ArubaOS 6.5.1.3

Release Notes

aruba

a Hewlett Packard
Enterprise company

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

ArubaOS 6.5.1.3 is a software patch release that includes new features and enhancements introduced in this release, and fixes to issues identified in previous releases.

See the Upgrade Procedure on page 23 for instructions on how to upgrade your controller to this release.

Chapter Overview

- New Features provides a description of features and enhancements introduced in this release.
- Regulatory Updates describes the regulatory updates in this release.
- Resolved Issues describes the issues resolved in this release.
- Known Issues describes the known and outstanding issues identified in this release.
- Upgrade Procedure describes the procedures for upgrading a controller to this release.
- Acronyms and Abbreviations lists the acronyms and abbreviations used in the document.

For information regarding prior releases, refer to the corresponding Release Notes on support.arubanetworks.com.

Supported Browsers

The following browsers are officially supported for use with ArubaOS 6.5.1.3 WebUI:

- Microsoft Internet Explorer 10.x and 11 on Windows 7 and Windows 8
- Mozilla Firefox 23 or later on Windows Vista, Windows 7, and Mac OS
- Apple Safari 5.1.7 or later on Mac OS
- Chrome 51.0.2704.103 m (64-bit)
- Microsoft Edge 25.10586.0.0 and Microsoft Edge HTML 13.10586

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	hpe.com/networking/support
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

This chapter describes the new features, enhancements, and hardware introduced in ArubaOS 6.5.1.3. For more information about these features, refer to the *ArubaOS 6.5.x User Guide*.

New Command

The following new command is introduced in ArubaOS 6.5.1.3.

show iap subnet

```
show iap subnet <subnet-name>
```

Description

This command troubleshoots IAP-VPN distributed L3 Branch ID (BID) allocation-related issues. This command provides an increased granularity in searching the BID provided by the controller.

Syntax

Parameter	Description
`<subnet-name>`	Specific subnet name of the BID.

Example

The following example displays the BID subnet details. To know the subnet name, execute the **show iap table long** command.

```
(host) #show iap subnet 192.0.2.1-192.0.2.254,5

Max BID : 32
BID Bitmap :
   1 : 03000000
   2 : 00000000
Dead Branch List :
   1 : 4d852f8d01a4dab1425dc14cc2e287cdc6d216b698bab1bea3 BID:6
   2 : 7ba7671101a5c06850061b7330599d5a2a7d5d69b7fb865c59 BID:7
Allocated BID Branch List :
   1 : 4d852f8d01a4dab1425dc14cc2e287cdc6d216b698bab1bea3 BID:6
```

```
2 : 7ba7671101a5c06850061b7330599d5a2a7d5d69b7fb865c59 BID:7
```

The output of this command includes the following fields.

Field	Description
BID Bitmap	Internal data structure to allocate BID to branches.
Dead Branch List	List of branches that are inactive at a time.
Allocated BID Branch List	List of branches that have valid BIDs.

Modified Commands

The following commands are modified in ArubaOS 6.5.1.3.

interface vlan

```
interface vlan <id>
   filter-broadcast-on-helper
```

The **filter-broadcast-on-helper** parameter is introduced.

Parameter	Description	Default
filter-broadcast-on-helper	Filter DHCP discover broadcast if the DHCP server relay agent is configured.	disabled

Usage Guideline

When the **filter-broadcast-on-helper** parameter is enabled and the DHCP server relay agent is configured on the VLAN interface, client DHCP broadcast packets are not flooded, but sent as unicast packets to the configured DHCP server relay agent. When this parameter is disabled, client DHCP broadcast packets are flooded to the trusted ports, and sent as unicast packets to the configured DHCP server relay agent. This parameter is disabled by default.

Example

The following command configures a DHCP server relay agent and filters DHCP discover broadcast packets on VLAN ID 1.

```
(host) (config) #interface vlan 1
(host) (config) #ip helper-address 192.0.2.1
(host) (config-subif)#filter-broadcast-on-helper
```

packet-capture datapath

```
packet-capture datapath
   mac <mac-address> {all | decrypted | encrypted}
```

The **wifi-client** parameter is replaced with the **mac** parameter.

Parameter	Description
`mac <mac-address>`	MAC address of the wired or wireless client.

Example

```
(host) #packet-capture datapath mac 9c:1c:12:8a:b4:00 all
```

Chapter 3
Regulatory Updates

This chapter describes the regulatory updates in ArubaOS 6.5.1.3.

Contact your local Aruba sales representative about device availability and support for your country.

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the controller Command Line Interface (CLI) and execute the **show ap allowed-channels country-code <country-code> ap-type <ap-model>** command.

The following default Downloadable Regulatory Table (DRT) version is part of ArubaOS 6.5.1.3:

- DRT-1.0_58258

For a complete list of countries certified with different AP models, refer to the DRT Release Notes at support.arubanetworks.com.

The FCC has changed the rules for operation in all of the 5 GHz bands. For more information, refer to the *FCC DFS Regulatory Change Impact and Resolution Plan - Support Advisory* available in Support Advisories.

The ntp-4.2.8p9 security release is integrated in ArubaOS 6.5.1.3. In addition, the following issues are resolved in this release.

Table 3: *Resolved Issues in ArubaOS 6.5.1.3*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
140113 140886 144529 151560	**Symptom:** The user-table of the controller displayed an incorrect user-role for a wireless client connected to an Instant AP in an IAP-VPN deployment. This issue is resolved by allowing the client to retain its existing role as it moves from one SSID to the other. **Scenario:** This issue occurred because the controller failed to inherit the role from the previous user entry and derived an incorrect or new role for the client when it switched from one SSID to another across VLANs.	Remote AP	All platforms	ArubaOS 6.4.4.6	ArubaOS 6.5.1.3
144302 153465	**Symptom:** An AP stopped responding and rebooted. The log file for the event listed the reason as **Reboot caused by kernel panic: Out of memory**. Improvements in the wireless driver of the AP resolved the issue. **Scenario:** This issue occurred when clients roamed in an L2 network, resulting in a gradual decrease in the memory of the AP. This issue was observed in 320 Series access points running ArubaOS 6.4.4.10 or later versions.	AP-Platform	320 Series access points	ArubaOS 6.4.4.10	ArubaOS 6.5.1.3
147291 147922	**Symptom:** An AP generated the following error message: **An internal system error has occurred at file sapd_msg.c function sapd_papi_snd_cb line 1579 error Message to 127.0.0.1:RF Client failed: err Connection timed out msgcode 1003 arg 0x784184**. The fix ensures that the AP stops generating this error message. **Scenario:** The error messages did not have any impact on the network. This issue was observed in 90 Series access points running ArubaOS 6.5.1.0 or later versions.	AP-Platform	90 Series access points	ArubaOS 6.5.1.0	ArubaOS 6.5.1.3

Table 3: *Resolved Issues in ArubaOS 6.5.1.3*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
148249 148251 148252 148263	**Symptom:** A controller was inaccessible after it was rebooted by unplugging the power multiple times. The fix ensures that the controller is accessible even after a hard reboot. **Scenario:** This issue occurred when a controller was hard rebooted multiple times immediately after saving the configuration. This issue was limited to 7005 controller model running ArubaOS 6.4.3.9-FIPS or later versions.	Controller-Platform	7005 controllers	ArubaOS 6.4.3.9-FIPS	ArubaOS 6.5.1.3
148909 156395	**Symptom:** A local controller stopped responding resulting in user traffic disruption. This issue is resolved by fixing the datapath session leaks that were observed in the local controller. **Scenario:** This issue occurred when a large amount of traffic was generated and Web Content Classification (WebCC) and Deep Packet Inspection (DPI) were enabled on the controller. This resulted in datapath session leaks. This issue was observed in a master-local deployment with 7200 Series controllers running ArubaOS 6.4.4.9 or later versions.	Controller-Datapath	7200 Series controllers	ArubaOS 6.4.4.9	ArubaOS 6.5.1.3
148995	**Symptom:** The controller incorrectly reported multiple debug kernel log messages on the syslog server. The issue is resolved by disabling the kernel debug messages. **Scenario:** These messages were generated as part of a debug code. These messages had no impact on the network. This issue was observed in controllers running ArubaOS 6.4.4.9 or later versions.	AP-Platform	All platforms	ArubaOS 6.4.4.9	ArubaOS 6.5.1.3
149640	**Symptom:** An AP stopped responding and rebooted. The log file for the event listed the reason as **kernel panic: Fatal exception in interrupt**. Improvements in the wireless driver of the AP resolved the issue. **Scenario:** This issue occurred due to a corruption in the memory of the AP. This issue was observed in AP-305 access points running ArubaOS 6.5.1.0 or later versions.	AP-Wireless	AP-305 access points	ArubaOS 6.5.1.0	ArubaOS 6.5.1.3

Table 3: *Resolved Issues in ArubaOS 6.5.1.3*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
149744	**Symptom:** When a user entered an incorrect credential on the external captive portal login page, an **internal server error** message was displayed on the Web browser instead of the **authentication failed** message. The fix ensures that the correct message is displayed on the Web browser when a user provides an incorrect credential. **Scenario:** This issue occurred when the HTTPS protocol was used for the login page and the password was sent as cleartext over HTTP. This issue was observed in controllers running ArubaOS 6.4.4.8 or later versions.	Captive Portal	All platforms	ArubaOS 6.4.4.8	ArubaOS 6.5.1.3
149766	**Symptom:** Clients failed to connect to an SSID after deleting an unused VLAN ID from the VLAN pool. The fix ensures that a change in the VLAN pool correctly updates the VLAN of the virtual AP profile. **Scenario:** This issue occurred when the **preserve-vlan** parameter was enabled in the virtual AP profile. This issue was observed in controllers running ArubaOS 6.4.4.6 or later versions.	AP-Platform	All platforms	ArubaOS 6.4.4.6	ArubaOS 6.5.1.3
149941	**Symptom:** An AP failed to establish a tunnel with the master (primary LMS) controller when the traffic between the AP and the primary LMS was blocked for more than 5 minutes. The fix ensures that the AP can successfully establish a tunnel with the primary LMS. **Scenario:** This issue occurred under the following circumstances: • CPsec was enabled on the primary LMS and the standby (backup LMS) controller. • The backup LMS was in the VRRP backup state. • When the AP failed over to the backup LMS, the AP established an IPsec tunnel and sent HELLO messages to the backup LMS. • As the backup LMS was in the VRRP backup state, it rejected the HELLO messages. • Once the HELLO message timed out, the AP deleted the IPsec tunnel and failed to toggle back to the primary LMS. This issue was observed in a master-standby deployment with controllers running ArubaOS 6.4.4.9 or later versions.	AP-Platform	All platforms	ArubaOS 6.4.4.9	ArubaOS 6.5.1.3

Table 3: *Resolved Issues in ArubaOS 6.5.1.3*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
150488	**Symptom:** An AP did not allow more than 49 clients to associate with it. The fix ensures that the number of client associations allowed is based on the AP capacity. **Scenario:** This issue occurred when WPA-PSK-AES encryption was used in bridge-forwarding mode. This issue was observed in 200 Series, 210 Series, 220 Series, and 270 Series access points running ArubaOS 6.4.4.9 or later versions.	AP-Wireless	200 Series, 210 Series, 220 Series, and 270 Series access points	ArubaOS 6.4.4.9	ArubaOS 6.5.1.3
150591 152214 152215 154630	**Symptom:** A memory leak was observed on the controller station management process that handles AP management and user association. Improvements in the station management process fixed the issue. **Scenario:** This issue occurred when clients moved from one AP to another. This issue was observed in controllers running ArubaOS 6.5.1.0 or later versions.	Station Management	All platforms	ArubaOS 6.5.1.0	ArubaOS 6.5.1.3
150759 154237 154576 154659 154660 155679	**Symptom:** An AP stopped responding and rebooted. The log file for the event listed the reason as **kernel panic: Fatal exception**. Improvements in the wireless driver of the AP resolved the issue. **Scenario:** This issue was observed in 310 Series and 320 Series access points running ArubaOS 6.5.1.2 and ArubaOS 6.4.4.9, respectively.	Wi-Fi Driver	310 Series and 320 Series access points	ArubaOS 6.4.4.9	ArubaOS 6.5.1.3
150829 152809 153998	**Symptom:** A client failed to obtain an IP address from the DHCP server. As a result, the client entry was not displayed in the user table of the controller. The fix ensures that the clients get an IP address from the DHCP server. **Scenario:** This issue occurred when the **Enforce DHCP** option was enabled in the AAA profile of an AP operating in split-tunnel forwarding mode. This issue was observed in controllers running ArubaOS 6.5.0.2 or later versions.	AP-Datapth	All platforms	ArubaOS 6.5.0.2	ArubaOS 6.5.1.3
150838 152014 152015	**Symptom:** A Samsung Galaxy player was authenticated successfully but the controller did not display the client in the user table. Improvements in the wireless driver of the AP resolved the issue. **Scenario:** This issue occurred when the HT and A-MPDU settings were enabled on the AP. This issue was observed in AP-205 and AP-225 access points running ArubaOS 6.4.4.10 or later versions.	AP-Wireless	AP-205 and AP-225 access points	ArubaOS 6.4.4.10	ArubaOS 6.5.1.3

Table 3: *Resolved Issues in ArubaOS 6.5.1.3*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
150934 151166 152533 152535	**Symptom:** An AP randomly failed to detect a change in PoE power. The fix ensures that the AP changes its power profile whenever it detects a change in PoE power. **Scenario:** This issue occurred when the power profile changed from 802.11af to 802.11at in a High Availability (HA) mode. This issue was observed in APs running ArubaOS 6.5.1.0 or later versions.	AP-Platform	All platforms	ArubaOS 6.5.1.0	ArubaOS 6.5.1.3
151258	**Symptom:** An AP stopped responding and rebooted. The log file for the event listed the reason as **power loss**. The fix ensures that the AP operates in the 802.3af mode when it detects 802.3af power on the switch port. **Scenario:** This issue occurred under the following circumstances: • The AP was connected to an HP switch. • The switch port was configured with 802.3af power. • The AP detected the power as 802.3at resulting in a reboot. This issue was observed in 330 Series access points running ArubaOS 6.5.0.0 or later versions.	AP-Platform	330 Series access points	ArubaOS 6.5.0.0	ArubaOS 6.5.1.3
151431	**Symptom:** The proxy-state attribute was found missing from the CoA request or Disconnect-ACK packet sent from the controller to the RADIUS proxy server. The fix ensures that the proxy-state attribute is included in the CoA request and Disconnect-ACK packet. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.2.6 or later versions.	RADIUS	All platforms	ArubaOS 6.4.2.6	ArubaOS 6.5.1.3
151641	**Symptom:** The controller stopped sending logs to an external syslog server. This issue is resolved by successfully processing the IP address of the remote logging server. **Scenario:** This issue occurred when the **facility** parameter was set in the **logging** command. For example, **logging <ip-address> facility <local0-local7>**. This issue was observed in controllers running ArubaOS 6.5.1.0 or later versions.	Logging	All platforms	ArubaOS 6.5.1.0	ArubaOS 6.5.1.3
151674	**Symptom:** Multiple RADAR detections were observed on all DFS channels of an AP. This issue is resolved by fixing the false detection on the European Telecommunications Standards Institute (ETSI) DFS domain. **Scenario:** This issue was observed in 320 Series access points running ArubaOS 6.4.4.8 or later versions.	AP-Wireless	320 Series access points	ArubaOS 6.4.4.8	ArubaOS 6.5.1.3

Table 3: *Resolved Issues in ArubaOS 6.5.1.3*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
151973 153597 153731 154438	**Symptom:** The WebUI of a local controller was inaccessible. In addition, the local controller stopped responding and rebooted. The log file for the event listed the reason as **Nanny rebooted machine - fpapps process died**. The fix ensures that the local controller does not reboot and the WebUI of the local controller is accessible. **Scenario:** This issue occurred when Hotspot 2.0 was enabled and 802.1X termination was disabled on the controller. This issue was observed in a master-local deployment with controllers running ArubaOS 6.4.3.7 or later versions.	Controller-Platform	All platforms	ArubaOS 6.4.3.7	ArubaOS 6.5.1.3
152062	**Symptom:** Intermittent kernel crash was observed in an AP. This issue is resolved by adding a crash protection mechanism during a PoE power change state in the AP. **Scenario:** This issue occurred when the PoE hardware detection on the AP was at 802.3af but the LLDP negotiated at 802.3at. Due to this, a race condition occurred. This issue was observed in 270 Series access points running ArubaOS 6.4.4.8 or later versions.	AP-Platform	270 Series access points	ArubaOS 6.4.4.8	ArubaOS 6.5.1.3
152184 152185 154114 154657 154686 154738 154771 156155 156158	**Symptom:** An AP stopped responding and rebooted. The log file for the event suggested a memory corruption. Upgrading the Serial Boot Loader (SBL) in the AP resolved this issue. **Scenario:** This issue was observed in 310 Series access points running ArubaOS 6.5.0.0 or later versions.	AP-Platform	310 Series access points	ArubaOS 6.5.0.0	ArubaOS 6.5.1.3
152209 152210 152621 154601	**Symptom:** On establishing a mesh link using the bridge-forwarding mode, the controller failed to forward the ARP packet of its gateway to clients behind the mesh portal. The fix ensures that the controller successfully forwards the ARP packet to the clients. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.1.0 or later versions.	Mesh	All platforms	ArubaOS 6.5.1.0	ArubaOS 6.5.1.3

Table 3: *Resolved Issues in ArubaOS 6.5.1.3*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
152369 152427	**Symptom:** An AP stopped responding and rebooted. The log file for the event listed the reason as **soft lockup - CPU#0 stuck**. Improvements in the wireless driver of the AP resolved the issue. **Scenario:** This issue occurred due to a race condition between the virtual AP initialization and the LLDP PoE message. When the wireless driver of the AP tried to enable the virtual AP, it turned off the radio. This resulted in a soft lock. This issue was observed in 200 Series, 210 Series, 220 Series, and 270 Series access points running ArubaOS 6.4.4.9 or later versions.	AP-Platform	200 Series, 210 Series, 220 Series, 270 Series access points	ArubaOS 6.4.4.9	ArubaOS 6.5.1.3
152499	**Symptom:** Few Instant APs failed to establish a VPN connection with the controller. This issue is resolved by deleting the older security associations without deleting the newly formed security association. **Scenario:** This issue occurred when an Instant AP reconnected to the controller but its source port changed during the reconnection. The inner IP was not cleared as part of security association cleanup and all security associations, including the newly formed security association, were cleared. This issue was observed in controllers running ArubaOS 6.4.4.9 or later versions.	IPsec	All platforms	ArubaOS 6.4.4.9	ArubaOS 6.5.1.3
152525	**Symptom:** The controller assigned IP address to clients from an incorrect VLAN. The fix ensures that the IP address is assigned from the correct VLAN. **Scenario:** This issue occurred after the reauthentication timer set on the 802.1X profile expired. This issue was observed in controllers running ArubaOS 6.4.3.9 or later versions.	Base OS Security	All platforms	ArubaOS 6.4.3.9	ArubaOS 6.5.1.3
152614 155789	**Symptom:** After a full configuration synchronization, the AirGroup chat ID **_presence._tcp** was found missing from the running configuration of the local controller. The fix ensures that the missing chat ID is included in the running configuration of the local controller. **Scenario:** This issue was observed in a master-local deployment with controllers running ArubaOS 6.5.0.0 or later versions.	AirGroup	All platforms	ArubaOS 6.5.0.0	ArubaOS 6.5.1.3

Table 3: *Resolved Issues in ArubaOS 6.5.1.3*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
152883	**Symptom:** A 2930F switch failed to process an L2 frame when connected to a controller. The fix ensures that the controller does not add an extra 4-byte frame check sequence when connected to the switch. **Scenario:** This issue occurred when the devices were connected as part of an L2 GRE tunnel. In an L2 GRE tunnel, the controller added an extra 4-byte frame check sequence. The switch failed to remove this frame check sequence from an L2 frame. This issue was observed in controllers running ArubaOS 6.5.1.0 or later versions.	Controller-Platform	All platforms	ArubaOS 6.5.1.0	ArubaOS 6.5.1.3
152908	**Symptom:** Multiple processes crashed in a controller unexpectedly. The log file for the event listed the reason as **Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**. The fix ensures that the security associations are deleted only when they are not marked as ready or if the negotiation fails. Deleting such security associations frees up the memory. **Scenario:** This issue occurred because the controller was out of memory. Due to a number of retries from the Instant APs that failed to establish a VPN connection, majority of the memory was consumed in storing the certificate for each connection. This issue was observed in controllers running ArubaOS 6.4.4.9 or later versions.	Controller-Platform	All platforms	ArubaOS 6.4.4.9	ArubaOS 6.5.1.3
154288	**Symptom:** 802.11v BSS transition management failures were observed during a client match event which directed a client to another BSSID. This issue is resolved by modifying 802.11v client match steering requests so that the target radio BSSID matches the BSSID used by the client, rather than the base BSSID of the radio. **Scenario:** This issue occurred when the clients were steered to another BSSID based on the base BSSID of the AP radio. This issue was observed in controllers and APs running ArubaOS 6.5.1.1 or later versions.	ARM	All platforms	ArubaOS 6.5.1.1	ArubaOS 6.5.1.3
154381	**Symptom:** Clients failed to access the captive portal page. The fix ensures that the clients can successfully access the captive portal page. **Scenario:** This issue occurred for clients connecting to the controller using L2TP over IPsec. This issue was observed in controllers running ArubaOS 6.5.0.3 or later versions.	Captive Portal	All platforms	ArubaOS 6.5.0.3	ArubaOS 6.5.1.3

Table 3: *Resolved Issues in ArubaOS 6.5.1.3*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
154407	**Symptom:** VIA client failed to establish a connection with the controller. Improvements in the ISAKMP hash algorithm resolved the issue. **Scenario:** This issue occurred when a custom ISAKMP policy was configured on the controller. This issue was observed in controllers running ArubaOS 6.5.1.2.	IPsec	All platforms	ArubaOS 6.5.1.2	ArubaOS 6.5.1.3
154628	**Symptom:** The controller incorrectly displayed high memory utilization on the **Dashboard > Controller > Gauges** page of the WebUI. This issue is resolved by recalibrating the memory gauge in the WebUI. With this change, the memory gauge on this page indicates 93% memory utilization at the yellow section of the gauge, and 97% memory utilization at the red section of the gauge. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.1.0 or later versions.	WebUI	All platforms	ArubaOS 6.5.1.0	ArubaOS 6.5.1.3
155261 155440 156581	**Symptom:** An AP failed to broadcast an SSID on the 802.11g radio. Improvements in the wireless driver of the AP resolved the issue. **Scenario:** Continuous 802.11g radio resets were observed on the AP. This issue was observed in 200 Series, AP-205H, 210 Series, and 220 Series access points running ArubaOS 6.5.0.3, ArubaOS 6.5.1.2, or earlier versions.	AP-Platform	200 Series, AP-205H, 210 Series, and 220 Series access points	ArubaOS 6.5.0.3	ArubaOS 6.5.1.3
155527	**Symptom:** An AP stopped responding and rebooted. The log file for the event listed the reason as **Reboot caused by kernel panic: Fatal exception**. Improvements in the AP memory management resolved the issue. **Scenario:** This issue was observed in 210 Series access points running ArubaOS 6.5.1.2.	AP-Wireless	210 Series access points	ArubaOS 6.5.1.2	ArubaOS 6.5.1.3

This chapter describes the known and outstanding issues identified in ArubaOS 6.5.1.3.

Table 4: *Known Issues in ArubaOS 6.5.1.3*

Bug ID	Description	Component	Platform	Reported Version
148348 152019 152020	**Symptom:** An AP stops responding and reboots unexpectedly. The log file for the event lists the reason as **kernel panic**. **Scenario:** This issue is observed in 310 Series access points running ArubaOS 6.5.1.0 or later versions. **Workaround:** None.	AP-Wireless	310 Series access points	ArubaOS 6.5.1.0
148977 155343	**Symptom:** A branch office controller randomly loses configuration updates from the master controller. **Scenario:** This issue occurs after a new license is sent from the master controller to the branch office controller. Thereafter, license-dependent configuration updates are not sent to the branch office controller. This issue is observed in a master-branch office controller deployment with controllers running ArubaOS 6.5.0.0 or later versions. **Workaround:** None.	Licensing	All platforms	ArubaOS 6.5.0.0
152352	**Symptom:** Multiple APs stop responding and reboot. The log file for the event lists the reason as **Reboot caused by kernel panic: Fatal exception in interrupt**. **Scenario:** This issue is caused by a corruption in the datapath bridge table entry for the AP. The bridge table comprises of AP statistics such as its MAC address, VLAN, assigned VLAN, destination, and flag information. This issue is observed in 330 Series access points running ArubaOS 6.5.0.1 or later versions. **Workaround:** None.	AP-Datapath	330 Series access points	ArubaOS 6.5.0.1

Table 4: *Known Issues in ArubaOS 6.5.1.3*

Bug ID	Description	Component	Platform	Reported Version
152602 154513	**Symptom:** The master controller fails to delete the stale route entries of the branch office controller. When you attempt to manually delete an entry, the controller does not delete the entry and displays the following error message: **ERROR: Cannot Delete Static Route**. **Scenario:** This issue occurs when you change the VLAN IP address of the branch office controller and upload the updated CSV file (static IP address template) on the master controller. This triggers a reboot of the branch office controller but fails to delete the stale route entries from the master controller. This issue is observed in a master-branch office controller deployment with controllers running ArubaOS 6.5.1.1 or later versions. **Workaround:** None.	Branch Office Controller	All platforms	ArubaOS 6.5.1.1
152890 153324	**Symptom:** A controller stops responding and reboots. The log file for the event lists the reason as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue occurs when the WebCC feature is enabled on the controller. This issue is observed in controllers running ArubaOS 6.5.0.2 or later versions. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.5.0.2
154422	**Symptom:** Clients fail to establish a VPN connection using L2TP over IPsec. **Scenario:** This issue occurs when the clients are behind a NAT device. This issue is observed in controllers running ArubaOS 6.5.0.3 or later versions. **Workaround:** None.	L2TP	All platforms	ArubaOS 6.5.0.3
154483	**Symptom:** A controller stops responding and reboots. The log file for the event lists the reason as **isakmpd** and **datapath timeout**. **Scenario:** This issue is triggered when you delete the global CA certificate from ISAKMP which is referenced in the group certificate. This issue is observed in controllers running ArubaOS 6.5.0.2 or later versions. **Workaround:** None.	IPsec	All platforms	ArubaOS 6.5.0.2

Maximum Number of NAT Pools

A controller supports a maximum of 60 NAT pools.

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

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

Topics in this chapter include:

Upgrade Caveats

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

- 120 Series access points, 600 Series, 3000 Series, M3, and 6000 controllers are not supported from ArubaOS 6.5.x. Do not upgrade to ArubaOS 6.5.x if your deployment contains a mix of these controllers in a master-local setup.
- If your controller is running ArubaOS 6.4.0.0 or later versions, do not use a Windows-based TFTP server to copy the ArubaOS image to the nonboot partition of the controller for upgrading or downgrading. Use FTP or SCP to copy the image.
- Starting from ArubaOS 6.4.x, you cannot create redundant firewall rules in a single ACL. ArubaOS will consider a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
  - source IP/alias
  - destination IP/alias

- proto-port/service

If you are upgrading from ArubaOS 6.1 or earlier and your configuration contains an ACL with redundant firewall rules, upon upgrading, only the last rule will remain.

For example, in the following ACL, both ACE entries could not be configured in ArubaOS 6.4.x. When the second ACE is added, it overwrites the first.

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

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

- When upgrading the software in a multicontroller 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 Multicontroller Network on page 27.)

GRE Tunnel-Type Requirements

This section describes the important points to remember when configuring an L2 GRE tunnel with respect to tunnel type:

- ArubaOS 6.5.1.3 continues to support L2 GRE tunnel type zero, but it is recommended to use a non-zero tunnel type.
- If both L2 and L3 tunnels are configured between endpoint devices, you must use a non-zero tunnel type for L2 GRE tunnels.

Important Points to Remember and Best Practices

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

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any other changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of your network by answering the following questions:
  - How many APs are assigned to each controller? Verify this information by navigating to the **Monitoring > NETWORK > All Access Points** section of the WebUI, or by executing the **show ap active** and **show ap database** CLI commands.

- How are those APs discovering the controller (DNS, DHCP Option, Broadcast)?
- What version of ArubaOS is currently on the controller?
- Are all controllers in a master-local cluster running the same version of software?
- Which services are used on the controllers (employee wireless, guest access, remote AP, wireless voice)?

- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software images to the controller. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to this version of ArubaOS, assess your software license requirements and load any new or expanded licenses you may require. For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the *ArubaOS 6.5.x User Guide*.

Memory Requirements

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

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

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 execute the **halt** command before power cycling.

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

- **Crash Data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 26 to copy the **crash.tar** file to an external server, and then execute the **tar clean crash** command to delete the file from the controller.
- **Flash Backups:** Use the procedures described in Backing up Critical Data on page 26 to back up the flash directory to a file named **flash.tar.gz**, and then execute the **tar clean flash** command to delete the file from the controller.

- **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 26 to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the controller.

Backing up Critical Data

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

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

Backing up and Restoring Compact Flash in the WebUI

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

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

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

Backing up and Restoring Compact Flash in the CLI

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

1. Make sure you are in the **enable** mode in the controller CLI, and execute the following command:

   ```
   (host) # write memory
   ```
2. Execute the **backup** command to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.

```
(host) # backup flash
Please wait while we tar relevant files from flash...
Please wait while we compress the tar file...
Checking for free space on flash...
Copying file to flash...
File flashbackup.tar.gz created successfully on flash.
```

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

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

   You can later transfer the backup flash file from the external server or storage device to the compact flash file system by executing the **copy** command.

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

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

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

Upgrading in a Multicontroller Network

In a multicontroller 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 26.

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

To upgrade an existing multicontroller system to this version of ArubaOS:

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 rebooted simultaneously, use the following guidelines:
   a. Upgrade the software image on all the controllers. Reboot the master controller. After the master controller completes rebooting, you can reboot the local controllers simultaneously.
   b. Verify that the master and all local controllers are upgraded properly.

Installing the FIPS Version of ArubaOS 6.5.1.3

Download the FIPS version of the software from https://support.arubanetworks.com.

Instructions on Installing FIPS Software

Before you install a FIPS version of the software on a controller that is currently running a non-FIPS version of the software, follow the procedure below. If you are currently running a FIPS version of the software on the controller, you do not have to perform a **write erase** to reset the configuration as mentioned in step 2.

Follow the steps below to install the FIPS software on a controller that is currently running a non-FIPS version of the software:

1. Install the FIPS version of the software on the controller.
2. Execute the **write erase** command to reset the configuration to the factory default; otherwise, you cannot log in to the controller using the CLI or WebUI.
3. Reboot the controller by executing the **reload** command.

This is the only supported method of moving from non-FIPS software to FIPS software.

Upgrading to ArubaOS 6.5.1.3

The following sections provide the procedures for upgrading the controller to ArubaOS 6.5.1.3 by using the WebUI and the CLI.

Install Using the WebUI

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash space available for an upgrade using the WebUI. For details, see Memory Requirements on page 25.

When you navigate to the **Configuration** tab of the controller's WebUI, the controller may display the **Error getting information: command is not supported on this platform** message. This error occurs when you upgrade the controller from the WebUI and navigate to the **Configuration** tab as soon as the controller completes rebooting. This error is expected and disappears after clearing the Web browser cache.

When upgrading from an existing ArubaOS 6.4.x release, it is required to set AMON packet size manually to a desired value. However, the packet size is increased to 32K by default for fresh installations of ArubaOS 6.4.3.9.

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

1. Download ArubaOS 6.5.1.3 from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Validate the SHA hash for a software image:
   a. Download the **Aruba.sha256** file from the download directory.

b. To verify the image, load the image onto a Linux system and execute the **sha256sum <filename>** command or use a suitable tool for your operating system that can generate a **SHA256** hash of a file.

c. Verify that the output produced by this command matches the hash value found on the support site.

The ArubaOS image file is digitally signed, and is verified using RSA2048 certificates preloaded on the controller at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the controller will not load a corrupted image.

4. Log in to the ArubaOS WebUI from the PC or workstation.
5. Navigate to the **Maintenance > Controller > Image Management** page.
   a. Select the **Local File** option.
   b. Click **Browse** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the nonboot partition from the **Partition to Upgrade** radio button.
8. Choose **Yes** in the **Reboot Controller After Upgrade** radio button to automatically reboot after upgrading. Choose **No**, if you do not want the controller to reboot immediately.

Upgrade will not take effect until you reboot the controller.

9. Choose **Yes** in the **Save Current Configuration Before Reboot** radio button.
10. Click **Upgrade**.

    When the software image is uploaded to the controller, a popup window displays the **Changes were written to flash successfully** message.
11. Click **OK**.

    If you chose to automatically reboot the controller in step 8, 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 > NETWORK > All WLAN Controllers** page to verify the upgrade.

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

1. Log in to the WebUI to verify all your controllers are up after the reboot.
2. Navigate to the **Monitoring > NETWORK > Network Summary** page to determine if your APs are up and ready to accept clients. In addition, verify that the number of access points and clients are what you would expect.
3. Verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use and in different locations when possible.

5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 26 for information on creating a backup. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses.

Install Using the CLI

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash space available for an upgrade using the CLI. For details, see Memory Requirements on page 25.

To install the ArubaOS software image from a PC or workstation using the CLI on the controller:

1. Download ArubaOS 6.5.1.3 from the customer support site.
2. Open an SSH session on your master (and local) controllers.
3. Execute the **ping** command to verify the network connection from the target controller to the SCP/FTP/TFTP server.

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

   or

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

   or

   ```
   (host)# ping <scphost>
   ```
4. Execute the **show image version** command to check if the ArubaOS images are loaded on the controller's flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.
5. Execute the **copy** command to load the new image onto the nonboot partition.

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

   or

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

   or

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

   or

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

The USB option is available on the 7000 Series and 7200 Series controllers.

6. Execute the **show image version** command to verify that the new image is loaded.
7. Reboot the controller.

   ```
   (host)# reload
   ```

8. Execute the **show version** command to verify that the upgrade is complete.
   ```
   (host)# show version
   ```

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

1. Log in to the CLI to verify that all your controllers are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of access points and clients are what you expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 26 for information on creating a backup.

Downgrading

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

If you upgraded from ArubaOS 3.3.x to ArubaOS 5.0, the upgrade script encrypts the internal database. New entries created in ArubaOS 6.5.1.3 are lost after the downgrade (this warning does not apply to upgrades from ArubaOS 3.4.x to ArubaOS 6.1).

If you do not downgrade to a previously saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from ArubaOS 6.5.1.3 to 5.0.3.2, changes made to WIPS in ArubaOS 6.x prevent the new predefined IDS profile assigned to an AP group from being recognized by the older version of ArubaOS. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.

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

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

Before You Begin

Before you reboot the controller with the preupgrade software version, you must perform the following steps:

1. Back up your controller. For details, see Backing up Critical Data on page 26.
2. Verify that the control plane security is disabled.
3. Set the controller to boot with the previously saved pre-ArubaOS 6.5.1.3 configuration file.
4. Set the controller to boot from the system partition that contains the previously running ArubaOS image.

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

5. After downgrading the software on the controller, perform the following steps:
   - Restore pre-ArubaOS 6.5.1.3 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.5.1.3 flash backup file.
   - You do not need to reimport the WMS database or RF Plan data. However, if you have added changes to RF Plan in ArubaOS 6.5.1.3, the changes do not appear in RF Plan in the downgraded ArubaOS version.
   - If you installed any certificates while running ArubaOS 6.5.1.3, you need to reinstall the certificates in the downgraded ArubaOS version.

Downgrading Using the WebUI

The following section describes how to use the WebUI to downgrade the software on the controller.

1. If the saved preupgrade 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 preupgrade configuration file.
   b. For **Destination Selection**, enter a file name (other than default.cfg) for Flash File System.
2. Set the controller to boot with your preupgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved preupgrade configuration file from the **Configuration File** drop-down list.
   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) by performing the following steps:
   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 preupgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The controller reboots after the countdown period.
6. When the boot process is complete, verify that the controller is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

Downgrading Using the CLI

The following section describes how to use the CLI to downgrade the software on the controller.

1. If the saved preupgrade 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 preupgrade configuration file.

   ```
   (host) # boot config-file   <backup configuration filename>
   ```

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

   In the following example, partition 1, the backup system partition, contains the backup release ArubaOS 6.1.3.2. Partition 0, the default boot partition, contains the ArubaOS 6.5.1.3 image.

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

   ```
   (host) # boot system partition 1
   ```

5. Reboot the controller.

   ```
   (host) # reload
   ```

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

   ```
   (host) # show image version
   ```

Before You Call Technical Support

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

1. Provide a detailed network topology (including all the devices in the network between the user and the Aruba controller with IP addresses and Interface numbers if possible).
2. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless Network Interface Card (NIC) make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
3. Provide the controller logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
4. Provide the syslog file of the controller at the time of the problem. Aruba strongly recommends that you consider adding a syslog server if you do not already have one to capture logs from the controller.
5. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have an outage in a network that worked in the past, a network configuration that has never worked, or a brand new installation.

6. Let the support person know if there are any recent changes in your network (external to the Aruba controller) or any recent changes to your controller and/or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) of when the problem first occurred. If the problem is reproducible, list the exact steps taken to re-create the problem.
8. Provide any wired or wireless sniffer traces taken during the time of the problem.
9. Provide the controller site access information, if possible.

Appendix A
Acronyms and Abbreviations

The following table lists the acronyms and abbreviations used in Aruba documents.

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
3G	Third Generation of Wireless Mobile Telecommunications Technology
4G	Fourth Generation of Wireless Mobile Telecommunications Technology
AAA	Authentication, Authorization, and Accounting
ABR	Area Border Router
AC	Access Category
ACC	Advanced Cellular Coexistence
ACE	Access Control Entry
ACI	Adjacent Channel interference
ACL	Access Control List
AD	Active Directory
ADO	Active X Data Objects
ADP	Aruba Discovery Protocol
AES	Advanced Encryption Standard
AIFSN	Arbitrary Inter-frame Space Number
ALE	Analytics and Location Engine

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
ALG	Application Layer Gateway
AM	Air Monitor
AMON	Advanced Monitoring
AMP	AirWave Management Platform
A-MPDU	Aggregate MAC Protocol Data Unit
A-MSDU	Aggregate MAC Service Data Unit
ANQP	Access Network Query Protocol
ANSI	American National Standards Institute
AP	Access Point
API	Application Programming Interface
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
AVF	AntiVirus Firewall
BCMC	Broadcast-Multicast
BGP	Border Gateway protocol
BLE	Bluetooth Low Energy
BMC	Beacon Management Console
BPDU	Bridge Protocol Data Unit
BRAS	Broadband Remote Access Server

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
BRE	Basic Regular Expression
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CA	Certification Authority
CAC	Call Admission Control
CALEA	Communications Assistance for Law Enforcement Act
CAP	Campus AP
CCA	Clear Channel Assessment
CDP	Cisco Discovery Protocol
CDR	Call Detail Records
CEF	Common Event Format
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CLI	Command-Line Interface
CN	Common Name
CoA	Change of Authorization
CoS	Class of Service
CPE	Customer Premises Equipment

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
CPsec	Control Plane Security
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSA	Channel Switch Announcement
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSR	Certificate Signing Request
CSV	Comma Separated Values
CTS	Clear to Send
CW	Contention Window
DAS	Distributed Antenna System
dB	Decibel
dBm	Decibel Milliwatt
DCB	Data Center Bridging
DCE	Data Communication Equipment
DCF	Distributed Coordination Function
DDMO	Distributed Dynamic Multicast Optimization
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
DFT	Discreet Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMO	Dynamic Multicast optimization
DN	Distinguished Name
DNS	Domain Name System
DOCSIS	Data over Cable Service Interface Specification
DoS	Denial of Service
DPD	Dead Peer Detection
DPI	Deep Packet Inspection
DR	Designated Router
DRT	Downloadable Regulatory Table
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum
DST	Daylight Saving Time
DTE	Data Terminal Equipment
DTIM	Delivery Traffic Indication Message
DTLS	Datagram Transport Layer Security
DU	Data Unit

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
EAP	Extensible Authentication Protocol
EAP-FAST	EAP-Flexible Authentication Secure Tunnel
EAP-GTC	EAP-Generic Token Card
EAP-MD5	EAP-Method Digest 5
EAP-MSCHAP EAP-MSCHAPv2	EAP-Microsoft Challenge Handshake Authentication Protocol
EAPoL	EAP over LAN
EAPoUDP	EAP over UDP
EAP-PEAP	EAP-Protected EAP
EAP-PWD	EAP-Password
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
ECC	Elliptical Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EIGRP	Enhanced Interior Gateway Routing Protocol
EIRP	Effective Isotropic Radiated Power
EMM	Enterprise Mobility Management
ESI	External Services Interface
ESS	Extended Service Set

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
ESSID	Extended Service Set Identifier
EULA	End User License Agreement
FCC	Federal Communications Commission
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FIB	Forwarding Information Base
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
FQLN	Fully Qualified Location Name
FRER	Frame Receive Error Rate
FRR	Frame Retry Rate
FSPL	Free Space Path Loss
FTP	File Transfer Protocol
GBps	Gigabytes per second
Gbps	Gigabits per second
GHz	Gigahertz
GIS	Generic Interface Specification
GMT	Greenwich Mean Time
GPP	Guest Provisioning Page
GPS	Global Positioning System

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
GVRP	GARP or Generic VLAN Registration Protocol
H2QP	Hotspot 2.0 Query Protocol
HA	High Availability
HMD	High Mobility Device
HSPA	High-Speed Packet Access
HT	High Throughput
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS	Internet Authentication Service
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IDS	Intrusion Detection System
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
IKE PSK	Internet Key Exchange Pre-shared Key
IoT	Internet of Things
IP	Internet Protocol
IPM	Intelligent Power Monitoring
IPS	Intrusion Prevention System
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
JSON	JavaScript Object Notation
KBps	Kilobytes per second
Kbps	Kilobits per second
L2TP	Layer-2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDPC	Low-Density Parity-Check
LEA	Law Enforcement Agency
LEAP	Lightweight Extensible Authentication Protocol

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
LED	Light Emitting Diode
LEEF	Long Event Extended Format
LI	Lawful Interception
LLDP	Link Layer Discovery Protocol
LLDP-MED	LLDP–Media Endpoint Discovery
LMS	Local Management Switch
LNS	L2TP Network Server
LTE	Long Term Evolution
MAB	MAC Authentication Bypass
MAC	Media Access Control
MAM	Mobile Application Management
MBps	Megabytes per second
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MD5	Message Digest 5
MDM	Mobile Device Management
mDNS	Multicast Domain Name System
MFA	Multi-factor Authentication
MHz	Megahertz

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
MIB	Management Information Base
MIMO	Multiple-Input Multiple-Output
MLD	Multicast Listener Discovery
MPDU	MAC Protocol Data Unit
MPLS	Multiprotocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSS	Maximum Segment Size
MSSID	Mesh Service Set Identifier
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
MU-MIMO	Multi-User Multiple-Input Multiple-Output
MVRP	Multiple VLAN Registration Protocol
NAC	Network Access Control
NAD	Network Access Device
NAK	Negative Acknowledgment Code
NAP	Network Access Protection
NAS	Network Access Server Network-attached Storage
NAT	Network Address Translation

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
NetBIOS	Network Basic Input/Output System
NIC	Network Interface Card
Nmap	Network Mapper
NMI	Non-Maskable Interrupt
NMS	Network Management Server
NOE	New Office Environment
NTP	Network Time Protocol
OAuth	Open Authentication
OCSP	Online Certificate Status Protocol
OFA	OpenFlow Agent
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier
OKC	Opportunistic Key Caching
OS	Operating System
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
OVA	Open Virtual Appliance
OVF	Open Virtualization Format
PAC	Protected Access Credential

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
PAP	Password Authentication Protocol
PAPI	Proprietary Access Protocol Interface
PCI	Peripheral Component Interconnect
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PEAP-GTC	Protected Extensible Authentication Protocol-Generic Token Card
PEF	Policy Enforcement Firewall
PFS	Perfect Forward Secrecy
PHB	Per-hop behavior
PIM	Protocol-Independent Multicast
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMK	Pairwise Master Key
PoE	Power over Ethernet
POST	Power On Self Test
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PPTP	PPP Tunneling Protocol

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
PRNG	Pseudo-Random Number Generator
PSK	Pre-Shared Key
PSU	Power Supply Unit
PVST	Per VLAN Spanning Tree
QoS	Quality of Service
RA	Router Advertisement
RADAR	Radio Detection and Ranging
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RAP	Remote AP
RAPIDS	Rogue Access Point and Intrusion Detection System
RARP	Reverse ARP
REGEX	Regular Expression
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio Frequency Identification
RIP	Routing Information Protocol
RRD	Round Robin Database

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
RSA	Rivest, Shamir, Adleman
RSSI	Received Signal Strength Indicator
RSTP	Rapid Spanning Tree Protocol
RTCP	RTP Control Protocol
RTLS	Real-Time Location Systems
RTP	Real-Time Transport Protocol
RTS	Request to Send
RTSP	Real Time Streaming Protocol
RVI	Routed VLAN Interface
RW RoW	Rest of World
SA	Security Association
SAML	Security Assertion Markup Language
SAN	Subject Alternative Name
SCB	Station Control Block
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SDN	Software Defined Networking
SDR	Software-Defined Radio

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SDU	Service Data Unit
SD-WAN	Software-Defined Wide Area Network
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIRT	Security Incident Response Team
SKU	Stock Keeping Unit
SLAAC	Stateless Address Autoconfiguration
SMB	Small and Medium Business
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SNIR	Signal-to-Noise-Plus-Interference Ratio
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SoC	System on a Chip

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SoH	Statement of Health
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
STBC	Space-Time Block Coding
STM	Station Management
STP	Spanning Tree Protocol
STRAP	Secure Thin RAP
SU-MIMO	Single-User Multiple-Input Multiple-Output
SVP	SpectraLink Voice Priority
TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFTP	Trivial File Transfer Protocol
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TLV	Type-length-value
ToS	Type of Service

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
TPC	Transmit Power Control
TPM	Trusted Platform Module
TSF	Timing Synchronization Function
TSPEC	Traffic Specification
TTL	Time to Live
TTLS	Tunneled Transport Layer Security
TXOP	Transmission Opportunity
U-APSD	Unscheduled Automatic Power Save Delivery
UCC	Unified Communications and Collaboration
UDID	Unique Device Identifier
UDP	User Datagram Protocol
UI	User Interface
UMTS	Universal Mobile Telecommunication System
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VA	Virtual Appliance

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
VBN	Virtual Branch Networking
VBR	Virtual Beacon Report
VHT	Very High Throughput
VIA	Virtual Intranet Access
VIP	Virtual IP Address
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over IP
VoWLAN	Voice over Wireless Local Area Network
VPN	Virtual Private Network
VRD	Validated Reference Design
VRF	Visual RF
VRRP	Virtual Router Redundancy Protocol
VSA	Vendor-Specific Attributes
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WebUI	Web browser User Interface
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
WIDS	Wireless Intrusion Detection System

Table 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
WINS	Windows Internet Naming Service
WIPS	Wireless Intrusion Prevention System
WISPr	Wireless Internet Service Provider Roaming
WLAN	Wireless Local Area Network
WME	Wireless Multimedia Extensions
WMI	Windows Management Instrumentation
WMM	Wi-Fi Multimedia
WMS	WLAN Management System
WPA	Wi-Fi Protected Access
WSDL	Web Service Description Language
WWW	World Wide Web
WZC	Wireless Zero Configuration
XAuth	Extended Authentication
XML	Extensible Markup Language
XML-RPC	XML Remote Procedure Call
ZTP	Zero Touch Provisioning