS

ArubaOS 3.4.0

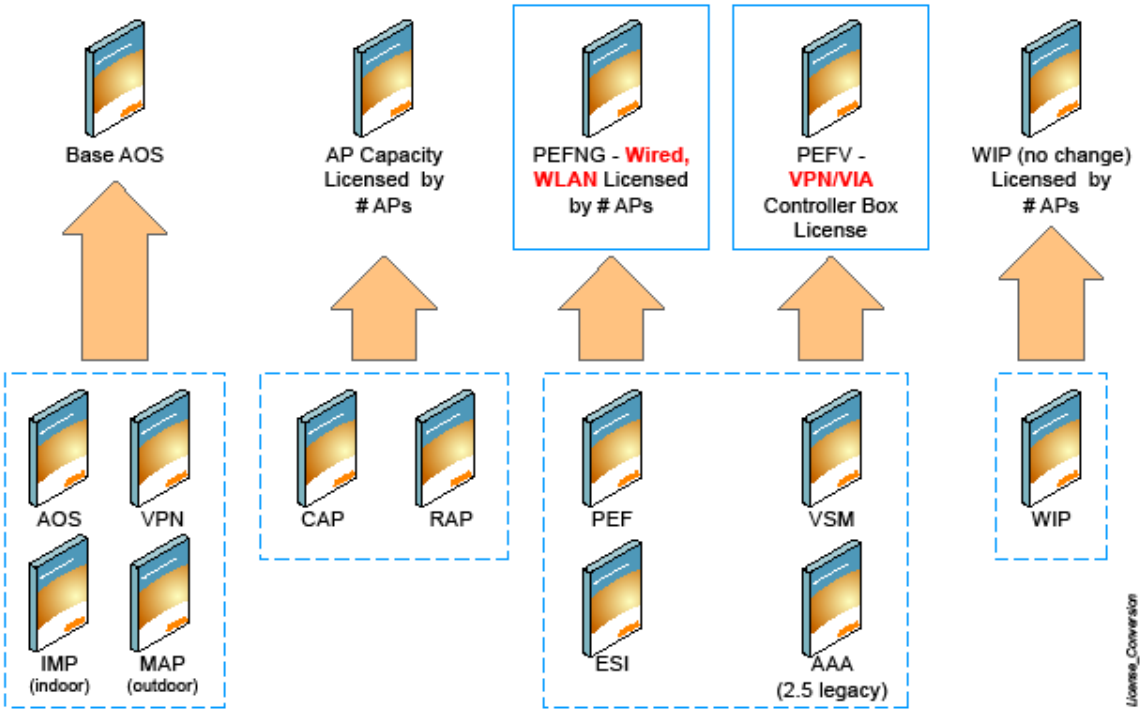
- ESI was merged into PEF

ArubaOS Legacy and End-of-Life

- AAA was merged into ESI with the release of ArubaOS 2.5.3.
- CIM is End-of-life

Releases older than ArubaOS 2.5.4 have been End-of-Lifed.

Figure 1 *Licensing Consolidation ArubaOS 5.0*



Upgrading from 5.0.x to 6.1

CAUTION

If you are running ArubaOS 5.0.3.1 (or later) you can directly upgrade to ArubaOS 6.1.2.8. However, upgrading from an ArubaOS version earlier than 5.0.3.1 requires an upgrade hop. You must first upgrade to the latest ArubaOS 5.0.4.x build before upgrading to ArubaOS 6.1.2.8.

If you are upgrading from 5.0.x to 6.1, your control plane security settings will be retained during the upgrade. If you had enabled the control plane security feature in ArubaOS 5.0, the feature will still be enabled after you upgrade to ArubaOS 6.1. If you to downgrade to ArubaOS 5.0, you will not need to disable control plane security

Upgrading from 3.x to 6.1.x

If you are running ArubaOS 3.4.4.1 or a later version in the 3.4.4.x code stream, you can directly upgrade to ArubaOS 6.1.2.8. However, upgrading from a 3.x ArubaOS version earlier than 3.4.4.1 requires an upgrade hop. You must first upgrade to the latest ArubaOS 3.4.4.x build before upgrading to ArubaOS 6.1.2.8.

NOTE

All versions assume that you have upgraded to the most recent version as posted on the Aruba download site. For instance, 3.3.x assumes you have upgraded to the most recent version of 3.3.x.x.

Upgrading from RN-3.x.x to 6.1.x

If you are upgrading from a release older than RN-3.x.x.x release, you must upgrade to the most recent version of ArubaOS 5.0.4.x build that is available on the support site before upgrading to ArubaOS 6.1.2.8.

NOTE

Once you have completed the upgrade to the latest version of ArubaOS 5.0.4.x, then follow the steps in "Install ArubaOS 6.1.2.8 using the WebUI" on page 67 to complete your last "upgrade hop".

Caveat

Should you need to downgrade from ArubaOS 6.1, you can only downgrade to version RN-3.1.4 or higher.

Upgrading from 6.0.x to 6.1.x

CAUTION

If you are running ArubaOS 6.0.1.0 (or later) you can directly upgrade to ArubaOS 6.1.2.8. However, upgrading from an ArubaOS version earlier than 6.0.1.0 requires an upgrade hop. You must first upgrade to the latest ArubaOS 6.0.1.x build before upgrading to ArubaOS 6.1.2.8.Read all the following information before you upgrade to ArubaOS 6.1.2.8.

Read all the following information before you upgrade to ArubaOS 6.1.2.8.

- "Caveats" on page 66
- "Load New Licenses" on page 66
- "Save your Configuration" on page 66
- "Install ArubaOS 6.1.2.8 using the WebUI" on page 67

Caveats

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

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

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

Load New Licenses

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

Software licenses in ArubaOS 5.0 were consolidated and in some instances license names and modules were renamed to more accurately represent the modules supported by the licenses (see Figure 1).

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

Save your Configuration

Before upgrading, save your configuration and back up your controllers data files (see "Managing Flash Memory" on page 62). Saving your configuration saves the **admin** and **enable** passwords in the proper format.

Saving the Configuration in the WebUI

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

Saving the Configuration in the CLI

Enter the following command in enable or config mode:

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

Install ArubaOS 6.1.2.8 using the WebUI

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

When upgrading the software in a multi-controller network (one that uses two or more Aruba controllers), special care must be taken to upgrade all the controllers in the network and to upgrade them in the proper sequence.(See “Upgrading in a Multi-Controller Network” on page 73.)

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

You can directly upgrade to ArubaOS 6.1.2.8 if you are running one of the following 6.0.x releases: [6.0.1.0, 6.0.1.2, 6.0.1.2, 6.0.1.3, or 6.0.1.x]. However, upgrading from a version of ArubaOS 6.0.0.0 or 6.0.0.1 requires an upgrade hop. You must first upgrade to the latest ArubaOS 6.0.1.x build before upgrading to ArubaOS 6.1.2.8. Read all the following information before you upgrade to ArubaOS 6.1.2.8.

You can directly upgrade to ArubaOS 6.1.2.8 if you are running one of the following 5.0.x releases: [5.0.3.1, 5.0.3.2, 5.0.3.3, or 5.0.4.x]. However, upgrading from an ArubaOS version earlier than 5.0.3.1 requires an upgrade hop. You must first upgrade to the latest ArubaOS 5.0.4.x build before upgrading to ArubaOS 6.1.2.8. Read all the following information before you upgrade to ArubaOS 6.1.2.8.

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

1. If you are running an ArubaOS 3.x.x.x version earlier than ArubaOS 3.4.4.1, you must download the latest version of ArubaOS 3.4.4.x. Then proceed to Step 4.
2. If you are running:
   a. Any ArubaOS RN-3.x.x version, or
   b. ArubaOS 5.0.x.x version earlier than ArubaOS 5.0.3.1, you must download the latest version of ArubaOS 5.0.4.x. Then proceed to Step 4
3. If you are running ArubaOS versions 6.0.0.0 or 6.0.0.1, you must download the latest version of ArubaOS 6.0.1.x.
4. Download ArubaOS 6.1.2.8 from the customer support site.
5. Upload the new software image(s) to a PC or workstation on your network.
6. Log in to the WebUI from the PC or workstation.
7. Navigate to the **Maintenance>Controller>Image Management** page. Select the **Upload Local File** option, then click **Browse** to navigate to the image file (saved in Step 1 - 4) on your PC or workstation.

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

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

   OR

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

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

   OR

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

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

   OR

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

   - 3.4.4.1 or the latest 3.4.x.x
   - 5.0.3.1 or the latest 5.0.x.x—Review "Upgrading With RAP-5s and RAP-5WNs" on page 69 before proceeding further
   - 6.0.1.0 or the latest 6.0.x.x
   - 6.1.2.0 or the latest 6.1.2.x

   a. Select the ArubaOS 6.1.2.8 image file downloaded in Step 4.
   a. Follow the procedure in Steps 8 - 12.
8. Make sure you select the non-boot **partition to upgrade**. To see the current boot and non-boot partitions, navigate to the **Maintenance>Controller>Boot Parameters** page.
9. Select **Yes** for **Reboot Controller After Upgrade**.
10. Click **Upgrade**.
11. When the software image is uploaded to the controller, a popup appears. Click **OK** in the popup window. The reboot process starts automatically within a few seconds (unless you cancel it).

12. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring>Controller>Controller Summary** page to verify the upgrade, including country code. The **Country** field displays the country code configured on the controller.


NOTE

If the ArubaOS version on the Controller Summary page shows ArubaOS 6.1.2.8, the upgrade is completed. Proceed with Step 13 to verify that all the APs are up and active and that clients are able to connect to the APs and can access resources successfully.

13. Execute the **ping -t** command to verify all your controllers are up after the reboot.
14. Open a Secure Shell session (SSH) on your Master Controller.
15. Execute the **show ap database** command to determine if your APs are up and ready to accept clients.
16. Execute the **show ap active** to view the up and running APs.
17. Cycle between step 15 and step 16 until a sufficient amount of APs are confirmed up and running.

    The **show ap database** command displays all of the APs, up or down. If some access points are down, execute the **show datapath session table** <*access point ip address*> command and verify traffic is passing. If not, attempt to ping them. If they still do not respond, execute a **show ap database long** command to view the wired mac address of the AP; locate it in your infrastructure.
18. Verify that the number of access points and clients are what you would expected.
19. Test a different type of client for each access method (802.1x, VPN, Remote AP, Captive Portal, Voice) and in different locations when possible.
20. 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 62 for information on creating a backup.
21. Repeat steps 7 (option 4) through 20 to complete the upgrade to ArubaOS 6.1.2.8.

Upgrading With RAP-5s and RAP-5WNs

If you have completed the first upgrade hop to the latest ArubaOS 5.0.4.x version, and your WLAN includes RAP-5/RAP-5WN, do not proceed until completing the following process. Once complete, proceed to step 21 on page 69.

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

   ```
   show ap image version
   ```
2. If the Flash (Provisioning/Backup) Image Version String shows the letters "rn" for example as 3.3.2.11-rn-3.0, note down those AP names and IP addresses.
3. For each of the RAP-5/RAP-5WN noted in the step-ii, upgrade the provisioning image on the backup flash partition by executing the following command:

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

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

   ```
   show ap image version
   ```

   The Flash (Provisioning/Backup) Image Version String should now show for example 5.0.3.3 and not contain the letters "rn".
5. If you omit the above process or fail to complete the Flash (Provisioning/Backup) Image upgrade to 5.0.4.x and the RAP-5/RAP-5WN was reset to factory defaults, the RAP will not be able to connect to the controller running 6.1.2.x and upgrade its production software image.

Install ArubaOS 6.1.2.8 using the CLI

CAUTION

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

CAUTION

You can directly upgrade to ArubaOS 6.1.2.8 if you are running one of the following 6.0.x releases: [6.0.1.0, 6.0.1.2, 6.0.1.2, 6.0.1.3, or 6.0.1.x]. However, upgrading from a version of ArubaOS 6.0.0.0 or 6.0.0.1 requires an upgrade hop. You must first upgrade to the latest ArubaOS 6.0.1.x build before upgrading to ArubaOS 6.1.2.8. Read all the following information before you upgrade to ArubaOS 6.1.2.8.

CAUTION

You can directly upgrade to ArubaOS 6.1.2.8 if you are running one of the following 5.0.x releases: [5.0.3.1, 5.0.3.2, 5.0.3.3, or 5.0.4.x]. However, upgrading from any ArubaOS RN-3.x.x version or ArubaOS 5.0.x.x version earlier than 5.0.3.1 requires an upgrade hop. You must first upgrade to the latest ArubaOS 5.0.4.x build before upgrading to ArubaOS 6.1.2.8. Read all the following information before you upgrade to ArubaOS 6.1.2.8.

CAUTION

You can directly upgrade to ArubaOS 6.1.2.8 if you are running one of the following 3.4.4.x releases: [3.4.4.1, 3.4.4.2, 3.4.4.3, or a later 3.4.x.x]. However, upgrading from an ArubaOS 3.x.x.x version earlier than 3.4.4.1 requires an upgrade hop. You must first upgrade to the latest ArubaOS 3.4.x.x build before upgrading to ArubaOS 6.1.2.8. Read all the following information before you upgrade to ArubaOS 6.1.2.8.

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

1. There are 4 upgrade paths to ArubaOS 6.1.2.8. Depending on the current ArubaOS version running on the Aruba controller(s), you will have to perform an upgrade hop as explained in options 1 to 4.

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

a. Download the latest version of ArubaOS 3.4.4.x

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

OR

Option 2: If upgrading from

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

a. Download the latest version of ArubaOS 5.0.4.x

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

NOTE

Review “Upgrading With RAP-5s and RAP-5WNs” on page 69 before proceeding to upgrade to ArubaOS 6.1.2.8

OR

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

a. Download the latest ArubaOS 6.0.1.x version

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

c. Follow the procedure in Steps 8 - 12.

OR

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

- 3.4.4.1 or the latest 3.4.x.x
- 5.0.3.1 or the latest 5.0.x.x —Review "Upgrading With RAP-5s and RAP-5WNs" on page 69 before proceeding further
- 6.0.1.0 or the latest 6.0.1.x
- 6.1.2.0 or the latest 6.1.2.1

Proceed with step 2

2. Download ArubaOS 6.1.2.8 from the customer support site.
3. From a laptop/desktop, execute the **ping -t** command to verify all your controllers are up after the reboot following the first upgrade hop in Step 1.
4. Open a Secure Shell session (SSH) on your Master (and Local) Controller(s).
5. Execute the **show ap database** command to determine the state of all your APs.
6. Execute the **show ap active** command to view the already up and running APs ready to accept clients.
7. Cycle between step 5 and step 6 until a sufficient amount of APs are confirmed to be up and running. The **show ap database** command displays all of the APs, up or down. If some access points are down, execute the **show datapath session table <access point ip address>** command and verify traffic is passing. If not, attempt to ping them. If they still do not respond, execute a **show ap database long** command to view the wired mac address of the AP; locate it in your infrastructure.
8. Verify that the number of access points and clients are what you would expect.
9. Test a different type of client for each access method (802.1x, VPN, Remote AP, Captive Portal, Voice) and in different locations when possible.
10. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See "Backing up Critical Data" on page 62 for information on creating a backup.
11. Use the following command to check the current running ArubaOS version:

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

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

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

```
256M bytes of Supervisor Card System flash (model=NAND 256MB)
```

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

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

    or

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

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

    ```
    (hostname) #show image version
    ---------------------------------
    Partition               : 0:0 (/dev/mtdblock9) **Default boot**
    Software Version        : ArubaOS 5.0.3.3
    Build number            : 28008
    Label                   : 28008
    Built on                : Thu Apr 21 12:09:15 PDT 2011
    ---------------------------------
    Partition               : 0:1 (/dev/mtdblock10)
    Software Version        : ArubaOS 5.0.3.0
    Build number            : 26207
    Label                   : 26207
    Built on                : Tue Nov 30 08:35:45 PST 2010
    ```

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

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

    or

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

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

    ```
    (hostname)# show image version
    ---------------------------------
    Partition               : 0:0 (/dev/mtdblock9)
    Software Version        : ArubaOS 5.0.3.3
    Build number            : 28008
    Label                   : 28008
    Built on                : Thu Apr 21 12:09:15 PDT 2011
    ---------------------------------
    Partition               : 0:1 (/dev/mtdblock10) **Default boot**
    Software Version        : ArubaOS 6.1.2.8
    Build number            : 31653
    Label                   : 31653
    Built on                : Fri Dec 29 00:03:14 PDT 2011
    ```

17. Reboot the controller:

    ```
    (hostname)# reload
    ```

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

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

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

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

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

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 62.


NOTE

For proper operation, all controllers in the network must be upgraded with the same version of ArubaOS software. For redundant (VRRP) environments, the controllers should be the same model.

To upgrade an existing multi-controller system to ArubaOS 6.1.2.8:

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.

Pre-shared Key for Inter-Controller Communication

A pre-shared key (PSK) is used to create IPSec tunnels between a master and backup master controllers and between master and local controllers. These inter-controller IPSec tunnels carry management traffic such as mobility, configuration, and master-local information.


NOTE

An inter-controller IPSec tunnel can be used to route data between networks attached to the controllers. To route traffic, configure a static route on each controller specifying the destination network and the name of the IPSec tunnel.

There is a default PSK to allow inter-controller communications, however, for security you need to configure a a unique PSK for each controller pair. You can use either the WebUI or CLI to configure a 6-64 character PSK on master and local controllers.

Do not use the default global PSK on a master or standalone controller. If you have a multi-controller network then configure the local controllers to match the new IPSec PSK key on the master controller. Leaving the PSK set to the default value exposes the IPSec channel to serious risk, therefore you should always configure a unique PSK for each controller pair.

Downgrading after an Upgrade

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

If you upgraded from 3.3.x to 5.0, the upgrade script encrypts the internal database. Any new entries that were created in ArubaOS 6.1.2.8 will be lost after downgrade (this warning does not apply to upgrades from 3.4.x to 6.1),

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

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

If you do not use a previously-saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from ArubaOS 6.1.2.8 to 5.0.3.2, due to changes made to WIPS in 6.x, the new predefined IDS profile assigned to an AP group will not be recognized by the older version of ArubaOS. This unrecognized profile will prevent associated APs from coming and display a profile error.

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

3. Set the controller to boot from the system partition that contains the previously running ArubaOS image.

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

After downgrading the software on the controller:

- Restore pre-6.1 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.1.2.8 flash backup file.
- You do not need to re-import the WMS database or RF Plan data. However, if you have added changes to RF Plan in ArubaOS 6.1.2.8, the changes will not appear in RF Plan in the downgraded ArubaOS version.
- If you installed any certificates while running ArubaOS 6.1.2.8, you need to reinstall the certificates in the downgraded ArubaOS version.

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

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

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

Downgrading using the WebUI

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

Downgrading using the CLI

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

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

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

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

3. Execute the **show image version** command to view the partition on which your previous software image is stored.

   In the following example, partition 0, the backup system partition, contains the backup release 5.0.3.3. Partition 1, the default boot partition, contains the ArubaOS 6.1.2.8 image:

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


NOTE

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

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

```
# boot system partition 0
```

5. Reboot the controller:

```
# reload
```

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

```
# show image version
```

Controller Migration

This section outlines the steps involved in migrating from an Aruba PPC controller environment to MIPS controller environment. These steps takes into consideration the common Aruba WLAN controller environment. You must have an operational PPC controller in the environment when migrating to a new controller. The controllers are classified as:

- MIPS Controllers—M3, 3000 Series, 600 Series
- PPC Controllers—200, 800, 2400, 5000 and SC1/SC2


NOTE

Use this procedure to upgrade from one Aruba controller model to another. Take care to ensure that the new controller has equal or greater capacity than the controller you are replacing and verify that your new controller supports the ArubaOS version you are migrating to.

Migration instructions include:

- "Single Controller Environment" on page 76
- "Multiple Master Controller Environment" on page 77
- "Master/Local Controller Environment" on page 77

Single Controller Environment

A single controller environment is one active controller, or one master controller that may have standby master controller that backs up the master controller.

- Replacing the standby controller—Does not require downtime
- Replacing the master controller—Requires downtime

Multiple Master Controller Environment

An all master environment is considered an extension of the single master controller. You can back up the master controllers with a standby controller. In an all master controller deployment, each master controller is migrated as if it were in a standalone single controller environment.

For every master-standby controller pair

- Replacing the standby controller—Does not require downtime
- Replacing the master controller—Requires downtime

Master/Local Controller Environment

In a master/local environment, replace the master controller first and then replace the local controllers.

- Replacing the local standbys (when present)
- Replacing local controllers—one controller at a time

Before You Start

You must have:

- Administrative access to the controller via the network
- Administrative access to the controller via the controller's serial port
- Pre-configured FTP/TFTP server that can be reached from the controller
- Aruba serial cable
- The ArubaOS version (same as the rest of the network)

Basic Migration Steps

1. Ensure that the ArubaOS version on the newer controllers match the ArubaOS version on the rest of the controllers in your network.
2. Backup the old controller data and move the backup files to a safe place that is easily accessible through FTP/TFTP.
3. Physically swap the hardware (for example, mounting, cabling, power).
4. Initialize the new controller with the correct license.
5. Install the backed up data onto the new controller.
6. Test the new setup.

Before You Call Technical Support

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

1. Provide a detailed network topology (including all the devices in the network between the user and the Aruba controller with IP addresses and Interface numbers if possible).
2. Provide the controller logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
3. Provide the syslog file of the controller at the time of the problem.

   Aruba strongly recommends that you consider adding a syslog server if you do not already have one to capture from the controller.

4. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have:
   - an outage in a network that worked in the past.
   - a network configuration that has never worked.
   - a brand new installation.
5. Let the support person know if there are any recent changes in your network (external to the Aruba controller) or any recent changes to your controller and/or AP configuration.
6. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) when the problem first occurred.
8. If the problem is reproducible, list the exact steps taken to recreate the problem.
9. Provide any wired or wireless sniffer traces taken during the time of the problem.
10. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless NIC make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
11. Provide the controller site access information, if possible.