ArubaOS 6.5.4.5

a Hewlett Packard
Enterprise company

Release Notes

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 04	Removed description of known issue 159774.
Revision 03	The following changes are made in this revision: ■ Updated platform of resolved issue 168530. ■ Updated commands in description of no support for cell size reduction feature.
Revision 02	The following changes are made in this revision: ■ Updated platform of resolved issue 167520. ■ Added description of resolved issue 172733.
Revision 01	Initial release.

ArubaOS 6.5.4.5 is a software release that includes new features and enhancements introduced in this release, fixes to issues identified in previous releases as well as the known and outstanding issues in this release.

NOTE

See the Upgrade Procedure on page 48 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.
- Glossary of Terms lists the acronyms and abbreviations used in the document.

NOTE

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 6.5.4.5 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 and/or enhancements introduced in ArubaOS 6.5.4.5. For more information about these features, refer to the *ArubaOS 6.5.4.x User Guide*.

AP-Platform

No Support for AP Image Preload

Starting from ArubaOS 6.5.4.5, AP image preload is not supported. The following **image-preload** commands are not supported:

```
ap image-preload activate all-aps
ap image-preload activate specific-aps
ap image-preload add ap-group
ap image-preload add ap-name
ap image-preload cancel
ap image-preload clear-all
ap image-preload delete ap-group
ap image-preload delete ap-name
```

AP-Wireless

No Support for Cell Size Reduction

Starting from ArubaOS 6.5.4.5, the **cell-size-reduction** parameter in the **rf dot11a-radio-profile** and **rf dot11g-radio-profile** commands does not take effect for 300 Series access points. Any value configured for the **cell-size-reduction** parameter is disregarded by the 300 Series access points.

Controller-Platform

NTP Authentication Option

Starting from ArubaOS 6.5.4.5, a new NTP authentication option using SHA1 digest is available. A new parameter, **sha1**, is introduced in the **ntp authentication-key** command. You can configure this option in the CLI using the **ntp authentication-key <keyid> sha1 <keyvalue>** command. The **show ntp authentication-keys** command, with which you can verify the NTP authentication key type, now shows the sha1 key type as well along with the secret in encoded format, when SHA1 authentication is configured.

Retrieving Crash Information from Controllers

To access the crash files after upgrading a controller to ArubaOS 6.5.4.5, you must clear the old crash files. Remember the following important points regarding the old crash files cleanup:

- Before you upgrade to ArubaOS 6.5.4.5, ensure that you clean up the old crash files if any, using the **tar crash** command.
- If you have upgraded a controller to ArubaOS 6.5.4.5 before cleaning up the old crash files and if there are no new crashes after the upgrade, you must still clean up the old crash files using the **tar crash** command.
- If you execute the **tar crash** command:
  - before cleaning up the old crash files, the **crash.tar** and **crash1.tar** files are created.
  - after cleaning up the old crash files, only the **crash.tar** file is created.

When you report a crash, execute the **copy** command to copy the **crash.tar** and **crash1.tar** files (if applicable), and share the files with Technical Support.

Modified Commands

The following CLI commands are modified in ArubaOS 6.5.4.5:

show ip ospf interface

The output of this command now displays the transmit and receive errors:

Example

```
(host) #show ip ospf interface tunnel 100

Tunnel 100 is up, line protocol is up
Internet Address 12.12.0.1, Mask 255.255.255.0, Area 0.0.1.0
Router ID 16.2.0.101, Network Type POINT_TO_POINT, Cost: 1
Transmit Delay is 1 sec, State PTPST, Priority 1
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
Neighbor Count is 1
Tx Stat: Hellos 162 DbDescr 2 LsReq 1 LsUpdate 1 LsAck 1 Pkts 167
Tx Err:  BufNull 0 BufCorrupt 0 NoMem 0 SendFail 167
Rx Stat: Hellos 160 DbDescr 3 LsReq 0 LsUpdate 2 LsAck 1 Pkts 166
LoopSend 0 RxVirtualLink 0
Rx Err:  DisCd 0 BadVer 0 BadNet 0 BadArea 0 BadDstAdr 0 BadAuType 0
BadAuth 0 BadNeigh 0 BadPckType 0 BadVirtLink 0
IntfDown 0 MySource 0 Legal 0
```

show ip ospf neighbor

The output of this command now displays the total number of neighbors or routes, active LSAs, and retransmit LSAs.

Example

```
(host) #show ip ospf neighbor

OSPF Neighbor Table
-------------------
Neighbor ID  Pri  State          Address      Interface
-----------  ---  -----          -------      ---------
10.8.228.5   1    INIT/DROTHER   10.8.228.5   Vlan 10

(host) #show ip ospf

OSPF is currently running with Router ID 10.8.228.8
Number of areas in this router is 1
Area 0.0.0.0
        Number of interfaces in this area is 3
        Area is normal area
        SPF algorithm executed 1 times
Number of neighbors in this router is 1
Number of Active LSAs in this router is 1
Number of Retransmit LSAs in this router is 0
```

show ip route

The output of this command now displays the administrative distance and cost in [AD/Cost] format.

Example

```
(host) #show ip route

        Codes:  C - connected, O - OSPF, R - RIP, S - static
                M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN/Branch

Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10
Gateway of last resort is 10.7.73.77 to network 0.0.0.0 at cost 1
S* 0.0.0.0/0 [1/0] via 10.7.73.77*
S 172.0.0.0/8 [1/0] via 172.16.1.253*
```

New Commands

The following CLI commands are added in ArubaOS 6.5.4.5:

ipvpn-tunnel-trusted

This command configures an IAP VPN tunnel as **trusted**. When an IAP VPN tunnel is trusted, a datapath user entry is not created for each user who is connected behind the IAP VPN tunnel. Hence, Broadcast-Multicast (BCMC) optimization, if configured, is not applied.

Example

```
(host) (config) #iapvpn-tunnel-trusted
```

no ipvpn-tunnel-trusted

This command configures an IAP VPN tunnel as **untrusted**. When an IAP VPN tunnel is untrusted (default behavior), a datapath user entry is created for each user who is connected behind the IAP VPN tunnel. Hence, BCMC optimization, if configured, is applied.

Example

```
(host) (config) #no iapvpn-tunnel-trusted
```

show memory iapmgr

The output of this command displays the memory information of the **IAP Manager** process.

Example

```
(host) #show memory iapmgr

 Type           Num Allocs     Size Allocs      Peak Allocs      Peak Size
------         ------------   -------------    -------------    -----------

default              1863          176748             1878         182052

 PC             Allocs           Size
----            ------           ----
  0x41357c             1            256
0x2aaf1730             1             64
0x2aaf3628             8            640
0x2aaf38e0             1           1168
0x2aaf46b0             4            272
0x2aaf568c             1             80
0x2aaf56c0             1           4096
0x2ab232c8           549          17568
0x2ab233bc            43           2752
0x2ab23408            43           9412
0x2ab23424            43           9412
0x2ab23474            43           2752
0x2ab2471c           515          16480
0x2ab24768           515           7510
```

```
0x2ab24fd8              1             32
0x2ab26de4             51            612
0x2ab26f28              9            144
0x2acc41e4              5             80
0x2ad22228              9            900
0x2ad2a31c              1           4204
0x2ad2a6b0              1          41000
0x2ad2a6c8              1          41000
0x2ad30bd0              1           4168
0x2ad52190              1           3612
0x2ae08a60              3           8294

total                          176748                        182052
```

Remote AP

Enhancements in USB Initialization of 4G/LTE Modem

Starting from ArubaOS 6.5.4.5, you can configure two AP Names (APNs) during USB initialization of a 4G/LTE USB modem. While the first APN initiates the connection to obtain an IP address, the second APN sends and receives data. Use a semicolon (;) as a delimiter to create two separate strings for the APN configurations in the following commands under the AP provisioning profile:

```
(host) (config) #ap provisioning-profile <profile-name>
(host) (Provisioning profile "<profile-name>") #usb-init <APN1-string>; <APN2-string>
```

Example

The following sample configuration includes the string values for two APN configurations:

```
(host) (config) #ap provisioning-profile default
(host) (Provisioning profile "default") #usb-init "AT+CGDCONT=1,\"IP\",\"APN1\";1,1,\"APN2\""
```

You must obtain the APN from your ISP and ensure that each APN entry follows the manufacturer's AT command reference.

SNMP

Enhancement to SNMP Authentication Failed Trap

Starting from ArubaOS 6.5.4.5, the **SNMP Authentication Failure** trap includes the IPv4 address of the source that is failing authentication.

Chapter 3
Regulatory Updates

This chapter describes the regulatory updates in ArubaOS 6.5.4.5.

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 6.5.4.5:

- DRT-1.0_63516

For a complete list of countries and the regulatory domains in which the APs are certified for operation, refer to the Downloadable Regulatory Table or 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.

Chapter 4
Resolved Issues

This chapter describes the issues resolved in ArubaOS 6.5.4.5.

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
116718 156226	**Symptom:** The downstream traffic did not pass through from an AP to its associated client. This fix ensures that the AP transmits data to the clients without service interruption. **Scenario:** This issue occurred when the clients did not respond to the add block acknowledgment frame request from the AP. This issue was observed in access points running ArubaOS 6.5.2.0 or later versions.	AP-Wireless	All platforms	ArubaOS 6.5.2.0	ArubaOS 6.5.4.5
125335 138340 152333 159970 167506 168399 169246 169314 169523 169568 169596 170181 170238 170446 170740 170956 171337 172736 172884 173586 173613 173769	**Symptom:** A controller stopped responding and rebooted unexpectedly. The log file listed the reason for the event listed as **kernel panic: Intent:cause:register 12:86:e0:2**. The fix ensures that the controller works as expected. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.3.4 or later versions.	Controller-Platform	All platforms	ArubaOS 6.5.3.4	ArubaOS 6.5.4.5
138808	**Symptom:** An AP failed to perform wireless containment. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue occurred when an AP functioning in the AM mode was unable to send containment-related frames. This issue was observed in AP-205, 210 Series, 220 Series, and 270 Series access points running ArubaOS 6.4.3.6 or later versions.	Air Management-IDS	AP-205, 210 Series, 220 Series, or 270 Series access points	ArubaOS 6.4.3.6	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
140779	**Symptom:** SNMP enterprise-specific traps did not contain the enterprise trap OID. The fix ensures that the traps contain the enterprise trap OID. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.4.5.	SNMP	All platforms	ArubaOS 6.4.4.5	ArubaOS 6.5.4.5
142460 171486	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **mac_to_str_r,remove_dos_sta,timer_handler,TimerExpiredOnTimer,DispProcessPrio,main**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in AP-135 access points running ArubaOS 6.5.3.3 or later versions.	Station Management	AP-135 access points	ArubaOS 6.5.3.3	ArubaOS 6.5.4.5
146158	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Fatal exception at NIP d98945d4 LR d988a998 CTR: c000c724**. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-205, 210 Series, 220 Series, and 270 Series access points running ArubaOS 6.4.2.15 or later versions.	AP-Wireless	AP-205, 210 Series, 220 Series, or 270 Series access points	ArubaOS 6.4.2.15	ArubaOS 6.5.4.5
148853 171107	**Symptom:** A standby controller failed to complete database synchronization because the master controller timed out before the standby controller acknowledged the request. The issue is resolved by increasing the timeout value on the master controller for standby database synchronization. **Scenario:** This issue occurred when the size of the WMS database was large and hence, the standby controller took a longer time to acknowledge. This issue was observed in controllers running ArubaOS 6.3.1.24 or later versions in a master-standby topology.	Database	All platforms	ArubaOS 6.3.1.24	ArubaOS 6.5.4.5
148870 168168 173411	**Symptom:** Although OpenFlow was not enabled, the **OpenFlow** process in a controller crashed and the controller rebooted unexpectedly. This issue is resolved by updating an IPsec tunnel if it already exists in the cache. **Scenario:** This issue occurred when the **OpenFlow** process attempted to add an IPsec tunnel that already existed in the cache. This issue was observed in controllers running ArubaOS 6.5.1.5.	SDN	All platforms	ArubaOS 6.5.1.5	ArubaOS 6.5.4.5
150543 172480	**Symptom:** The **SNMPD** process in a controller crashed unexpectedly. The fix ensures that the **SNMPD** process does not crash. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.2.1.	SNMP	All platforms	ArubaOS 6.5.2.1	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
154899	**Symptom:** The **BLE Relay** process in a controller crashed unexpectedly. The fix ensures that the **BLE Relay** process does not crash and the controller works as expected. **Scenario:** This issue was observed in a controller running ArubaOS 6.5.1.2 or later versions.	BLE	All platforms	ArubaOS 6.5.1.2	ArubaOS 6.5.4.5
155721	**Symptom:** APs frequently changed channels. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue occurred because of false radar detection. This issue was observed in 200 Series, 210 Series, 220 Series, and 270 Series access points running ArubaOS 6.4.2.16 or later versions.	AP-Wireless	200 Series, 210 Series, 220 Series, or 270 Series access points	ArubaOS 6.4.2.16	ArubaOS 6.5.4.5
156484 171487 172129 174740	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Unable to handle kernel paging request for data at address 0x00000022**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in 210 Series, 220 Series, 270 Series, and AP-225 access points running ArubaOS 6.5.2.0 or later versions.	AP-Platform	210 Series, 220 Series, 270 Series, or AP-225 access points	ArubaOS 6.5.2.0	ArubaOS 6.5.4.5
158187 166203 167558	**Symptom:** The WebUI displayed the **show profile-list aaa radius modifier start0" data: null** error when a user navigated to the **Configuration > Security > Authentication > Server > RADIUS Server** page. This issue is resolved by adding license checks that restrict the **Accounting-Request** and **Access-Request** modifiers in the **radius server** profile list when a required license does not exit. **Scenario:** This issue occurred when a controller did not have a PEF license. This issue was observed in controllers running ArubaOS 6.5.1.1 or later versions.	WebUI	All platforms	ArubaOS 6.5.1.1	ArubaOS 6.5.4.5
158459	**Symptom:** An SNMP query in a controller retrieved an incorrect value for the associated user count in an AP. The fix ensures that the SNMP query retrieves the correct value. **Scenario:** This issue was observed in access points running ArubaOS 6.4.4.9 or later versions.	AP-Platform	All platforms	ArubaOS 6.4.4.9	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
158719 158720	**Symptom:** A controller crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (Intent:cause:register 56:86:50:2)**. The fix ensures that the controller does not crash and works as expected. **Scenario:** This issue occurred when two Ethernet ports of an AP were plugged into a switch which led to a loop and datapath spike in the controller. This issue was observed in controllers running ArubaOS 6.4.3.6 or later versions.	Controller-Platform	All platforms	ArubaOS 6.4.3.6	ArubaOS 6.5.4.5
159046	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: __bug**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in AP-135 access points running ArubaOS 6.5.0.3.	AP-Wireless	AP-135 access points	ArubaOS 6.5.0.3	ArubaOS 6.5.4.5
159833 165229	**Symptom:** A user could not enable or disable OSPF on a GRE tunnel interface. The fix ensures that a user can enable or disable OSPF on a GRE tunnel. **Scenario:** This issue is observed in controllers running ArubaOS 6.4.3.4 or later versions.	OSPF	All platforms	ArubaOS 6.4.3.4	ArubaOS 6.5.4.5
160278 164501	**Symptom:** An IP address was not assigned to a wireless client when a wired and a wireless network were in the same VLAN. The fix ensures that an IP address is assigned to the client . **Scenario:** This issue occurred when more than one Ethernet port of an AP were connected to a switch. This issue was observed in RAP-3WN test access point running ArubaOS 6.5.1.2.	AP Datapath	RAP-3WN test access points	ArubaOS 6.5.1.2	ArubaOS 6.5.4.5
160308 161434	**Symptom:** A controller crashed and rebooted unexpectedly. The log file listed the reason for the event as **Nanny rebooted machine - low on free memory (Intent:cause:register 34:86:0)**. The fix ensures that the controller has enough memory to work as expected. **Scenario:** This issue occurred when a controller was low on memory. This issue was observed in controllers running ArubaOS 6.4.4.12 or later versions.	Controller-Datapath	All platforms	ArubaOS 6.4.4.12	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
160492 168039 171523	**Symptom:** Users were unable to connect to VIA. The fix ensures that users connect to VIA. **Scenario:** This issue occurred when a controller sent an incorrect value for **NAS-Port-Type** for VIA web authentication. This issue was observed in controllers running ArubaOS 6.5.3.0.	RADIUS	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
160854	**Symptom:** A voice client failed to pass traffic because it did not receive an ARP response. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue occurred when CAC and aggregation were enabled on voice clients. This issue was observed in controllers running ArubaOS 6.4.4.10 or later versions.	AP-Wireless	All platforms	ArubaOS 6.4.4.10	ArubaOS 6.5.4.5
161049	**Symptom:** The **tx-power** resolution values were inconsistent in the **RADIO_STATS** AMON message. The fix ensures that the **tx-power** resolution values are consistent. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.2.0 or later versions.	ARM	All platforms	ArubaOS 6.5.2.0	ArubaOS 6.5.4.5
161366	**Symptom:** An AP failed to respond and rebooted unexpectedly. The log file listed the reason for this event as **SAPD: Unable to contact switch: HELLO-TIMEOUT**. Enhancements made to the Ethernet driver resolved this issue. **Scenario:** This issue occurred when the Rx traffic was halted because of an error condition. This issue was observed in 220 Series access points running ArubaOS 6.4.4.12 or later versions.	AP-Wireless	220 Series access points	ArubaOS 6.4.4.12	ArubaOS 6.5.4.5
162021 167981	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Assertion failed! (pdev->ar_rx_ops->attn_msdu_done(rx_desc)):htt_rx_debug**. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue was observed in access points running ArubaOS 6.5.2.0.	AP-Wireless	All platforms	ArubaOS 6.5.2.0	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
162038 166923	**Symptom:** The output of the **show ap debug system-status** command displayed incorrect speed and duplex information. However, the output of the **show ap debug port status** command displayed the correct information. The fix ensures that the output of the **show ap debug system-status** command displays the correct speed and duplex information. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.3.0 or later versions.	AP-Platform	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
162527	**Symptom:** Some access points falsely detected a radar event and changed the channel on the radio. The fix ensures that APs do not detect false radar events and work as expected. **Scenario:** This issue was observed in AP-134 and AP-135 access points running ArubaOS 6.4.4.12 or later versions.	AP-Platform	AP-134 or AP-135 access points	ArubaOS 6.4.4.12	ArubaOS 6.5.4.5
162561	**Symptom:** An AP showed reduced performance. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue occurred when an AP attempted to retransmit packets with missing frames. This issue was observed in 320 Series access points running ArubaOS 6.5.1.5 or later versions.	AP-Wireless	320 Series access points	ArubaOS 6.5.1.5	ArubaOS 6.5.4.5
162605	**Symptom:** A client was active on two APs at the same time. The fix ensures that an AP ages out the client entry from its user table. **Scenario:** This issue occurred when a client roamed from one AP to another AP that terminated on a different controller and one of the APs failed to age out the client entry from its user table. This issue was observed in 200 Series access points running ArubaOS 6.5.3.4 or later versions.	AP-Wireless	220 Series access points	ArubaOS 6.5.3.4	ArubaOS 6.5.4.5
162735	**Symptom:** The **datapath** process in a controller panicked and the controller rebooted unexpectedly. The fix ensures that the controller works as expected. **Scenario:** This issue occurred because of packet-metadata corruption like invalid packet reference-count or invalid ingress-CPU information. This issue was observed in controllers running ArubaOS 6.5.4.0.	Controller-Platform	All platforms	ArubaOS 6.5.4.0	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
162870	**Symptom:** A client experienced slow connection when an AP used a 4G modem for uplink. The fix ensures that the clients get an improved connection speed. **Scenario:** This issue occurred when the driver in some 4G modems corrupted the packets in the AP. This issue was observed in AP-203R, AP-203RP, AP-205, and AP-205H access points running ArubaOS 6.5.3.0.	AP-Platform	AP-203R, AP-203RP, AP-205, or AP-205H access points	ArubaOS 6.5.4.0	ArubaOS 6.5.4.5
162977 167907	**Symptom:** Incorrect roles were applied to a client after authentication. The fix ensures that the correct roles are applied. **Scenario:** This issue was observed in bridge users connected to the APs running ArubaOS 6.3.1.20 or later versions	Base OS Security	All platforms	ArubaOS 6.3.1.20	ArubaOS 6.5.4.5
162993 172569	**Symptom:** The database synchronization between a master and standby controller failed. The fix ensures that database synchronization works as expected. **Scenario:** This issue occurred when TLS v1.2 was enabled in SSL protocol of a web server profile. This issue was not limited to any specific controller model or ArubaOS version.	Database	All platforms	ArubaOS 6.5.4.3	ArubaOS 6.5.4.5
163066	**Symptom:** A controller rebooted unexpectedly. The log file listed the reason s for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. The fix ensures that the controller works as expected. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.0.3 or later versions.	Controller-Datapath	All platforms	ArubaOS 6.5.0.3	ArubaOS 6.5.4.5
163093	**Symptom:** A controller crashed and rebooted unexpectedly. The log file listed the reason for the event as **Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:0)**. The fix ensures that the controller works as expected. **Scenario:** This issue occurred due to a race condition. This issue was observed in controllers running ArubaOS 6.4.3.2 or later versions.	Controller-Platform	All platforms	ArubaOS 6.4.3.2	ArubaOS 6.5.4.5
163547	**Symptom:** An AP displayed the **anul_get_max_amsdu_size(2126): WARN: AMSDU size is not explicitly configured** warning message. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue was observed in access points running ArubaOS 6.5.1.5.	AP-Wireless	All platforms	ArubaOS 6.5.1.5`	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
163617	**Symptom:** The **datapath** process in a controller crashed and the controller rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:60)**. The fix ensures the **WebCC** process processes the URL and the controller works as expected. **Scenario:** This issue occurred because of an invalid character in the client's URL. This issue was observed in controllers running ArubaOS 6.4.4.12 or later versions.	Controller-Datapath	All platforms	ArubaOS 6.4.4.12	ArubaOS 6.5.4.5
163973	**Symptom:** A wired user was not assigned the correct role after the user completed 802.1X authentication. This issue is resolved by assigning the correct role to wired users if the role changes and the user is not assigned an L3 role. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.1.7 or later versions.	Base OS Security	All platforms	ArubaOS 6.5.1.7	ArubaOS 6.5.4.5
164090 166976 168170 169670 174706	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue was observed in access points running ArubaOS 6.5.3.2.	AP-Wireless	All platforms	ArubaOS 6.5.3.2	ArubaOS 6.5.4.5
164388	**Symptom:** The **System** LED in an AP was lit solid amber although power restriction was not applied to the AP. The fix ensures that the **System** LED in an AP lights: ■ solid amber when restricted power mode (802.3AF PoE or IPM) without network restriction is applied to the AP ■ flashing amber when restricted power mode (802.3AF PoE or IPM) with network restriction (uplink negotiated in sub-optimal speed) is applied to the AP ■ solid green when neither power restriction nor network restriction is applied to the AP **Scenario:** This issue occurred when IPM was enabled in an AP. This issue was observed in access points running ArubaOS 6.5.3.1.	AP-Platform	All platforms	ArubaOS 6.5.3.1	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
164517 164803 166690	**Symptom:** A controller did not list the users in in bridge mode. The fix ensures that the **channel_pwr_change** flag is cleared. **Scenario:** This issue occurred when the **SAPM** process in a controller did not send the ACL configuration to an AP. This issue was observed in controllers running ArubaOS 6.5.1.3.	AP Datapath	All platforms	ArubaOS 6.5.1.3	ArubaOS 6.5.4.5
164543 168530 168773 168823 172724 172817 174044	**Symptom:** A client was unable to connect to an SSID. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue occurred when an AP failed to respond to 802.11 authentication requests. This issue was observed in 300 Series access points running ArubaOS 6.5.3.0 or later versions.	AP-Wireless	300 Series access points	ArubaOS 6.5.3.1	ArubaOS 6.5.4.5
164607 169102 169316	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: L2 single-bit error detected**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred because of memory corruption. This issue was observed in 320 Series access points running ArubaOS 6.5.4.0 or later versions.	AP-Wireless	320 Series access points	ArubaOS 6.5.4.0	ArubaOS 6.5.4.5
164659	**Symptom:** The output of the **show ap debug dot11r efficiency** command displayed 0% as the value in the **Hit (%)** and **Miss (%)** columns. The fix ensures that the CLI output displays the correct values. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.3.0 or later versions.	Station Management	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
164993 168818	**Symptom:** A controller displayed the status of an IAP-VPN branch as **DOWN** although the IAP displayed the status of the same IAP-VPN branch as **UP**. The fix ensures that the controller displays the correct status of an IAP-VPN branch. **Scenario:** This issue occurred in an unstable network when two IAPs, which used dynamic inner IP address pool or static inner IP address, came up as master IAPs in the same swarm and established VPN connections with a controller. When the network stabilized, one master IAP rebooted to rejoin the swarm as a slave IAP but the **IAPMgr** process in the controller displayed the status of the IAP-VPN branch as **DOWN**. This issue was observed in controllers running ArubaOS 6.4.4.11 or later versions.	Remote AP	All platforms	ArubaOS 6.4.4.11	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
165349	**Symptom:** A client was unable to connect to an AP. This issue is resolved by using the cached MAC address of the new active controller instead of the striping IP address. **Scenario:** This issue occurred during a HA failover under the under the following conditions: ■ The network topology included APs with hardware offload capability ■ The HA active and standby controllers were in the same subnet ■ The same striping IP address was configured between controllers ■ The AP and the controllers were in the same subnet. This issue was observed in controllers running ArubaOS 6.5.2.0.	AP Datapath	All platforms	ArubaOS 6.5.2.0	ArubaOS 6.5.4.5
165366	**Symptom:** A wrong IP address was assigned to a client. This issue is resolved by adding DHCP-based UDR support for IP mobility when a mobility service is not provided to the client. **Scenario:** This issue occurred when DHCP-based VLAN derivation was configured with invalid L3 mobility and the **no mobile-ip** parameter was enabled in the WLAN Virtual AP profile. This issue was observed in 7200 Series controllers running ArubaOS 6.4.4.10 or later versions	Mobility	7200 Series controllers	ArubaOS 6.4.4.10	ArubaOS 6.5.4.5
165384	**Symptom:** The user role of clients changed to an initial role unexpectedly. The fix ensures that a correct user role is assigned to clients. **Scenario:** This issue occurred when a local controller failed and the AP switched to the master controller. The clients connected to the AP were de-authenticated and assigned the initial role. This issue was observed in 200 Series, 210 Series, and 220 Series access points running ArubaOS 6.4.4.14 or later versions.	AP-Wireless	200 Series, 210 Series, or 220 Series access points	ArubaOS 6.4.4.14	ArubaOS 6.5.4.5
165595	**Symptom:** A controller displayed the following error messages: ■ **Unexpected stm (Station management) runtime error at wifi_ refresh_assoc_drv** ■ **An internal system error has occurred at file messenger.c function msgr_vap_stats_v2 line 5267 error msgr_vap_stats_v2** The fix ensures that the controller does not display these error messages. **Scenario:** This issue occurred when a backup Virtual AP was configured for an AP. This issue was observed in controllers running ArubaOS 6.5.3.0.	Air Management-IDS	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
165668 166189	**Symptom:** An existing client lost its IP address and a new client was unable to obtain an IP address. The fix ensures that an existing client retains its IP address and a new client receives an IP address. **Scenario:** This issue occurred when wired devices were connected to a Remote AP. This issue was observed in RAP-3WNP and RAP-155 access points running ArubaOS 6.5.2.0.	AP Datapath	RAP-3WNP or RAP-155 access points	ArubaOS 6.5.2.0	ArubaOS 6.5.4.5
165713 163795	**Symptom:** False radar events were detected on APs. Enhancements made to the radar detection algorithm resolved this issue. **Scenario:** This issue was observed in AP-225 access points running ArubaOS 6.4.4.12 or later versions.	AP-Wireless	AP-225 access points	ArubaOS 6.4.4.12	ArubaOS 6.5.4.5
165900 171831	**Symptom:** An ARP entry was not displayed for wired users. The fix ensures that the ARP entry is displayed. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.3.0.	Controller-Platform	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
165903	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Crash [02] : 0x009A5AE7**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred because of a firmware assert event in rate control. This issue was observed in AP-314 access points running ArubaOS 6.5.1.7.	AP-Wireless	AP-314 access points	ArubaOS 6.5.1.7	ArubaOS 6.5.4.5
166007 167633	**Symptom:** An AP took a longer time to process the configuration after a failover. This delayed the reconnection of a client with the AP. The fix ensures that the AP processes the configuration faster after a failover. **Scenario:** This issue was observed in AP-305 access points running ArubaOS 6.5.1.7.	AP-Platform	AP-305 access points	ArubaOS 6.5.1.7	ArubaOS 6.5.4.5
166154	**Symptom:** A user observed inconsistent GRE headers in DNS packets sent by Apple devices. This issue is resolved by not setting the flags in the GRE header for statically configured GRE tunnels with keepalive disabled. **Scenario:** This issue was observed in controllers where GRE tunnels were statically configured and keepalive was disabled. This issue was observed in controllers running ArubaOS 6.5.0.3.	Controller-Datapath	All platforms	ArubaOS 6.5.0.3	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
166183 169183	**Symptom:** An AP did not boot. When the AP was manually rebooted, it displayed the **bcm96xxx-wdt ff800428.watchdog: Watchdog timer stopped** message in the console log. The fix ensures that the AP boots correctly. **Scenario:** This issue was observed in access points running ArubaOS 6.5.3.1.	AP-Platform	All platforms	ArubaOS 6.5.3.1	ArubaOS 6.5.4.5
166228 168270	**Symptom:** A user was unable to connect to a wireless network because a controller was unresponsive. The fix ensures that users are able to connect to the Wi-Fi network. **Scenario:** This issue occurred when a specific type of Google cast query was sent to a controller. This issue was observed in controllers running ArubaOS 6.4.4.10.	AirGroup	All platforms	ArubaOS 6.4.4.10	ArubaOS 6.5.4.5
166268	**Symptom:** A controller failed to establish SSL connection with a Palo Alto Networks (PAN) firewall server. The log file listed the reason for the event as **SSL Alert (Level: Fatal, Description: Bad Record MAC)**. This issue is resolved by setting FIPS mode in OpenSSL **Scenario:** This issue occurred when the **Extifmgr** process used FIPS-mode OpenSSL. This issue was observed in controllers running ArubaOS 6.5.0.4-FIPS or later versions.	Base OS Security	All platforms	ArubaOS 6.5.0.4-FIPS	ArubaOS 6.5.4.5
166676 167114 167869 168338 169127 172795 172859 173325	**Symptom:** An AP incorrectly advertised HT information elements in the beacons though the **high-throughput-enable** parameter was disabled in the radio profile. The fix ensures that the HT information elements are advertised only when HT is enabled in the radio profile. **Scenario:** This issue occurred when the **high-throughput-enable** parameter was disabled in the **rf dot11g-radio-profile** command. This issue was observed in 200 Series, AP-205H, AP-207, 210 Series, 220 Series, AP-228, 270 Series, and AP-277 access points running ArubaOS 6.5.3.4.	Controller-Platform	200 Series, AP-205H, AP-207, 210 Series, 220 Series, AP-228, 270 Series, or AP-227 access points	ArubaOS 6.5.3.4	ArubaOS 6.5.4.5
166678	**Symptom:** A remote AP authenticated a wired client without any credential check. This issue is resolved by deleting all remote AP users with the same MAC address if they are wired clients and their ports are changed. **Scenario:** This issue occurred when a wired client that used a spoofed MAC address of an authenticated client was connected to a remote AP. This issue was observed in remote access points running ArubaOS 6.5.0.3.	Base OS Security	All platforms	ArubaOS 6.5.0.3	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
166755	**Symptom:** Clients disassociated from a dual radio AP. The fix ensures that the clients do not disassociate when the other radio switches modes. **Scenario:** This issue occurred when a client was connected to one radio and the other radio switched between spectrum monitor mode and AP mode. This issue was observed in access points running ArubaOS 6.4.4.12 or later versions.	Station Management	All platforms	ArubaOS 6.4.4.12	ArubaOS 6.5.4.5
166838	**Symptom:** The output of the **show ap debug radio-stats** command displayed incorrect values for Tx data bytes and Rx data bytes. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-305 access points running ArubaOS 6.5.3.0.	AP-Wireless	AP-305 access points	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
166865 169423	**Symptom:** The output of the **show ap debug radio-stats** command displayed incorrect values for Tx data bytes and Rx data bytes. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-207 access points running ArubaOS 6.5.3.0.	AP-Wireless	AP-207 access points	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
166945	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Fatal exception**. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-224 access points running ArubaOS 6.4.4.12	AP-Wireless	AP-224 access points	ArubaOS 6.4.4.12	ArubaOS 6.5.4.5
166963 167520 167719 171713	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **Broken heartbeat tunnel**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in AP-203H and AP-207 access points ArubaOS 6.5.1.6 or later versions.	AP Datapath	AP-203H or AP-207 access points	ArubaOS 6.4.4.12	ArubaOS 6.5.4.5
167045 169550	**Symptom:** The **authentication** process in a controller crashed and the WebUI of the controller was inaccessible. The fix ensures that **authentication** process works as expected. **Scenario:** This issue occurred when the **show global-usertable** command was executed. This issue was observed in controllers running ArubaOS 6.5.1.3 or later versions in a master-local topology.	Base OS Security	All platforms	ArubaOS 6.5.1.3	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
167056	**Symptom:** The **Remote Intf** column in the output of the **show ap lldp neighbors** command incorrectly displayed the port description instead of the port ID. The issue is resolved by: ■ Providing port ID and port descriptions in separate columns for the APs. ■ Displaying only the port ID for the controllers. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.4.6 or later versions.	LLDP	All platforms	ArubaOS 6.4.4.6	ArubaOS 6.5.4.5
167070	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - at aruba_mesh_am_hook_entrance ()**. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue was observed in access points running ArubaOS 6.5.1.7.	AP-Wireless	All platforms	ArubaOS 6.5.1.7	ArubaOS 6.5.4.5
167089	**Symptom:** A controller crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:2c)**. The fix ensures that the controller works as expected. **Scenario:** This issue was observed in 7205 controllers running ArubaOS 6.5.3.0.	Controller-Datapath	7205 controllers	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
167098 167373 169128 169709 173867	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Take care of the HOST ASSERT first**. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue was observed in access points running ArubaOS 6.5.4.0 or later versions.	AP-Wireless	AP-303H and AP-365 access points	ArubaOS 6.5.4.0	ArubaOS 6.5.4.5
167111	**Symptom:** Clients were unable to pass traffic although they received an IP address from the correct VLAN. The fix ensures that the clients can pass traffic as expected. **Scenario:** This issue occurred when the netdestination configurations were updated. This issue was observed in controllers running ArubaOS 6.5.3.0 or later versions.	Base OS Security	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
167229 167548 167864 168537 168972 169050 169199 169563 170137 170202 170252 170431 170522 170786 170823 170914 171189 171499 171697 171919 171935 172894 172897 172932 172958 172961 173211 173333 173497 173770 174120 174124 174720	**Symptom:** An AP rebooted unexpectedly. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue occurred because of memory corruption. This issue was observed in access points running ArubaOS 6.5.3.3.	AP-Wireless	All platforms	ArubaOS 6.5.3.3	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
167418 167550 167957 168626 168634 169027 169159 169278 169681 169909 170922 171101 171103 171726 172951 172987 173031 173338 173359 173414 173443 173465	**Symptom:** A controller rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the controller works as expected. **Scenario:** This issue occurred when DPI was disabled. This issue was observed in controllers running ArubaOS 6.5.3.1 in a master-local topology.	Controller-Datapath	All platforms	ArubaOS 6.5.3.1	ArubaOS 6.5.4.5
167479 167829	**Symptom:** A controller rebooted unexpectedly and did not generate a core dump file. The fix ensures that the controller generates a core dump file when it reboots. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.3.0.	Controller-Platform	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
167706	**Symptom:** A controller crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the controller does not crash and works as expected. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.4.0.	Controller-Datapath	All platforms	ArubaOS 6.5.4.0	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
167747 171565 172711	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Unable to handle kernel NULL pointer dereference at virtual address**. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue occurred when debug logging and core dump generation were halted. This issue was observed in AP-325 access points running ArubaOS 6.5.3.0.	AP-Wireless	AP-325 access points	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
167812	**Symptom:** A user was not able to view a Google Chromecast or Apple TV devices. The fix ensures that an AirGroup shared-user-list is case insensitive. **Scenario:** This issue occurred when the AirGroup shared-user-list had the same letter case (uppercase or lowercase). This issue was observed in controllers running ArubaOS 6.5.1.5.	AirGroup	AP-325 access points	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
167825 167826 171609	**Symptom:** A controller crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:2c)**. The fix ensures that the controller does not crash and works as expected. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.3.2 or later versions.	Controller-Datapath	All platforms	ArubaOS 6.5.3.2	ArubaOS 6.5.4.5
167919	**Symptom:** A scanner declined the action frames sent by APs, resulting in poor wireless performance. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-228 access points running ArubaOS 6.4.4.6 or later versions.	AP-Wireless	AP-228 access points	ArubaOS 6.4.4.6	ArubaOS 6.5.4.5
168031	**Symptom:** The crash log from a controller had incomplete core dumps. The fix ensures that the crash log contains the complete dump information. **Scenario:** This issue occurred when a controller crashed and generated a crash log. This issue was observed in controllers running ArubaOS 6.5.3.2.	Controller-Platform	All platforms	ArubaOS 6.5.3.2	ArubaOS 6.5.4.5
168052	**Symptom:** An SSH connection to a controller failed. The fx ensures that the SSH connection succeeds. **Scenario:** This issue occurred when the cumulative length of the SSH username and password exceeded 28 characters. This issue was observed in controllers running ArubaOS 6.5.3.1.	Authentication	All platforms	ArubaOS 6.5.3.1	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
168069 163041	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **AP rebooted due to loss power**. The fix ensures that the AP checks if the link partner is 802.3BZ capable before attempting auto-negotiation. **Scenario:** This issue occurred when a link partner was not capable of 802.3BZ or when the AP did not auto-negotiate 5000BASE-T with a third party switch. This issue is observed in AP-335 access points running ArubaOS 6.5.3.0 or later versions.	AP-Platform	AP-335 access points	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
168079 168813	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Fatal exception in interrupt**. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-325 access points running ArubaOS 6.5.3.0.	AP-Wireless	AP-325 access points	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
168157 170007 173928 174042	**Symptom:** The output of the **show ap mesh active** command displayed a mesh portal as working in 2.4 GHz mode and the mesh point EIRP and maximum EIRP values as 0 although the flex-radio mode in the **ap system-profile** was configured as **2.4GHz-and-5GHz**. The fix ensures that the mesh portal works in configured mode and the output of the command displays the correct EIRP and maximum EIRP values. **Scenario:** This issue was observed in access points running ArubaOS 6.4.4.16.	Mesh	All platforms	ArubaOS 6.4.4.16	ArubaOS 6.5.4.5
168485 171167	**Symptom:** The AeroScout Location Engine was not able to receive Wi-Fi tags from the server. The fix ensures that the AeroScout Location Engine receive Wi-Fi tags from the server. **Scenario:** This issue occurred when the AP firewall blocked the UDP port 1144. This issue was observed in access points running ArubaOS 6.5.3.0 or later versions.	AP-Platform	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
168499 168711	**Symptom:** The ARM feature did not work in an AP. The fix ensures that the ARM feature works as expected. **Scenario:** This issue occurred when an AP, in APM mode, scanned the 40 MHz and a difference between the operating bandwidth and the configured bandwidth pushed the AP out of APM mode. This issue was observed in APs running ArubaOS 6.5.3.1.	ARM	All platforms	ArubaOS 6.5.3.1	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
168795	**Symptom:** A WebCC URL cloud look-up failed in a controller. The log file listed the reason for the event as **<ERRS> |web_cc| web_cc_callback: URL lookup failed**. The fix ensures that the WebCC URL cloud look-up succeeds in a controller. **Scenario:** This issue occurred when WebCC was enabled on a controller. This issue was observed in controllers running ArubaOS 6.5.3.0 or later versions.	WebCC	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
168909 171735 172218	**Symptom:** The noise floor value in a DFS channel was higher than expected. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue occurred when ARM scanning was enabled in an AP. This issue was observed in AP-315 and AP-335 access points running ArubaOS 6.5.3.3.	AP-Wireless	AP-315 or AP-335 access points	ArubaOS 6.5.3.3	ArubaOS 6.5.4.5
168971 169581 169880	**Symptom:** An AP failed to respond and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Fatal exception in interrupt**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in AP-303H, 300 Series, 310 Series, 320 Series, 330 Series, and 360 Series access points running ArubaOS 6.5.3.0.	Mesh	AP-303H, 300 Series, 310 Series, 320 Series, 330 Series, and 360 Series access points	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
169010 169073 173778	**Symptom:** An AP failed to respond and rebooted unexpectedly. The log file listed the reason for the event as **Unhandled fault: external abort on nonlinefetch (0x1008) at 0xe6000000**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in 300 Series access points running ArubaOS 6.5.3.0.	AP-Platform	300 Series access points	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
169029	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **panic-dump.apkys-invrec-pnt.2017-09-07_21-13-04**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in AP-275 access points running ArubaOS 6.5.3.1.	Mesh	AP-275 access points	ArubaOS 6.5.3.1	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169131 170473 171299 171823	**Symptom:** AppRF failed to block traffic. The fix ensures that AppRF blocks the desired traffic. **Scenario:** This issue occurred when DPI and WebCC were enabled in a controller. This issue was observed in 7200 Series controllers running ArubaOS 6.4.4.15 or later versions.	Controller-Datapath	7200 Series controllers	ArubaOS 6.4.4.15	ArubaOS 6.5.4.5
169288	**Symptom:** A log file displayed the **An internal system error has occurred at file aeroscout.c function rtls_send_message line 190 error sendto failed -e-101 l-74 ip-192.168.20.100 port-27425** error although an AP could reach an RTLS server. The fix ensures that the error is not displayed incorrectly. **Scenario:** This issue was observed in access points running ArubaOS 6.5.1.6 or later versions.	Air Management-IDS	All platforms	ArubaOS 6.5.1.6	ArubaOS 6.5.4.5
169474	**Symptom:** Some clients were unable to associate to certain APs. The log file displayed the reason as **AP is resource constrained**. The fix ensures that the clients could connect to the APs. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.4.2 or later versions.	AP-Wireless	All platforms	ArubaOS 6.4.4.2	ArubaOS 6.5.4.5
169494	**Symptom:** A client was not able to connect to an AP. The log file listed the reason for the event as **AP is resource constrained**. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue was observed in access points running ArubaOS 6.5.3.0.	AP-Wireless	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
169522 170177	**Symptom:** An AP failed to supply power through the Power Sourcing Equipment (PSE) port because the port was disabled after a reboot. This fix ensures that an AP reboot does not disable the PSE port. **Scenario:** This issue occurred when: ■ An AP was rebooted using the **apboot** command on the controller. ■ An AP rebooted on its own. This issue was observed in AP-303H access points running ArubaOS 6.5.4.0 or later versions.	AP-Platform	AP-303H access points	ArubaOS 6.5.4.0	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169530	**Symptom:** An Android device took long time to compete WPA Group Temporal Key handshake with an AP. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue occurred when the AP sent WPA GTK to the Android device without encryption. This issue was observed in access points running ArubaOS 6.5.3.1.	AP-Wireless	All platforms	ArubaOS 6.5.3.1	ArubaOS 6.5.4.5
169535	**Symptom:** A client was not unable to view the custom Captive Portal page in the standby controller. The fix ensures that the client can view the custom Captive Portal page in the standby controller. **Scenario:** This issue occurred when a user added a new standby controller which did not have the custom Captive Portal page. This issue was observed in controllers running ArubaOS 6.5.1.7 or later versions in a master-standby topology.	Database	All platforms	ArubaOS 6.4.4.2	ArubaOS 6.5.4.5
169540 170180	**Symptom:** The **Station Management** process in a controller crashed unexpectedly. The fix ensures that the number of Virtual APs is set after checking that the AP is in mesh recovery mode. **Scenario:** This issue occurred when an AP switched to mesh recovery mode and the number of Virtual APs was incorrectly set to maximum number of SSIDs. This issue was observed in controllers running ArubaOS 6.5.3.0.	Controller-Platform	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
169626	**Symptom:** A controller sent an unwanted attribute (FIlter-ID) to a RADIUS server in the interim accounting packets. The fix ensures that RADIUS accounting interim update does not contain Filter-Id attribute for an IPv6 client. **Scenario:** This issue occurred when RADIUS interim accounting was enabled on a controller. This issue was observed in controllers running ArubaOS 6.5.3.4 or later versions.	Radius	All platforms	ArubaOS 6.5.3.4	ArubaOS 6.5.4.5
169819	**Symptom:** The cellular-handoff assist feature was disabled in the WLAN Virtual AP profile when a controller was reloaded. The fix ensures that the cellular-handoff assist feature is not disabled in a controller. **Scenario:** This issue occurred when the **cellular-handoff assist** parameter was erroneously removed from the configuration when a controller reloaded. This issue was observed in controllers running ArubaOS 6.5.3.0.	Configuration	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169973 172425	**Symptom:** The **Station Manager** process in a master controller stopped responding after executing the **clear gap-db stale** command. The fix ensures that the **Station Manager** process works as expected. **Scenario:** This issue occurred when load balancing was enabled. This issue was observed in controllers running ArubaOS 6.4.2.6 or later versions in a cluster topology.	AP-Platform	All platforms	ArubaOS 6.4.2.6	ArubaOS 6.5.4.5
170002	**Symptom:** An AP crashed and rebooted unexpectedly. Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue was observed in 300 Series access points running ArubaOS 6.5.3.3.	AP-Wireless	300 Series access points	ArubaOS 6.5.3.3	ArubaOS 6.5.4.5
170085	**Symptom:** The Tx power value that was configured in the **dot11a-radio-profile** or **dot11g-radio-profile** was lost when a controller was reloaded. The fix ensures that the controller retains the configured Tx power value. **Scenario:** This issue occurred when an AP rejected the configured Tx power value and used the default Tx power value. This issue was observed in access points running ArubaOS 6.5.3.0.	AP-Platform	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
170111	**Symptom:** The **STM** process in a controller stopped responding when a user executed the **clear gab-db stale-ap ap-name** command. The fix ensures that the **STM** process works as expected when the command is executed. **Scenario:** This issue occurred in a cluster topology with load balancing enabled. This issue was observed in controllers running ArubaOS 6.4.4.16 or later versions.	AP-Platform	All platforms	ArubaOS 6.4.4.16	ArubaOS 6.5.4.5
170217 170241 172242 172882 172939 173032 173087	**Symptom:** Some clients were unable to connect to an SSID when 802.11r was enabled on a controller. The fix ensures that the clients successfully connect to the SSID without service interruption. **Scenario:** This issue occurred when the clients attempted a full 802.1X authentication after an 802.11R roam. This issue was observed in controllers running ArubaOS 6.5.3.3 or later versions.	Base OS Security	All platforms	ArubaOS 6.5.3.3	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
170770	**Symptom:** A client was not able to connect to an SSID. The log file listed the reason for the event as **Error: error_no_free_slots.** The issue is resolved by updating the AMON process with the correct IP address and by not publishing the users who are connected in bridge mode. **Scenario:** This issue occurred when the **Authentication** process published the users who were connected in bridge mode and did not clear them. Thus, the assigned capacity was filled and new users were not allowed. This issue was observed in controllers running ArubaOS 6.5.3.0.	Base OS Security	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
170816	**Symptom:** A certificate-based Remote AP failed to come up. The fix ensures that: ■ The Remote AP attempts authentication against all authentication servers that are part of an authentication server group. ■ The Remote AP attempts authentication starting from the first authentication server in the authentication server group if authentication fails. **Scenario:** This issue occurred when a Remote AP failed to authenticate against all authentication servers that were part of an authentication server group. Although authentication failed, the Remote AP stored the name of the last authentication server and attempted other authentication requests against the same server. This issue was observed in controllers running ArubaOS 6.5.3.0.	Certificate Manager	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
170832	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **Fatal exception in interrupt @ ol_rx_flush_ handler+0x40/0x118 [umac] / ol_rx_indication_handler.** Enhancements made to the wireless driver resolved this issue. **Scenario:** This issue was observed in AP-305 access points running ArubaOS 6.5.3.0.	AP-Wireless	AP-305 access points	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
170872 172034 172521 172573	**Symptom:** The **mDNS** process in a controller crashed and the controller rebooted unexpectedly. The fix ensures that the **mDNS** process does not crash and the controller works as expected. **Scenario:** This issue occurred because of memory corruption. This issue was observed in controllers running ArubaOS 6.5.3.3 or later versions.	AirGroup	All platforms	ArubaOS 6.5.3.3	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
170993	**Symptom:** The WebUI displayed a blank page when a user navigated to the **Security > Authentication Servers > RADIUS Server > CPPM Server Group** page and clicked **Show Reference**. The fix ensures that the WebUI displays the correct page. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.3.2.	WebUI	All platforms	ArubaOS 6.5.3.2	ArubaOS 6.5.4.5
171093	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Critical process /aruba/bin/sapd [pid 30240] DIED**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when an adhoc network advertising a valid SSID was detected by the AP under the following configuration conditions: ■ The WMS on master was disabled. ■ The **detect-valid-ssid-misuse** and **protect-ssid** parameters were enabled in the **ids unauthorized-device-profile**. This issue was observed in AP-325 access points running ArubaOS 6.5.3.0.	Air Management-IDS	AP-325 access points	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
171113	**Symptom:** Bandwidth contracts in the target role were not applied to a split tunnel user. The fix ensures that the bandwidth contracts in the target role are applied to a split tunnel user. **Scenario:** This issue occurred when a user used COA to change the role of a split tunnel user. This issue was not limited to any specific access point model or ArubaOS version.	AP Datapath	All platforms	ArubaOS 6.5.4.3	ArubaOS 6.5.4.5
171233	**Symptom:** A site-to-site VPN failed to come up. The fix ensures that the site-to-site VPN comes up as expected. **Scenario:** This issue occurred when the IKE/IPsec security association related to a 32-bit destination network mask was broken but the corresponding datapath route-cache entry was not deleted. This issue was observed in controllers running ArubaOS 6.5.3.3.	IPsec	All platforms	ArubaOS 6.5.3.3	ArubaOS 6.5.4.5
171374 171484 171485 171927	**Symptom:** An AP crashed unexpectedly. The log file listed the reason for the event as **ofald invoked oom-killer: gfp_mask=0x200d2, order=0, oom_adj=0**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in access points running ArubaOS 6.5.3.3.	SDN	All platforms	ArubaOS 6.5.3.3	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171382 174540	**Symptom:** A client that was associated with an AP showed low radio signal strength. The fix ensures that the client gets the correct radio signal strength. **Scenario:** This issue was observed in AP-207 access points running ArubaOS 6.5.1.0 or later versions.	AP-Platform	AP-207 access points	ArubaOS 6.5.1.3	ArubaOS 6.5.4.5
171441	**Symptom**: The **Configuration > Authentication > Advanced** page did not load completely in the WebUI. This issue is resolved by removing the survivability feature from the ArubaOS FIPS version. **Scenario**: This issue occurred because the ArubaOS FIPS version did not support the survivability feature. This issue was observed in controllers running ArubaOS 6.5.3.3.	WebUI	All platforms	ArubaOS 6.5.3.3	ArubaOS 6.5.4.5
171498	**Symptom:** An AP crashed unexpectedly. The log file listed the reason for the event as **AP process crash (core file: core.rapper.18-64-72-cf-e6-62.AP-334.62115)**. The fix ensures the AP works as expected. **Scenario:** This issue occurred when the AP was flooded with VPN requests. This issue was observed in AP-334 and AP-335 access points running ArubaOS 6.5.3.3.	AP-Platform	AP-334 or AP-335 access points	ArubaOS 6.5.3.3	ArubaOS 6.5.4.5
171923	**Symptom:** A client that was connected to the second Ethernet port of an AP in bridge mode was not assigned an IP address and was not able to send or receive traffic. The fix ensures that the client obtains an IP address and can send or receive traffic. **Scenario:** This issue was observed in access points running ArubaOS 6.5.3.0.	AP Datapath	All platforms	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
171976	**Symptom:** The output of the **show ap debug radio-stats** command did not display the correct counter values. The fix ensures that the command output displays the correct values. **Scenario:** This issue occurred when 802.11AC and 802.11N clients were connected to an AP. This issue was observed in AP-207 access points running ArubaOS 6.5.3.3.	AP-Wireless	AP-207 access points	ArubaOS 6.5.3.0	ArubaOS 6.5.4.5
172095	**Symptom:** A crash directory was missing from 7200 Series controller. This issue is resolved by moving all crash-related information to a fixed location. **Scenario:** This issue occurred when a process crashed in a 7200 Series controller. This issue was observed in controllers running ArubaOS 6.5.3.3 or later versions.	Controller-Platform	7200 Series controllers	ArubaOS 6.5.3.3	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
172102	**Symptom:** The **Station Management** process in a controller crashed unexpectedly. The fix ensures that **Station Management** process does not crash and the controller works as expected. **Scenario:** The issue was observed in controllers running ArubaOS 6.5.1.5.	UCC	All platforms	ArubaOS 6.5.1.5	ArubaOS 6.5.4.5
172243	**Symptom:** Although LLDP-MED configuration was enabled on all ports of an AP, ports E1 through E3 were disabled. The fix ensures that ports E1 through E3 are enabled. **Scenario:** This issue was observed in AP-303H access points running ArubaOS 6.5.3.4 or later versions.	AP-Platform	AP-303H access points	ArubaOS 6.5.3.4	ArubaOS 6.5.4.5
172468	**Symptom:** A client failed authentication against a RADIUS server. Enhancements made to the **authentication** process resolved this issue. **Scenario:** This issue occurred when the **authentication** process in a controller could not assign a sequence-number to a RADIUS request. As a result, the controller did not sent RADIUS requests to the RADIUS server. This issue was observed in controllers running ArubaOS 6.5.3.3.	RADIUS	All platforms	ArubaOS 6.5.3.3	ArubaOS 6.5.4.5
172665	**Symptom:** A controller did not clear the stale internal-user entries of IPsec tunnels from an HP switch. The controller displayed the **user delete for HP switches is not supported** error when a user issued the **aaa user delete** command. The fix ensures that the stale internal-user entries can be deleted. **Scenario:** This issue occurred when a controller included HP switch users as trusted users but omitted them from ageout user deletion. The HP switch users were retained as stale internal-user entries even after IPsec sessions between the user and the controller were terminated. This issue was observed in controllers running ArubaOS 6.5.2.0.	IPsec	All platforms	ArubaOS 6.5.2.0	ArubaOS 6.5.4.5
172788	**Symptom:** The SNMP OID **monAPInfoMonitorTime - 1.3.6.1.4.1.14823.2.2.1.6.7.1.1.1.6** showed all zeroes. This issue is resolved by using an improved monitoring start time to generate the correct OID. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.4.16.	Air Management-IDS	All platforms	ArubaOS 6.4.4.16	ArubaOS 6.5.4.5
172877	**Symptom:** A controller rebooted unexpectedly. The log file listed the reason for the event as **datapath timeout**. The fix ensures that the controller works as expected. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.1.8.	Controller-Datapath	All platforms	ArubaOS 6.5.1.8	ArubaOS 6.5.4.5

Table 3: *Resolved Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
172957 173225	**Symptom:** Clarity live data was not populated in a AirWave server. The fix ensures that the AP does not set the AMON header source IP address. **Scenario:** The issue occurred when an AP set the AMON header source IP address as the VRRP IP address. Hence AirWave did not update clarity live data. This issue was observed in controllers running ArubaOS 6.5.4.0.	Controller-Datapath	All platforms	ArubaOS 6.5.4.0	ArubaOS 6.5.4.5
173134	**Symptom:** The **Datapath** process in a controller crashed and the controller rebooted unexpectedly. The fix ensures that the **Datapath** process does not crash and the controller works as expected. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.4.0.	Controller-Datapath	All platforms	ArubaOS 6.5.4.0	ArubaOS 6.5.4.5
173230	**Symptom:** A remote AP rebooted intermittently. The log file listed the reason for the event as **Missed heartbeats**. The fix ensures that the remote AP works as expected. **Scenario:** This issue occurred when the Tx queue in the **IPsec** process was stuck. This issue was observed in RAP-155 remote access points running ArubaOS 6.5.3.1.	AP-Platform	RAP-155 remote access points	ArubaOS 6.5.3.1	ArubaOS 6.5.4.5
173594	**Symptom:** A controller showed high CPU utilization. This issue is resolved by moving SAE error messages under debug. **Scenario:** This issue occurred when SAE error messages were printed. This issue was observed in 7280 controllers running ArubaOS 6.5.4.0 or later versions.	Controller-Datapath	7280 controllers	ArubaOS 6.5.4.0	ArubaOS 6.5.4.5
174017	**Symptom:** The **halt** command did not work in a controller. The fix ensures that the **halt** command works as expected. **Scenario:** This issue occurred when the Tx queue in the **IPsec** process was stuck. This issue was observed in controllers running ArubaOS 6.5.3.4 or earlier versions.	Controller-Platform	All platforms	ArubaOS 6.5.3.4	ArubaOS 6.5.4.5
174864 175413 175448 175549	**Symptom:** A controller crashed and rebooted unexpectedly. The log file listed the reason for the event as **datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. The fix ensures that the controller does not crash and works as expected. **Scenario:** This issue was observed in controllers running ArubaOS 6.5.3.4 in a master-local topology.	Controller-Datapath	All platforms	ArubaOS 6.5.3.4	ArubaOS 6.5.4.5

This chapter describes the known and outstanding issues identified in ArubaOS 6.5.4.5.

Table 4: *Known Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version
148172	**Symptom:** A user cannot create VLANs as **Trusted** in a BOC interface. **Scenario:** This issue is observed in 7200 Series controllers running ArubaOS 6.5.0.0 in a master-branch topology. **Workaround:** None.	WebUI	7200 Series controllers	ArubaOS 6.5.0.0
154625 155709 155894 156383 158536 161789	**Symptom:** The VRRP state changes although heartbeats are not missed. **Scenario:** This issue occurs when a standby controller inadvertently transitions to master state because the master controller delays the processing of VRRP advertisements. This issue is observed in controllers running ArubaOS 6.5.0.3 in a local-master topology. **Workaround:** Disable debug logs and syslog server. Increase the advertisement interval.	Controller-Platform	All platforms	ArubaOS 6.5.0.3
156406	**Symptom:** A client, which connects to an AP in bridge mode, does not obtain an IP address. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.0.3. **Workaround:** None.	Management Authentication and User Rights	All platforms	ArubaOS 6.5.0.3
161655	**Symptom:** Some of the high-frequency radio statistics such as tx_time, rx_time, and rx_clear are not collected correctly per beacon period on some APs. **Scenario:** This issue is observed in access points running ArubaOS 6.5.2.0. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 6.5.2.0
165943	**Symptom:** The **Dashboard** page in the WebUI does not display the correct country information. **Scenario:** This issue is observed when **ip access-list geolocation global-geolocation-acl** is configured in a controller. This issue is observed in controllers running ArubaOS 6.5.3.1. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 6.5.3.1

Table 4: *Known Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version
166426 167050 170409	**Symptom:** A master and standby controller reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.1.9 in a master-standby topology. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.5.1.9
168789	**Symptom:** An AP with a 802.1X supplicant configuration fails to boot. **Scenario:** This issue occurs when an ACL denies DNS response from DNS server. This issue is observed in access points running ArubaOS 6.5.4.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 6.5.4.0
169184	**Symptom:** A controller does not send SYN packets for IPv6 VLANs in decrypt decrypt-tunnel and tunnel forwarding mode for the following ports: ■ SMTP ports 25 and 587 ■ Jabber port 5222 ■ SMB ports 445, 139, and so on **Scenario:** This issue is observed in controllers running ArubaOS 6.5.1.4. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.5.1.4
169622	**Symptom:** A syslog server reports the **aruba_change_channel 512 channel 6 mode 3 not found** error for some APs. **Scenario:** This issue is observed in AP-314 and AP-315 access points running ArubaOS 6.5.1.5. **Workaround:** None.	AP-Wireless	AP-314 or AP-315 access points	ArubaOS 6.5.1.5
170037 170055	**Symptom:** An AP does not discover a master controller through ADP. **Scenario:** This issue occurs when a static IP address is configured in an AP and the ACL denies ADP packets. This issue is observed in access points running ArubaOS 6.5.4.2. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 6.5.4.2

Table 4: *Known Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version
171896	**Symptom:** APs terminating on a controller in a HA topology come up with dirty configuration state (Indicated by **ID** flag). **Scenario:** This issue occurs under the following conditions: ■ HA over subscription is enabled in a controller. ■ CPsec is enabled in a controller. ■ The count of APs terminating on a standby controller exceeds twice the supported platform limit. This issue is observed in controllers running ArubaOS 6.5.1.9. **Workaround:** None.	Controller-Datapath	7200 Series controllers	ArubaOS 6.5.1.9
172390	**Symptom:** A branch controller loses the GRE tunnel destination IP address. **Scenario:** This issue occurs when a branch controller, which is manually configured with the IP address of a master controller, is rebooted. The IP address of the master controller is mapped with a FQDN but fails to resolve during the branch controller reboot. This issue is observed in controllers running ArubaOS 6.5.3.3. **Workaround:** None.	GRE	All platforms	ArubaOS 6.5.3.3
172506	**Symptom:** A controller discards the first TCP SYN packet when a client connects to a FTP server. **Scenario:** This issue occurs in a controller where DPI is enabled. This issue is observed in controllers running ArubaOS 6.4.4.14. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.4.4.14
173328	**Symptom:** A user cannot configure **block-redirect-url** on a standby controller. **Scenario:** This issue is observed in a standby controller running ArubaOS 6.5.4.2 in a master-standby topology. **Workaround:** None.	DPI	All platforms	ArubaOS 6.5.4.2

This chapter describes the known and outstanding issues identified in ArubaOS 6.5.4.5.

Table 5: *Known Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version
148172	**Symptom:** A user cannot create VLANs as **Trusted** in a BOC interface. **Scenario:** This issue is observed in 7200 Series controllers running ArubaOS 6.5.0.0 in a master-branch topology. **Workaround:** None.	WebUI	7200 Series controllers	ArubaOS 6.5.0.0
154625 155709 155894 156383 158536 161789	**Symptom:** The VRRP state changes although heartbeats are not missed. **Scenario:** This issue occurs when a standby controller inadvertently transitions to master state because the master controller delays the processing of VRRP advertisements. This issue is observed in controllers running ArubaOS 6.5.0.3 in a local-master topology. **Workaround:** Disable debug logs and syslog server. Increase the advertisement interval.	Controller-Platform	All platforms	ArubaOS 6.5.0.3
156406	**Symptom:** A client, which connects to an AP in bridge mode, does not obtain an IP address. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.0.3. **Workaround:** None.	Management Authentication and User Rights	All platforms	ArubaOS 6.5.0.3
161655	**Symptom:** Some of the high-frequency radio statistics such as tx_time, rx_time, and rx_clear are not collected correctly per beacon period on some APs. **Scenario:** This issue is observed in access points running ArubaOS 6.5.2.0. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 6.5.2.0
165943	**Symptom:** The **Dashboard** page in the WebUI does not display the correct country information. **Scenario:** This issue is observed when **ip access-list geolocation global-geolocation-acl** is configured in a controller. This issue is observed in controllers running ArubaOS 6.5.3.1. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 6.5.3.1
166426 167050 170409	**Symptom:** A master and standby controller reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. **Scenario:** This issue is observed in controllers running ArubaOS 6.5.1.9 in a master-standby topology. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.5.1.9

Table 5: *Known Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version
168789	**Symptom:** An AP with a 802.1X supplicant configuration fails to boot. **Scenario:** This issue occurs when an ACL denies DNS response from DNS server. This issue is observed in access points running ArubaOS 6.5.4.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 6.5.4.0
169184	**Symptom:** A controller does not send SYN packets for IPv6 VLANs in decrypt decrypt-tunnel and tunnel forwarding mode for the following ports: ■ SMTP ports 25 and 587 ■ Jabber port 5222 ■ SMB ports 445, 139, and so on **Scenario:** This issue is observed in controllers running ArubaOS 6.5.1.4. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.5.1.4
169622	**Symptom:** A syslog server reports the **aruba_change_channel 512 channel 6 mode 3 not found** error for some APs. **Scenario:** This issue is observed in AP-314 and AP-315 access points running ArubaOS 6.5.1.5. **Workaround:** None.	AP-Wireless	AP-314 or AP-315 access points	ArubaOS 6.5.1.5
170037 170055	**Symptom:** An AP does not discover a master controller through ADP. **Scenario:** This issue occurs when a static IP address is configured in an AP and the ACL denies ADP packets. This issue is observed in access points running ArubaOS 6.5.4.2. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 6.5.4.2
171896	**Symptom:** APs terminating on a controller in a HA topology come up with dirty configuration state (Indicated by **ID** flag). **Scenario:** This issue occurs under the following conditions: ■ HA over subscription is enabled in a controller. ■ CPsec is enabled in a controller. ■ The count of APs terminating on a standby controller exceeds twice the supported platform limit. This issue is observed in controllers running ArubaOS 6.5.1.9. **Workaround:** None.	Controller-Datapath	7200 Series controllers	ArubaOS 6.5.1.9

Table 5: *Known Issues in ArubaOS 6.5.4.5*

Bug ID	Description	Component	Platform	Reported Version
172390	**Symptom:** A branch controller loses the GRE tunnel destination IP address. **Scenario:** This issue occurs when a branch controller, which is manually configured with the IP address of a master controller, is rebooted. The IP address of the master controller is mapped with a FQDN but fails to resolve during the branch controller reboot. This issue is observed in controllers running ArubaOS 6.5.3.3. **Workaround:** None.	GRE	All platforms	ArubaOS 6.5.3.3
172506	**Symptom:** A controller discards the first TCP SYN packet when a client connects to a FTP server. **Scenario:** This issue occurs in a controller where DPI is enabled. This issue is observed in controllers running ArubaOS 6.4.4.14. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 6.4.4.14
173328	**Symptom:** A user cannot configure **block-redirect-url** on a standby controller. **Scenario:** This issue is observed in a standby controller running ArubaOS 6.5.4.2 in a master-standby topology. **Workaround:** None.	DPI	All platforms	ArubaOS 6.5.4.2

Maximum Number of NAT Pools

A controller supports a maximum of 60 NAT pools.

Chapter 6
Upgrade Procedure

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 in 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 or alias
  - destination IP or alias

- proto-port or 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 53.)

Failure to Upgrade to ArubaOS 6.5.0.0-FIPS

Customers upgrading from any FIPS version of ArubaOS prior to ArubaOS 6.5.0.0-FIPS to ArubaOS 6.5.0.0-FIPS or later version may experience symptoms that indicate an upgrade failure. Symptoms may include the apparent loss of configuration, being unable to gain administrative access to the controller, and/or the hostname of the controller being set back to the default value.

This condition is caused by a change in the FIPS requirement for the strength of the hashing algorithm that is used to protect the configuration file from outside tampering. Starting from ArubaOS 6.5.0.0-FIPS, all versions of ArubaOS are changed to use the stronger hashing algorithm to meet FIPS requirements. This change is known to create a challenge when upgrading or downgrading a controller between ArubaOS 6.4.0.0-FIPS version and ArubaOS 6.5.0.0-FIPS version. In some instances the new stronger hash value may be missing or incorrect. This may cause the controller to not boot normally.

The most common scenario is when a controller has been booted with any version of ArubaOS 6.5.0.0-FIPS or later version, is subsequently downgraded to any version of ArubaOS 6.4.0.0-FIPS or prior versions, and then at any point in the future is upgraded back to any version ArubaOS 6.5.0.0-FIPS or later version.

To restore service, Aruba recommends to roll back the ArubaOS to the previous version. This can be accomplished by:

1. Connect an administrative terminal to the console port of the controller.
2. Power cycle the controller to reboot it.
3. On the administrative terminal, interrupt the boot process when prompted to enter the cpboot bootloader.

4. Execute the **osinfo** command to display the versions of ArubaOS hosted on partition 0 and partition 1.
5. Execute the **def_part 0** or **def_part 1** command depending on which partition hosts the previous version ArubaOS 6.4.0.0-FIPS or later version.
6. Execute the **reset** or **bootf** to reboot the controller.

This restores the controller to the previous version of ArubaOS and controller configuration. Contact Aruba support for instructions to proceed with the upgrade.

GRE Tunnel-Type Requirements

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

- ArubaOS 6.5.4.5 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 51 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 51 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 51 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 51.

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 6.5.4.5

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 6.5.4.5

The following sections provide the procedures for upgrading the controller to ArubaOS 6.5.4.5 by using the WebUI and the CLI.

Install Using the WebUI

CAUTION

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 51.

NOTE

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.

Upgrading From an Older Version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. If you are running one of the following versions of ArubaOS, you must download and upgrade to an interim version of ArubaOS before upgrading to ArubaOS 6.5.0.0.

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

Follow step 2 to step 11 of the procedure described in Upgrading From a Recent Version of ArubaOS on page 54 to install the interim version of ArubaOS, and then repeat steps 1 through 11 of the procedure to download and install ArubaOS 6.5.0.0.

Upgrading From a Recent Version of ArubaOS

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

- ArubaOS 3.4.4.1 or later
- ArubaOS 5.0.3.1 or the latest version of ArubaOS 5.0.x
- ArubaOS 6.0.1.0 or later version of ArubaOS 6.x

NOTE

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 6.5.4.5 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 51 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 51.

Upgrading From an Older Version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. For more information, see Upgrading From an Older Version of ArubaOS on page 54.

Follow steps 2 through 7 of the procedure described in Upgrading From a Recent Version of ArubaOS on page 56 to install the interim version of ArubaOS, and then repeat steps 1 through 7 of the procedure to download and install ArubaOS 6.5.0.0.

Upgrading From a Recent Version of ArubaOS

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

- ArubaOS 3.4.4.1 or later
- ArubaOS 5.0.3.1 or the latest version of ArubaOS 5.0.x
- ArubaOS 6.0.1.0 or later version of ArubaOS 6.x

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

1. Download ArubaOS 6.5.4.5 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 51 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 6.5.4.5 are lost after the downgrade (this warning does not apply to upgrades from ArubaOS 3.4.x to ArubaOS 6.1).

Database versions are not compatible between different ArubaOS releases.

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 6.5.4.5 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 51.
2. Verify that the control plane security is disabled.
3. Set the controller to boot with the previously saved pre-ArubaOS 6.5.4.5 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 6.5.4.5 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.5.4.5 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 6.5.4.5, the changes do not appear in RF Plan in the downgraded ArubaOS version.
   - If you installed any certificates while running ArubaOS 6.5.4.5, 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 6.5.4.5 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
Glossary of Terms

The following table provides a brief description of the terminology used in this guide.

3DES
Triple Data Encryption Standard. 3DES is a symmetric-key block cipher that applies the DES cipher algorithm three times to each data block.

3G
Third Generation of Wireless Mobile Telecommunications Technology. See W-CDMA.

3GPP
Third Generation Partnership Project. 3GPP is a collaborative project aimed at developing globally acceptable specifications for third generation mobile systems.

4G
Fourth Generation of Wireless Mobile Telecommunications Technology. See LTE.

802.11
802.11 is an evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and Carrier Sense Multiple Access with collision avoidance (CSMA/CA) for path sharing.

802.11 bSec
802.11 bSec is an alternative to 802.11i. The difference between bSec and standard 802.11i is that bSec implements Suite B algorithms wherever possible. Notably, Advanced Encryption Standard-Counter with CBC-MAC is replaced by Advanced Encryption Standard - Galois/Counter Mode, and the Key Derivation Function (KDF) of 802.11i is upgraded to support SHA-256 and SHA-384.

802.11a
802.11a provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5 GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.

802.11ac
802.11ac is a wireless networking standard in the 802.11 family that provides high-throughput WLANs on the 5 GHz band.

802.11b
802.11b is a WLAN standard often called Wi-Fi and is backward compatible with 802.11. Instead of the Phase-Shift Keying (PSK) modulation method used in 802.11 standards, 802.11b uses Complementary Code Keying (CCK) that allows higher data speeds and makes it less susceptible to multipath-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.

802.11d

802.11d is a wireless network communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate. Configuration can be fine-tuned at the Media Access Control (MAC) layer level to comply with the rules of the country or district in which the network is to be used. Rules are subject to variation and include allowed frequencies, allowed power levels, and allowed signal bandwidth. 802.11d facilitates global roaming.

802.11e

802.11e is an enhancement to the 802.11a and 802.11b specifications that enhances the 802.11 Media Access Control layer with a coordinated Time Division Multiple Access (TDMA) construct. It adds error-correcting mechanisms for delay-sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability between business, home, and public environments such as airports and hotels, and offers all subscribers high-speed Internet access with full-motion video, high-fidelity audio, and VoIP.

802.11g

802.11g offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b standard. 802.11g employs Orthogonal Frequency Division Multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speed of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.

802.11h

802.11h is intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with military Radar systems and medical devices. Dynamic Frequency Selection (DFS) detects the presence of other devices on a channel and automatically switches the network to another channel if and when such signals are detected. Transmit Power Control (TPC) reduces the radio frequency (RF) output power of each network transmitter to a level that minimizes the risk of interference.

802.11i

802.11i provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards. It requires new encryption key protocols, known as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

802.11j

802.11j is a proposed addition to the 802.11 family of standards that incorporates Japanese regulatory extensions to 802.11a; the main intent is to add channels in the radio frequency (RF) band of 4.9 GHz to 5.0 GHz.

802.11k

802.11k is an IEEE standard that enables APs and client devices to discover the best available radio resources for seamless BSS transition in a WLAN.

802.11m

802.11m is an Initiative to perform editorial maintenance, corrections, improvements, clarifications, and interpretations relevant to documentation for 802.11 family specifications.

802.11n

802.11n is a wireless networking standard to improve network throughput over the two previous standards, 802.11a and 802.11g. With 802.11n, there will be a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz.

802.11r
802.11r is an IEEE standard for enabling seamless BSS transitions in a WLAN. 802.11r standard is also referred to as Fast BSS transition.

802.11u
802.11u is an amendment to the IEEE 802.11 WLAN standards for connection to external networks using common wireless devices such as smartphones and tablet PCs. The 802.11u protocol provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users to roam between partner networks without additional authentication. An 802.11u-capable device supports the Passpoint technology from the Wi-Fi Alliance Hotspot 2.0 R2 Specification that simplifies and automates access to public Wi-Fi.

802.11v
802.11v is an IEEE standard that allows client devices to exchange information about the network topology and RF environment. This information is used for assigning best available radio resources for the client devices to provide seamless connectivity.

802.1Q
802.1Q is an IEEE standard that enables the use of VLANs on an Ethernet network. 802.1Q supports VLAN tagging.

802.1X
802.1X is an IEEE standard for port-based network access control designed to enhance 802.11 WLAN security. 802.1X provides an authentication framework that allows a user to be authenticated by a central authority.

802.3af
802.3af is an IEEE standard for Power over Ethernet (PoE) version that supplies up to 15.4W of DC power. See PoE.

802.3at
802.3at is an IEEE standard for PoE version that supplies up to 25.5W of DC power. See PoE+.

AAA
Authentication, Authorization, and Accounting. AAA is a security framework to authenticate users, authorize the type of access based on user credentials, and record authentication events and information about the network access and network resource consumption.

ABR
Area Border Router. ABR is used for establishing connection between the backbone networks and the Open Shortest Path First (OSPF) areas. ABR is located near the border of one or more OSPF areas.

AC
Access Category. As per the IEEE 802.11e standards, AC refers to various levels of traffic prioritization in Enhanced Distributed Channel Access (EDCA) operation mode. The WLAN applications prioritize traffic based on the Background, Best Effort, Video, and Voice access categories. AC can also refer to Alternating Current, a form of electric energy that flows when the appliances are plugged to a wall socket.

ACC
Advanced Cellular Coexistence. The ACC feature in APs enable WLANs to perform at peak efficiency by minimizing interference from 3G/4G/LTE networks, distributed antenna systems, and commercial small cell/femtocell equipment.

Access-Accept
Response from the RADIUS server indicating successful authentication and containing authorization information.

Access-Reject
Response from RADIUS server indicating that a user is not authorized.

Access-Request
RADIUS packet sent to a RADIUS server requesting authorization.

Accounting-Request
RADIUS packet type sent to a RADIUS server containing accounting summary information.

Accounting-Response
RADIUS packet sent by the RADIUS server to acknowledge receipt of an Accounting-Request.

ACE
Access Control Entry. ACE is an element in an ACL that includes access control information.

ACI
Adjacent Channel Interference. ACI refers to interference or interruptions detected on a broadcasting channel, caused by too much power on an adjacent channel in the spectrum.

ACL
Access Control List. ACL is a common way of restricting certain types of traffic on a physical port.

Active Directory
Microsoft Active Directory. The directory server that stores information about a variety of things, such as organizations, sites, systems, users, shares, and other network objects or components. It also provides authentication and authorization mechanisms, and a framework within which related services can be deployed.

ActiveSync
Mobile data synchronization app developed by Microsoft that allows a mobile device to be synchronized with either a desktop or a server running compatible software products.

ad hoc network
An ad hoc network is a network composed of individual devices communicating with each other directly. Many ad hoc networks are Local Area Networks (LANs) where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point.

ADO
Active X Data Objects is a part of Microsoft Data Access Components (MDACs) that enables client applications to access data sources through an (Object Linking and Embedding Database) OLE DB provider. ADO supports key features for building client-server and Web-based applications.

ADP
Aruba Discovery Protocol. ADP is an Aruba proprietary Layer 2 protocol. It is used by the APs to obtain the IP address of the TFTP server from which it downloads the AP boot image.

AES

Advanced Encryption Standard. AES is an encryption standard used for encrypting and protecting electronic data. The AES encrypts and decrypts data in blocks of 128 bits (16 bytes), and can use keys of 128 bits, 192 bits, and 256 bits.

AIFSN

Arbitrary Inter-frame Space Number. AIFSN is set by the AP in beacon frames and probe responses. AIFS is a method of prioritizing a particular category of traffic over the other, for example prioritizing voice or video messages over email.

AirGroup

The application that allows the end users to register their personal mobile devices on a local network and define a group of friends or associates who are allowed to share them. AirGroup is primarily designed for colleges and other institutions. AirGroup uses zero configuration networking to allow Apple mobile devices, such as the AirPrint wireless printer service and the AirPlay mirroring service, to communicate over a complex access network topology.

AirWave Management Client

AirWave Management Client is a Windows software utility that enables client devices (such as a laptop) to act as passive RF sensors and augments the AirWave RAPIDS module.

ALE

Analytics and Location Engine. ALE gives visibility into everything the wireless network knows. This enables customers and partners to gain a wealth of information about the people on their premises. This can be very important for many different verticals and use cases. ALE includes a location engine that calculates associated and unassociated device location periodically using context streams, including RSSI readings, from WLAN controllers or Instant clusters.

ALG

Application Layer Gateway. ALG is a security component that manages application layer protocols such as SIP, FTP and so on.

AM

Air Monitor. AM is a mode of operation supported on wireless APs. When an AP operates in the Air Monitor mode, it enhances the wireless networks by collecting statistics, monitoring traffic, detecting intrusions, enforcing security policies, balancing wireless traffic load, self-healing coverage gaps, and more. However, clients cannot connect to APs operating in the AM mode.

AMON

Advanced Monitoring. AMON is used in Aruba WLAN deployments for improved network management, monitoring and diagnostic capabilities.

AMP

AirWave Management Platform. AMP is a network management system for configuring, monitoring, and upgrading wired and wireless devices on your network.

A-MPDU

Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.

A-MSDU

Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.

ANQP
Access Network Query Protocol. ANQP is a query and a response protocol for Wi-Fi hotspot services. ANQP includes information Elements (IEs) that can be sent from the AP to the client to identify the AP network and service provider. The IEs typically include information about the domain name of the AP operator, the IP addresses available at the AP, and information about potential roaming partners accessible through the AP. If the client responds with a request for a specific IE, the AP will send a Generic Advertisement Service (GAS) response frame with the configured ANQP IE information.

ANSI
American National Standards Institute. It refers to the ANSI compliance standards for products, systems, services, and processes.

API
Application Programming Interface. Refers to a set of functions, procedures, protocols, and tools that enable users to build application software.

app
Short form for application. It generally refers to the application that is downloaded and used on mobile devices.

ARM
Adaptive Radio Management. ARM dynamically monitors and adjusts the network to ensure that all users are allowed ready access. It enables full utilization of the available spectrum to support maximum number of users by intelligently choosing the best RF channel and transmit power for APs in their current RF environment.

ARP
Address Resolution Protocol. ARP is used for mapping IP network address to the hardware MAC address of a device.

Aruba Activate
Aruba Activate is a cloud-based service that helps provision your Aruba devices and maintain your inventory. Activate automates the provisioning process, allowing a single IT technician to easily and rapidly deploy devices throughout a distributed enterprise network.

ASCII
American Standard Code for Information Interchange. An ASCII code is a numerical representation of a character or an action.

band
Band refers to a specified range of frequencies of electromagnetic radiation.

BGP
Border Gateway Protocol. BGP is a routing protocol for exchanging data and information between different host gateways or autonomous systems on the Internet.

BLE
Bluetooth Low Energy. The BLE functionality is offered by Bluetooth® to enable devices to run for long durations with low power consumption.

BMC
Beacon Management Console. BMC manages and monitors beacons from the BLE devices. The BLE devices are used for location tracking and proximity detection.

BPDU
Bridge Protocol Data Unit. A BPDU is a data message transmitted across a local area network to detect loops in network topologies.

B-RAS
Broadband Remote Access Server. A B-RAS is a server that facilitates and converges traffic from multiple Internet traffic resources such as cable, DSL, Ethernet, or Broadband wireless.

BRE
Basic Regular Expression. The BRE syntax standards designed by the IEEE provides extension to the traditional Simple Regular Expressions syntax and allows consistency between utility programs such as grep, sed, and awk.

BSS
Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists of an AP and all its associated clients.

BSSID
Basic Service Set Identifier. The BSSID identifies a particular BSS within an area. In infrastructure BSS networks, the BSSID is the MAC address of the AP. In independent BSS or ad hoc networks, the BSSID is generated randomly.

BYOD
Bring Your Own Device. BYOD refers to the use of personal mobile devices within an enterprise network infrastructure.

CA
Certificate Authority or Certification Authority. Entity in a public key infrastructure system that issues certificates to clients. A certificate signing request received by the CA is converted into a certificate when the CA adds a signature generated with a private key. See digital certificate.

CAC
Call Admission Control. CAC regulates traffic volume in voice communications. CAC can also be used to ensure or maintain a certain level of audio quality in voice communications networks.

CALEA
Communications Assistance for Law Enforcement Act. To comply with the CALEA specifications and to allow lawful interception of Internet traffic by the law enforcement and intelligence agencies, the telecommunications carriers and manufacturers of telecommunications equipment are required to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

Campus AP
Campus APs are used in private networks where APs connect over private links (LAN, WLAN, WAN or MPLS) and terminate directly on controllers. Campus APs are deployed as part of the indoor campus solution in enterprise office buildings, warehouses, hospitals, universities, and so on.

captive portal
A captive portal is a web page that allows the users to authenticate and sign in before connecting to a public-access network. Captive portals are typically used by business centers, airports, hotel lobbies, coffee shops, and other venues that offer free Wi-Fi hotspots for the guest users.

CCA
Clear Channel Assessment. In wireless networks, the CCA method detects if a channel is occupied or clear, and determines if the channel is available for data transmission.

CDP
Cisco Discovery Protocol. CDP is a proprietary Data Link Layer protocol developed by Cisco Systems. CDP runs on Cisco devices and enables networking applications to learn about the neighboring devices directly connected to the network.

CDR
Call Detail Record. A CDR contains the details of a telephone or VoIP call, such as the origin and destination addresses of the call, the start time and end time of the call, any toll charges that were added through the network or charges for operator services, and so on.

CEF
Common Event Format. The CEF is a standard for the interoperability of event or log-generating devices and applications. The standard syntax for CEF includes a prefix and a variable extension formatted as key-value pairs.

CGI
Common Gateway Interface. CGI is a standard protocol for exchanging data between the web servers and executable programs running on a server to dynamically process web pages.

CHAP
Challenge Handshake Authentication Protocol. CHAP is an authentication scheme used by PPP servers to validate the identity of remote clients.

CIDR
Classless Inter-Domain Routing. CIDR is an IP standard for creating and allocating unique identifiers for networks and devices. The CIDR IP addressing scheme is used as a replacement for the older IP addressing scheme based on classes A, B, and C. With CIDR, a single IP address can be used to designate many unique IP addresses. A CIDR IP address ends with a slash followed by the IP network prefix, for example, 192.0.2.0/24.

ClearPass
ClearPass is an access management system for creating and enforcing policies across a network to all devices and applications. The ClearPass integrated platform includes applications such as Policy Manager, Guest, Onboard, OnGuard, Insight, Profile, QuickConnect, and so on.

ClearPass Guest
ClearPass Guest is a configurable ClearPass application for secure visitor network access management.

ClearPass Policy Manager
ClearPass Policy Manager is a baseline platform for policy management, AAA, profiling, network access control, and reporting. With ClearPass Policy Manager, the network administrators can configure and manage secure network access that accommodates requirements across multiple locations and multivendor networks, regardless of device ownership and connection method.

CLI
Command-Line Interface. A console interface with a command line shell that allows users to execute text input as commands and convert these commands to appropriate functions.

CN
Common Name. CN is the primary name used to identify a certificate.

CNA
Captive Network Assistant. CNA is a popup page shown when joining a network that has a captive portal.

CoA
Change of Authorization. The RADIUS CoA is used in the AAA service framework to allow dynamic modification of the authenticated, authorized, and active subscriber sessions.

CoS
Class of Service. CoS is used in data and voice protocols for classifying packets into different types of traffic (voice, video, or data) and setting a service priority. For example, voice traffic can be assigned a higher priority over email or HTTP traffic.

CPE
Customer Premises Equipment. It refers to any terminal or equipment located at the customer premises.

CPsec
Control Plane Security. CPsec is a secure form of communication between a controller and APs to protect the control plane communications. This is performed by means of using public-key self-signed certificates created by each master controller.

CPU
Central Processing Unit. A CPU is an electronic circuitry in a computer for processing instructions.

CRC
Cyclic Redundancy Check. CRC is a data verification method for detecting errors in digital data during transmission, storage, or retrieval.

CRL
Certificate Revocation List. CRL is a list of revoked certificates maintained by a certification authority.

cryptobinding
Short for cryptographic binding. A procedure in a tunneled EAP method that binds together the tunnel protocol and the tunneled authentication methods, ensuring the relationship between a collection of data assets. Cryptographic binding focuses on protecting the server; mutual cryptographic binding protects both peer and server.

CSA
Channel Switch Announcement. The CSA element enables an AP to advertise that it is switching to a new channel before it begins transmitting on that channel. This allows the clients, which support CSA, to transition to the new channel with minimal downtime.

CSMA/CA
Carrier Sense Multiple Access / Collision Avoidance. CSMA/CA is a protocol for carrier transmission in networks using the 802.11 standard. CSMA/CA aims to prevent collisions by listening to the broadcasting nodes, and informing devices not to transmit any data until the broadcasting channel is free.

CSR
Certificate Signing Request. In PKI systems, a CSR is a message sent from an applicant to a CA to apply for a digital identity certificate.

CSV
Comma-Separated Values. A file format that stores tabular data in the plain text format separated by commas.

CTS
Clear to Send. The CTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See RTS.

CW
Contention Window. In QoS, CW refers to a window set for access categories based on the type of traffic. Based on the type and volume of the traffic, the minimum and maximum values can be calculated to provide a wider window when necessary.

DAI
Dynamic ARP inspection. A security feature that validates ARP packets in a network.

DAS
Distributed Antenna System. DAS is a network of antenna nodes strategically placed around a geographical area or structure for additional cellular coverage.

dB
Decibel. Unit of measure for sound or noise and is the difference or ratio between two signal levels.

dBm
Decibel-Milliwatts. dBm is a logarithmic measurement (integer) that is typically used in place of mW to represent receive-power level. AMP normalizes all signals to dBm, so that it is easy to evaluate performance between various vendors.

DCB
Data Center Bridging. DCB is a collection of standards developed by IEEE for creating a converged data center network using Ethernet.

DCE
Data Communication Equipment. DCE refers to the devices that establish, maintain, and terminate communication network sessions between a data source and its destination.

DCF
Distributed Coordination Function. DCF is a protocol that uses carrier sensing along with a four-way handshake to maximize the throughput while preventing packet collisions.

DDMO
Distributed Dynamic Multicast Optimization. DDMO is similar to Dynamic Multicast Optimization (DMO) where the multicast streams are converted into unicast streams on the AP instead of the controller, to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DES
Data Encryption Standard. DES is a common standard for data encryption and a form of secret key cryptography, which uses only one key for encryption and decryption.

designated router
Designated router refers to a router interface that is elected to originate network link advertisements for networks using the OSPF protocol.

destination NAT
Destination Network Address Translation. Destination NAT is a process of translating the destination IP address of an end route packet in a network. Destination NAT is used for redirecting the traffic destined to a virtual host to the real host, where the virtual host is identified by the destination IP address and the real host is identified by the translated IP address.

DFS
Dynamic Frequency Selection. DFS is a mandate for radio systems operating in the 5 GHz band to be equipped with means to identify and avoid interference with Radar systems.

DFT
Discrete Fourier Transform. DFT converts discrete-time data sets into a discrete-frequency representation. See FFT.

DHCP
Dynamic Host Configuration Protocol. A network protocol that enables a server to automatically assign an IP address to an IP-enabled device from a defined range of numbers configured for a given network.

DHCP snooping
DHCP snooping enables the switch to monitor and control DHCP messages received from untrusted devices that are connected to the switch.

digital certificate
A digital certificate is an electronic document that uses a digital signature to bind a public key with an identity—information such as the name of a person or an organization, address, and so forth.

Digital wireless pulse
A wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance. Ultra Wideband radio can carry a huge amount of data over a distance up to 230 ft at very low power (less than 0.5 mW), and has the ability to carry signals through doors and other obstacles that tend to reflect signals at more limited bandwidths and a higher power.

Disconnect-Ack
Disconnect-Ack is a NAS response packet to a Disconnect-Request, which indicates that the session was disconnected.

Disconnect-Nak
Disconnect-Nak is NAS response packet to a Disconnect-Request, which indicates that the session was not disconnected.

Disconnect-Request
Disconnect-Request is a RADIUS packet type sent to a NAS requesting that a user or session be disconnected.

distribution certificate
Distribution certificate is used for digitally signing iOS mobile apps to enable enterprise app distribution. It verifies the identity of the app publisher.

DLNA
Digital Living Network Alliance. DLNA is a set of interoperability guidelines for sharing digital media among multimedia devices.

DMO
Dynamic Multicast Optimization. DMO is a process of converting multicast streams into unicast streams over a wireless link to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DN
Distinguished Name. A series of fields in a digital certificate that, taken together, constitute the unique identity of the person or device that owns the digital certificate. Common fields in a DN include country, state, locality, organization, organizational unit, and the “common name”, which is the primary name used to identify the certificate.

DNS
Domain Name System. A DNS server functions as a phone book for the intranet and Internet users. It converts human-readable computer host names into IP addresses and IP addresses into host names. It stores several records for a domain name such as an address 'A' record, name server (NS), and mail exchanger (MX) records. The Address 'A' record is the most important record that is stored in a DNS server, because it provides the required IP address for a network peripheral or element.

DOCSIS
Data over Cable Service Interface Specification. A telecommunication standard for Internet access through cable modem.

DoS
Denial of Service. DoS is any type of attack where the attackers send excessive messages to flood traffic and thereby preventing the legitimate users from accessing the service.

DPD
Dead Peer Detection. A method used by the network devices to detect the availability of the peer devices.

DPI
Deep Packet Inspection. DPI is an advanced method of network packet filtering that is used for inspecting data packets exchanged between the devices and systems over a network. DPI functions at the Application layer of the Open Systems Interconnection (OSI) reference model and enables users to identify, categorize, track, reroute, or stop packets passing through a network.

DRT
Downloadable Regulatory Table. The DRT feature allows new regulatory approvals to be distributed for APs without a software upgrade or patch.

DS
Differentiated Services. The DS specification aims to provide uninterrupted quality of service by managing and controlling the network traffic, so that certain types of traffic get precedence.

DSCP
Differentiated Services Code Point. DSCP is a 6-bit packet header value used for traffic classification and priority assignment.

DSL
Digital Subscriber Line. The DSL technology allows the transmission of digital data over telephone lines. A DSL modem is a device used for connecting a computer or router to a telephone line that offers connectivity to the Internet.

DSSS
Direct-Sequence Spread Spectrum. DSSS is a modulation technique used for reducing overall signal interference. This technique multiplies the original data signal with a pseudo random noise spreading code. Spreading of this signal makes the resulting wideband channel more noisy, thereby increasing the resistance to interference. See FHSS.

DST
Daylight Saving Time. DST is also known as summer time that refers to the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

DTE
Data Terminal Equipment. DTE refers to a device that converts user information into signals or re-converts the received signals.

DTIM
Delivery Traffic Indication Message. DTIM is a kind of traffic indication map. A DTIM interval determines when the APs must deliver broadcast and multicast frames to their associated clients in power save mode.

DTLS
Datagram Transport Layer Security. DTLS communications protocol provides communications security for datagram protocols.

dynamic authorization
Dynamic authorization refers to the ability to make changes to a visitor account's session while it is in progress. This might include disconnecting a session or updating some aspect of the authorization for the session.

dynamic NAT
Dynamic Network Address Translation. Dynamic NAT maps multiple public IP addresses and uses these addresses with an internal or private IP address. Dynamic NAT helps to secure a network by masking the internal configuration of a private network.

EAP
Extensible Authentication Protocol. An authentication protocol for wireless networks that extends the methods used by the PPP, a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

EAP-FAST
EAP – Flexible Authentication Secure Tunnel (tunneled).

EAP-GTC
EAP – Generic Token Card. (non-tunneled).

EAP-MD5
EAP – Method Digest 5. (non-tunneled).

EAP-MSCHAP
EAP Microsoft Challenge Handshake Authentication Protocol.

EAP-MSCHAPv2
EAP Microsoft Challenge Handshake Authentication Protocol Version 2.

EAPoL
Extensible Authentication Protocol over LAN. A network port authentication protocol used in IEEE 802.1X standards to provide a generic network sign-on to access network resources.

EAP-PEAP
EAP–Protected EAP. A widely used protocol for securely transporting authentication data across a network (tunneled).

EAP-PWD
EAP-Password. EAP-PWD is an EAP method that uses a shared password for authentication.

EAP-TLS
EAP–Transport Layer Security. EAP-TLS is a certificate-based authentication method supporting mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints. See RFC 5216.

EAP-TTLS
EAP–Tunneled Transport Layer Security. EAP-TTLS is an EAP method that encapsulates a TLS session, consisting of a handshake phase and a data phase. See RFC 5281.

ECC
Elliptical Curve Cryptography or Error correcting Code memory. Elliptical Curve Cryptography is a public-key encryption technique that is based on elliptic curve theory used for creating faster, smaller, and more efficient cryptographic keys. Error Correcting Code memory is a type of computer data storage that can detect and correct the most common kinds of internal data corruption. ECC memory is used in most computers where data corruption cannot be tolerated under any circumstances, such as for scientific or financial computing.

ECDSA
Elliptic Curve Digital Signature Algorithm. ECDSA is a cryptographic algorithm that supports the use of public or private key pairs for encrypting and decrypting information.

EDCA
Enhanced Distributed Channel Access. The EDCA function in the IEEE 802.11e Quality of Service standard supports differentiated and distributed access to wireless medium based on traffic priority and Access Category types. See WMM and WME.

EIGRP
Enhanced Interior Gateway Routing Protocol. EIGRP is a routing protocol used for automating routing decisions and configuration in a network.

EIRP
Effective Isotropic Radiated Power or Equivalent Isotropic Radiated Power. EIRP refers to the output power generated when a signal is concentrated into a smaller area by the Antenna.

ESI
External Services Interface. ESI provides an open interface for integrating security solutions that solve interior network problems such as viruses, worms, spyware, and corporate compliance.

ESS
Extended Service Set. An ESS is a set of one or more interconnected BSSs that form a single sub network.

ESSID
Extended Service Set Identifier. ESSID refers to the ID used for identifying an extended service set.

Ethernet
Ethernet is a network protocol for data transmission over LAN.

EULA
End User License Agreement. EULA is a legal contract between a software application publisher or author and the users of the application.

FCC
Federal Communications Commission. FCC is a regulatory body that defines standards for the interstate and international communications by radio, television, wire, satellite, and cable.

FFT
Fast Fourier Transform. FFT is a frequency analysis mechanism that aims at faster conversion of a discrete signal in time domain into a discrete frequency domain representation. See also DFT.

FHSS
Frequency Hopping Spread Spectrum. FHSS is transmission technique that allows modulation and transmission of a data signal by rapidly switching a carrier among many frequency channels in a random but predictable sequence. See also DSSS.

FIB
Forwarding Information Base. FIB is a forwarding table that maps MAC addresses to ports. FIB is used in network bridging, routing, and similar functions to identify the appropriate interface for forwarding packets.

FIPS
Federal Information Processing Standards. FIPS refers to a set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies, and by government contractors and vendors who work with these agencies.

firewall
Firewall is a network security system used for preventing unauthorized access to or from a private network.

FQDN
Fully Qualified Domain Name. FQDN is a complete domain name that identifies a computer or host on the Internet.

FQLN
Fully Qualified Location Name. FQLN is a device location identifier in the format: APname.Floor.Building.Campus.

frequency allocation
Use of radio frequency spectrum as regulated by governments.

FSPL
Free Space Path Loss. FSPL refers to the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space (usually air), with no obstacles nearby to cause reflection or diffraction.

FTP
File Transfer Protocol. A standard network protocol used for transferring files between a client and server on a computer network.

GARP
Generic Attribute Registration Protocol. GVRP is a LAN protocol that allows the network nodes to register and de-register attributes, such as network addresses, with each other.

GAS
Generic Advertisement Service. GAS is a request-response protocol, which provides Layer 2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps in determining a wireless network infrastructure before associating clients, and allows clients to send queries to multiple 802.11 networks in parallel.

gateway
Gateway is a network node that allows traffic to flow in and out of the network.

Gbps
Gigabits per second.

GBps
Gigabytes per second.

GET
GET refers HTTP request method or an SNMP operation method. The GET HTTP request method submits data to be processed to a specified resource. The GET SNMP operation method obtains information from the Management Information Base (MIB).

GHz
Gigahertz.

GMT
Greenwich Mean Time. GMT refers to the mean solar time at the Royal Observatory in Greenwich, London. GMT is the same as Coordinated Universal Time (UTC) standard, written as an offset of UTC +/- 00:00.

goodput
Goodput is the application level throughput that refers to the ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes.

GPS
Global Positioning System. A satellite-based global navigation system.

GRE
Generic Routing Encapsulation. GRE is an IP encapsulation protocol that is used to transport packets over a network.

GTC
Generic Token Card. GTC is a protocol that can be used as an alternative to MSCHAPv2 protocol. GTC allows authentication to various authentication databases even in cases where MSCHAPv2 is not supported by the database.

GVRP
GARP VLAN Registration Protocol or Generic VLAN Registration Protocol. GARP is an IEEE 802.1Q-compliant protocol that facilitates VLAN registration and controls VLANs within a larger network.

H2QP
Hotspot 2.0 Query Protocol.

hot zone
Wireless access area created by multiple hotspots that are located in close proximity to one another. Hot zones usually combine public safety APs with public hotspots.

hotspot
Hotspot refers to a WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can look up a local hotspot, contact it, and get connected through its network to reach the Internet.

HSPA
High-Speed Packet Access.

HT
High Throughput. IEEE 802.11n is an HT WLAN standard that aims to achieve physical data rates of close to 600 Mbps on the 2.4 GHz and 5 GHz bands.

HTTP
Hypertext Transfer Protocol. The HTTP is an application protocol to transfer data over the web. The HTTP protocol defines how messages are formatted and transmitted, and the actions that the w servers and browsers should take in response to various commands.

HTTPS
Hypertext Transfer Protocol Secure. HTTPS is a variant of the HTTP that adds a layer of security on the data in transit through a secure socket layer or transport layer security protocol connection.

IAS
Internet Authentication Service. IAS is a component of Windows Server operating systems that provides centralized user authentication, authorization, and accounting.

ICMP
Internet Control Message Protocol. ICMP is an error reporting protocol. It is used by network devices such as routers, to send error messages and operational information to the source IP address when network problems prevent delivery of IP packets.

IDS
Intrusion Detection System. IDS monitors a network or systems for malicious activity or policy violations and reports its findings to the management system deployed in the network.

IEEE
Institute of Electrical and Electronics Engineers.

IGMP
Internet Group Management Protocol. Communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.

IGMP snooping
IGMP snooping prevents multicast flooding on Layer 2 network by treating multicast traffic as broadcast traffic. Without IGMP snooping, all streams could be flooded to all ports on that VLAN. When multicast flooding occurs, end-hosts that happen to be in the same VLAN would receive all the streams only to be discarded without snooping.

IGP
Interior Gateway Protocol. IGP is used for exchanging routing information between gateways within an autonomous system (for example, a system of corporate local area networks).

IGRP
Interior Gateway Routing Protocol. IGRP is a distance vector interior routing protocol used by routers to exchange routing data within an autonomous system.

IKE
Internet Key Exchange. IKE is a key management protocol used with IPsec protocol to establish a secure communication channel. IKE provides additional feature, flexibility, and ease of configuration for IPsec standard.

IKEv1
Internet Key Exchange version 1. IKEv1 establishes a secure authenticated communication channel by using either the pre-shared key (shared secret), digital signatures, or public key encryption. IKEv1 operates in Main and Aggressive modes. See RFC 2409.

IKEv2
Internet Key Exchange version 2. IKEv2 uses the secure channel established in Phase 1 to negotiate Security Associations on behalf of services such as IPsec. IKEv2 uses pre-shared key and Digital Signature for authentication. See RFC 4306.

IoT
Internet of Things. IoT refers to the internetworking of devices that are embedded with electronics, software, sensors, and network connectivity features allowing data exchange over the Internet.

IPM
Intelligent Power Monitoring. IPM is a feature supported on certain APs that actively measures the power utilization of an AP and dynamically adapts to the power resources.

IPS
Intrusion Prevention System. The IPS monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, log the information, attempt to block the activity, and report it.

IPsec
Internet Protocol security. IPsec is a protocol suite for secure IP communications that authenticates and encrypts each IP packet in a communication session.

IPSG
Internet Protocol Source Guard. IPSG restricts IP address from untrusted interface by filtering traffic based on list of addresses in the DHCP binding database or manually configured IP source bindings. It prevents IP spoofing attacks.

IrDA
An industry-sponsored organization set up in 1993 to create international standards for the hardware and software used in infrared communication links. In this special form of radio transmission, a focused ray of light in the infrared frequency spectrum, measured in terahertz (THz), or trillions of hertz (cycles per second), is modulated with information and sent from a transmitter to a receiver over a relatively short distance.

ISAKMP
Internet Security Association and Key Management Protocol. ISAKMP is used for establishing Security Associations and cryptographic keys in an Internet environment.

ISP
Internet Service Provider. An ISP is an organization that provides services for accessing and using the Internet.

JSON
JavaScript Object Notation. JSON is an open-standard, language-independent, lightweight data-interchange format used to transmit data objects consisting of attribute–value pairs. JSON uses a "self-describing" text format that is easy for humans to read and write, and that can be used as a data format by any programming language.

Kbps
Kilobits per second.

KBps
Kilobytes per second.

keepalive
Signal sent at periodic intervals from one device to another to verify that the link between the two devices is working. If no reply is received, data will be sent by a different path until the link is restored. A keepalive can also be used to indicate that the connection should be preserved so that the receiving device does not consider it timed out and drop it.

L2TP
Layer-2 Tunneling Protocol. L2TP is a networking protocol used by the ISPs to enable VPN operations.

LACP
Link Aggregation Control Protocol. LACP is used for the collective handling of multiple physical ports that can be seen as a single channel for network traffic purposes.

LAG
Link Aggregation Group . A LAG combines a number of physical ports together to make a single high-bandwidth data path. LAGs can connect two switches to provide a higher-bandwidth connection to a public network.

LAN
Local Area Network. A LAN is a network of connected devices within a distinct geographic area such as an office or a commercial establishment and share a common communications line or wireless link to a server.

LCD
Liquid Crystal Display. LCD is the technology used for displays in notebook and other smaller computers. Like LED and gas-plasma technologies, LCDs allow displays to be much thinner than the cathode ray tube technology.

LDAP
Lightweight Directory Access Protocol. LDAP is a communication protocol that provides the ability to access and maintain distributed directory information services over a network.

LDPC
Low-Density Parity-Check. LDPC is a method of transmitting a message over a noisy transmission channel using a linear error correcting code. An LDPC is constructed using a sparse bipartite graph.

LEAP
Lightweight Extensible Authentication Protocol. LEAP is a Cisco proprietary version of EAP used in wireless networks and Point-to-Point connections.

LED
Light Emitting Diode. LED is a semiconductor light source that emits light when an electric current passes through it.

LEEF
Log Event Extended Format. LEEF is a type of customizable syslog event format. An extended log file contains a sequence of lines containing ASCII characters terminated by either the sequence LF or CRLF.

LI
Lawful Interception. LI refers to the procedure of obtaining communications network data by the Law Enforcement Agencies for the purpose of analysis or evidence.

LLDP
Link Layer Discovery Protocol. LLDP is a vendor-neutral link layer protocol in the Internet Protocol suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, which is principally a wired Ethernet.

LLDP-MED
LLDP–Media Endpoint Discovery. LLDP-MED facilitates information sharing between endpoints and network infrastructure devices.

LMS
Local Management Switch. In multi-controller networks, each controller acts as an LMS and terminates user traffic from the APs, processes, and forwards the traffic to the wired network.

LNS
L2TP Network Server. LNS is an equipment that connects to a carrier and handles the sessions from broadband lines. It is also used for dial-up and mobile links. LNS handles authentication and routing of the IP addresses. It also handles the negotiation of the link with the equipment and establishes a session.

LTE
Long Term Evolution. LTE is a 4G wireless communication standard that provides high-speed wireless communication for mobile phones and data terminals. See 4G.

MAB
MAC Authentication Bypass. Endpoints such as network printers, Ethernet-based sensors, cameras, and wireless phones do not support 802.1X authentication. For such endpoints, MAC Authentication Bypass mechanism is used. In this method, the MAC address of the endpoint is used to authenticate the endpoint.

MAC
Media Access Control. A MAC address is a unique identifier assigned to network interfaces for communications on a network.

MAM
Mobile Application Management. MAM refers to software and services used to secure, manage, and distribute mobile applications used in enterprise settings on mobile devices like smartphones and tablet computers. Mobile Application Management can apply to company-owned mobile devices as well as BYOD.

Mbps
Megabits per second

MBps
Megabytes per second

MCS
Modulation and Coding Scheme. MCS is used as a parameter to determine the data rate of a wireless connection for high throughput.

MD4
Message Digest 4. MD4 is an earlier version of MD5 and is an algorithm used to verify data integrity through the creation of a 128-bit message digest from data input.

MD5
Message Digest 5. The MD5 algorithm is a widely used hash function producing a 128-bit hash value from the data input.

MDAC
Microsoft Data Access Components. MDAC is a framework of interrelated Microsoft technologies that provides a standard database for Windows OS.

MDM
Mobile Device Management. MDM is an administrative software to manage, monitor, and secure mobile devices of the employees in a network.

mDNS
Multicast Domain Name System. mDNS provides the ability to perform DNS-like operations on the local link in the absence of any conventional unicast DNS server. The mDNS protocol uses IP multicast User Datagram Protocol (UDP) packets, and is implemented by the Apple Bonjour and Linux NSS-mDNS services. mDNS works in conjunction with DNS Service Discovery (DNS-SD), a companion zero-configuration technique specified. See RFC 6763.

MFA
Multi-factor Authentication. MFA lets you require multiple factors, or proofs of identity, when authenticating a user. Policy configurations define how often multi-factor authentication will be required, or conditions that will trigger it.

MHz
Megahertz

MIB
Management Information Base. A hierarchical database used by SNMP to manage the devices being monitored.

microwave
Electromagnetic energy with a frequency higher than 1 GHz, corresponding to wavelength shorter than 30 centimeters.

MIMO
Multiple Input Multiple Output. An antenna technology for wireless communications in which multiple antennas are used at both source (transmitter) and destination (receiver). The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed.

MISO
Multiple Input Single Output. An antenna technology for wireless communications in which multiple antennas are used at the source (transmitter). The antennas are combined to minimize errors and optimize data speed. The destination (receiver) has only one antenna.

MLD
Multicast Listener Discovery. A component of the IPv6 suite. It is used by IPv6 routers for discovering multicast listeners on a directly attached link.

MPDU
MAC Protocol Data Unit. MPDU is a message exchanged between MAC entities in a communication system based on the layered OSI model.

MPLS
Multiprotocol Label Switching. The MPLS protocol speeds up and shapes network traffic flows.

MPPE
Microsoft Point-to-Point Encryption. A method of encrypting data transferred across PPP-based dial-up connections or PPTP-based VPN connections.

MS-CHAP
Microsoft Challenge Handshake Authentication Protocol. MS-CHAP is Password-based, challenge-response, mutual authentication protocol that uses MD4 and DES encryption.

MS-CHAPv1
Microsoft Challenge Handshake Authentication Protocol version 1. MS-CHAPv1 extends the user authentication functionality provided on Windows networks to remote workstations. MS-CHAPv1 supports only one-way authentication.

MS-CHAPv2
Microsoft Challenge Handshake Authentication Protocol version 2. MS-CHAPv2 is an enhanced version of the MS-CHAP protocol that supports mutual authentication.

MSS
Maximum Segment Size. MSS is a parameter of the options field in the TCP header that specifies the largest amount of data, specified in bytes, that a computer or communications device can receive in a single TCP segment.

MSSID
Mesh Service Set Identifier. MSSID is the SSID used by the client to access a wireless mesh network.

MSTP
Multiple Spanning Tree Protocol. MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree.

MTU
Maximum Transmission Unit. MTU is the largest size packet or frame specified in octets (eight-bit bytes) that can be sent in networks such as the Internet.

MU-MIMO
Multi-User Multiple-Input Multiple-Output. MU-MIMO is a set of multiple-input and multiple-output technologies for wireless communication, in which users or wireless terminals with one or more antennas communicate with each other.

MVRP
Multiple VLAN Registration Protocol. MVRP is a Layer 2 network protocol used for automatic configuration of VLAN information on switches.

mW
milliWatts. mW is 1/1000 of a Watt. It is a linear measurement (always positive) that is generally used to represent transmission.

NAC
Network Access Control. NAC is a computer networking solution that uses a set of protocols to define and implement a policy that describes how devices can secure access to network nodes when they initially attempt to connect to a network.

NAD
Network Access Device. NAD is a device that automatically connects the user to the preferred network, for example, an AP or an Ethernet switch.

NAK
Negative Acknowledgement. NAK is a response indicating that a transmitted message was received with errors or it was corrupted, or that the receiving end is not ready to accept transmissions.

NAP
Network Access Protection. The NAP feature in the Windows Server allows network administrators to define specific levels of network access based on identity, groups, and policy compliance. The NAP Agent is a service that collects and manages health information for NAP client computers. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

NAS
Network Access Server. NAS provides network access to users, such as a wireless AP, network switch, or dial-in terminal server.

NAT
Network Address Translation. NAT is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

NetBIOS
Network Basic Input/Output System. A program that lets applications on different computers communicate within a LAN.

netmask
Netmask is a 32-bit mask used for segregating IP address into subnets. Netmask defines the class and range of IP addresses.

NFC
Near-Field Communication. NFC is a short-range wireless connectivity standard (ECMA-340, ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they touch or are brought closer (within a few centimeters of distance). The standard specifies a way for the devices to establish a peer-to-peer (P2P) network to exchange data.

NIC
Network Interface Card. NIC is a hardware component that allows a device to connect to the network.

Nmap
Network Mapper. Nmap is an open-source utility for network discovery and security auditing. Nmap uses IP packets to determine such things as the hosts available on a network and their services, operating systems and versions, types of packet filters/firewalls, and so on.

NMI
Non-Maskable Interrupt. NMI is a hardware interrupt that standard interrupt-masking techniques in the system cannot ignore. It typically occurs to signal attention for non-recoverable hardware errors.

NMS
Network Management System. NMS is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework.

NOE
New Office Environment. NOE is a proprietary VoIP protocol designed by Alcatel-Lucent Enterprise.

NTP
Network Time Protocol. NTP is a protocol for synchronizing the clocks of computers over a network.

OAuth
Open Standard for Authorization. OAuth is a token-based authorization standard that allows websites or third-party applications to access user information, without exposing the user credentials.

OCSP
Online Certificate Status Protocol. OCSP is used for determining the current status of a digital certificate without requiring a CRL.

OFDM
Orthogonal Frequency Division Multiplexing. OFDM is a scheme for encoding digital data on multiple carrier frequencies.

OID
Object Identifier. An OID is an identifier used to name an object. The OIDs represent nodes or managed objects in a MIB hierarchy. The OIDs are designated by text strings and integer sequences and are formally defined as per the ASN.1 standard.

OKC
Opportunistic Key Caching. OKC is a technique available for authentication between multiple APs in a network where those APs are under common administrative control. Using OKC, a station roaming to any AP in the network will not have to complete a full authentication exchange, but will instead just perform the 4-way handshake to establish transient encryption keys.

onboarding
The process of preparing a device for use on an enterprise network, by creating the appropriate access credentials and setting up the network connection parameters.

OpenFlow
OpenFlow is an open communications interface between control plane and the forwarding layers of a network.

OpenFlow agent
OpenFlow agent. OpenFlow is a software module in Software-Defined Networking (SDN) that allows the abstraction of any legacy network element, so that it can be integrated and managed by the SDN controller. OpenFlow runs on network devices such as switches, routers, wireless controllers, and APs.

Optical wireless
Optical wireless is combined use of conventional radio frequency wireless and optical fiber for telecommunication. Long-range links are provided by using optical fibers; the links from the long-range endpoints to end users are accomplished by RF wireless or laser systems. RF wireless at Ultra High Frequencies and microwave frequencies can carry broadband signals to individual computers at substantial data speeds.

OSI
Open Systems Interconnection. OSI is a reference model that defines a framework for communication between the applications in a network.

OSPF
Open Shortest Path First. OSPF is a link-state routing protocol for IP networks. It uses a link-state routing algorithm and falls into the group of interior routing protocols that operates within a single Autonomous System (AS).

OSPFv2
Open Shortest Path First version 2. OSPFv2 is the version 2 of the link-state routing protocol, OSPF. See RFC 2328.

OUI
Organizationally Unique Identifier. Synonymous with company ID or vendor ID, an OUI is a 24-bit, globally unique assigned number, referenced by various standards. The first half of a MAC address is OUI.

OVA
Open Virtualization Archive. OVA contains a compressed installable version of a virtual machine.

OVF
Open Virtualization Format. OVF is a specification that describes an open-standard, secure, efficient, portable and extensible format for packaging and distributing software for virtual machines.

PAC
Protected Access Credential. PAC is distributed to clients for optimized network authentication. These credentials are used for establishing an authentication tunnel between the client and the authentication server.

PAP
Password Authentication Protocol. PAP validates users by password. PAP does not encrypt passwords for transmission and is thus considered insecure.

PAPI
Process Application Programming Interface. PAPI controls channels for ARM and Wireless Intrusion Detection System (WIDS) communication to the master controller. A separate PAPI control channel connects to the local controller where the SSID tunnels terminate.

PBR
Policy-based Routing. PBR provides a flexible mechanism for forwarding data packets based on polices configured by a network administrator.

PDU
Power Distribution Unit or Protocol Data Unit. Power Distribution Unit is a device that distributes electric power to the networking equipment located within a data center. Protocol Data Unit contains protocol control Information that is delivered as a unit among peer entities of a network.

PEAP
Protected Extensible Authentication Protocol. PEAP is a type of EAP communication that addresses security issues associated with clear text EAP transmissions by creating a secure channel encrypted and protected by TLS.

PEF
Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFNG

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFV

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PFS

Perfect Forward Secrecy. PFS refers to the condition in which a current session key or long-term private key does not compromise the past or subsequent keys.

PHB

Per-hop behavior. PHB is a term used in DS or MPLS. It defines the policy and priority applied to a packet when traversing a hop (such as a router) in a DiffServ network.

PIM

Protocol-Independent Multicast. PIM refers to a family of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the Internet.

PIN

Personal Identification Number. PIN is a numeric password used to authenticate a user to a system.

PKCS#n

Public-key cryptography standard n. PKCS#n refers to a numbered standard related to topics in cryptography, including private keys (PKCS#1), digital certificates (PKCS#7), certificate signing requests (PKCS#10), and secure storage of keys and certificates (PKCS#12).

PKI

Public Key Infrastructure. PKI is a security technology based on digital certificates and the assurances provided by strong cryptography. See also certificate authority, digital certificate, public key, private key.

PLMN

Public Land Mobile Network. PLMS is a network established and operated by an administration or by a Recognized Operating Agency for the specific purpose of providing land mobile telecommunications services to the public.

PMK

Pairwise Master Key. PMK is a shared secret key that is generated after PSK or 802.1X authentication.

PoE

Power over Ethernet. PoE is a technology for wired Ethernet LANs to carry electric power required for the device in the data cables. The IEEE 802.3af PoE standard provides up to 15.4 W of power on each port.

PoE+
Power over Ethernet+. PoE+ is an IEEE 802.3at standard that provides 25.5W power on each port.

POST
Power On Self Test. An HTTP request method that requests data from a specified resource.

PPP
Point-to-Point Protocol. PPP is a data link (layer 2) protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption, and compression.

PPPoE
Point-to-Point Protocol over Ethernet. PPPoE is a method of connecting to the Internet, typically used with DSL services, where the client connects to the DSL modem.

PPTP
Point-to-Point Tunneling Protocol. PPTP is a method for implementing virtual private networks. It uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

private key
The part of a public-private key pair that is always kept private. The private key encrypts the signature of a message to authenticate the sender. The private key also decrypts a message that was encrypted with the public key of the sender.

PRNG
Pseudo-Random Number Generator. PRNG is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers.

PSK
Pre-shared key. A unique shared secret that was previously shared between two parties by using a secure channel. This is used with WPA security, which requires the owner of a network to provide a passphrase to users for network access.

PSU
Power Supply Unit. PSU is a unit that supplies power to an equipment by converting mains AC to low-voltage regulated DC power.

public key
The part of a public-private key pair that is made public. The public key encrypts a message and the message is decrypted with the private key of the recipient.

PVST
Per-VLAN Spanning Tree. PVST provides load balancing of VLANs across multiple ports resulting in optimal usage of network resources.

PVST+
Per-VLAN Spanning Tree+. PVST+ is an extension of the PVST standard that uses the 802.1Q trunking technology.

QoS
Quality of Service. It refers to the capability of a network to provide better service and performance to a specific network traffic over various technologies.

RA
Router Advertisement. The RA messages are sent by the routers in the network when the hosts send multicast router solicitation to the multicast address of all routers.

Radar
Radio Detection and Ranging. Radar is an object-detection system that uses radio waves to determine the range, angle, or velocity of objects.

RADIUS
Remote Authentication Dial-In User Service. An Industry-standard network access protocol for remote authentication. It allows authentication, authorization, and accounting of remote users who want to access network resources.

RAM
Random Access Memory.

RAPIDS
Rogue Access Point identification and Detection System. An AMP module that is designed to identify and locate wireless threats by making use of all of the information available from your existing infrastructure.

RARP
Reverse Address Resolution Protocol. RARP is a protocol used by a physical machine in a local area network for determining the IP address from the ARP table or cache of the gateway server.

Regex
Regular Expression. Regex refers to a sequence of symbols and characters defining a search pattern.

Registration Authority
Type of Certificate Authority that processes certificate requests. The Registration Authority verifies that requests are valid and comply with certificate policy, and authenticates the user's identity. The Registration Authority then forwards the request to the Certificate Authority to sign and issue the certificate.

Remote AP
Remote APs extend corporate network to the users working from home or at temporary work sites. Remote APs are deplyed at branch office sites and are connected to the central network on a WAN link.

REST
Representational State Transfer. REST is a simple and stateless architecture that the web services use for providing interoperability between computer systems on the Internet. In a RESTful web service, requests made to the URI of a resource will elicit a response that may be in XML, HTML, JSON or some other defined format.

RF
Radio Frequency. RF refers to the electromagnetic wave frequencies within a range of 3 kHz to 300 GHz, including the frequencies used for communications or Radar signals.

RFC
Request For Comments. RFC is a commonly used format for the Internet standards documentss.

RFID
Radio Frequency Identification. RFID uses radio waves to automatically identify and track the information stored on a tag attached to an object.

RIP
Routing Information Protocol. RIP prevents the routing loops by limiting the number of hops allowed in a path from source to destination.

RJ45
Registered Jack 45. RJ45 is a physical connector for network cables.

RMA
Return Merchandise Authorization. RMA is a part of the product returning process that authorizes users to return a product to the manufacturer or distributor for a refund, replacement, or repair. The customers who want to return a product within its Warranty period contact the manufacturer to initiate the product returning process. The manufacturer or the seller generates an authorization number for the RMA, which is used by the customers, when returning a product to the warehouse.

RMON
Remote Monitoring. RMON provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed LANs.

RoW
Rest of World. RoW or RW is an operating country code of a device.

RSA
Rivest, Shamir, Adleman. RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

RSSI
Received Signal Strength Indicator. RSSI is a mechanism by which RF energy is measured by the circuitry on a wireless NIC (0-255). The RSSI is not standard across vendors. Each vendor determines its own RSSI scale/values.

RSTP
Rapid Spanning Tree Protocol. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this.

RTCP
RTP Control Protocol. RTCP provides out-of-band statistics and control information for an Real-Time Transport Protocol session.

RTLS
Real-Time Location Systems. RTLS automatically identifies and tracks the location of objects or people in real time, usually within a building or other contained area.

RTP
Real-Time Transport Protocol. RTP is a network protocol used for delivering audio and video over IP networks.

RTS
Request to Send. RTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See CTS.

RTSP
Real Time Streaming Protocol. RTSP is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.

RVI
Routed VLAN Interface. RVI is a switch interface that forwards packets between VLANs.

RW
Rest of World. RoW or RW is an operating country code of a device.

SA
Security Association. SA is the establishment of shared security attributes between two network entities to support secure communication.

SAML
Security Assertion Markup Language. SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication.

SCEP
Simple Certificate Enrollment Protocol. SCEP is a protocol for requesting and managing digital certificates.

SCP
Secure Copy Protocol. SCP is a network protocol that supports file transfers between hosts on a network.

SCSI
Small Computer System Interface. SCSI refers to a set of interface standards for physical connection and data transfer between a computer and the peripheral devices such as printers, disk drives, CD-ROM, and so on.

SDN
Software-Defined Networking. SDN is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of the modern data center.

SDR
Server Derivation Rule. An SDR refers to a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on the rules defined under a server group. The SDRs override the default authentication roles and VLANs defined in the AAA and Virtual AP profiles.

SDU
Service Data Unit. SDU is a unit of data that has been passed down from an OSI layer to a lower layer and that has not yet been encapsulated into a PDU by the lower layer.

SD-WAN
Software-Defined Wide Area Network. SD-WAN is an application for applying SDN technology to WAN connections that connect enterprise networks across disparate geographical locations.

SFP
The Small Form-factor Pluggable. SFP is a compact, hot-pluggable transceiver that is used for both telecommunication and data communications applications.

SFP+
Small Form-factor Pluggable+. SFP+ supports up to data rates up to 16 Gbps.

SFTP
Secure File Transfer Protocol. SFTP is a network protocol that allows file access, file transfer, and file management functions over a secure connection.

SHA
Secure Hash Algorithm. SHA is a family of cryptographic hash functions. The SHA algorithm includes the SHA, SHA-1, SHA-2 and SHA-3 variants.

SIM
Subscriber Identity Module. SIM is an integrated circuit that is intended to securely store the International Mobile Subscriber Identity (IMSI) number and its related key, which are used for identifying and authenticating subscribers on mobile telephony devices.

SIP
Session Initiation Protocol. SIP is used for signaling and controlling multimedia communication session such as voice and video calls.

SIRT
Security Incident Response Team. SIRT is responsible for reviewing as well as responding to computer security incident reports and activity.

SKU
Stock Keeping Unit. SKU refers to the product and service identification code for the products in the inventory.

SLAAC
Stateless Address Autoconfiguration. SLAAC provides the ability to address a host based on a network prefix that is advertised from a local network router through router advertisements.

SMB
Server Message Block or Small and Medium Business. Server Message Block operates as an application-layer network protocol mainly used for providing shared access to files, printers, serial ports, and for miscellaneous communications between the nodes on a network.

SMS
Short Message Service. SMS refers to short text messages (up to 140 characters) sent and received through mobile phones.

SMTP
Simple Mail Transfer Protocol. SMTP is an Internet standard protocol for electronic mail transmission.

SNIR
Signal-to-Noise-Plus-Interference Ratio. SNIR refers to the power of a central signal of interest divided by the sum of the interference power and the power of the background noise. SINR is defined as the power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.

SNMP
Simple Network Management Protocol. SNMP is a TCP/IP standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMPv1
Simple Network Management Protocol version 1. SNMPv1 is a widely used network management protocol.

SNMPv2
Simple Network Management Protocol version 2. SNMPv2 is an enhanced version of SNMPv1, which includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications.

SNMPv2c
Community-Based Simple Network Management Protocol version 2. SNMPv2C uses the community-based security scheme of SNMPv1 and does not include the SNMPv2 security model.

SNMPv3
Simple Network Management Protocol version 3. SNMPv3 is an enhanced version of SNMP that includes security and remote configuration features.

SNR
Signal-to-Noise Ratio. SNR is used for comparing the level of a desired signal with the level of background noise.

SNTP
Simple Network Time Protocol. SNTP is a less complex implementation of NTP. It uses the same , but does not require the storage of state over extended periods of time.

SOAP
Simple Object Access Protocol. SOAP enables communication between the applications running on different operating systems, with different technologies and programming languages. SOAP is an XML-based messaging protocol for exchanging structured information between the systems that support web services.

SoC
System on a Chip. SoC is an Integrated Circuit that integrates all components of a computer or other electronic system into a single chip.

source NAT
Source NAT changes the source address of the packets passing through the router. Source NAT is typically used when an internal (private) host initiates a session to an external (public) host.

SSH
Secure Shell. SSH is a network protocol that provides secure access to a remote device.

SSID
Service Set Identifier. SSID is a name given to a WLAN and is used by the client to access a WLAN network.

SSL
Secure Sockets Layer. SSL is a computer networking protocol for securing connections between network application clients and servers over the Internet.

SSO
Single Sign-On. SSO is an access-control property that allows the users to log in once to access multiple related, but independent applications or systems to which they have privileges. The process authenticates the user across all allowed resources during their session, eliminating additional login prompts.

STBC
Space-Time Block Coding. STBC is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas and to exploit the various received versions of the data to improve the reliability of data transfer.

STM
Station Management. STM is a process that handles AP management and user association.

STP
Spanning Tree Protocol. STP is a network protocol that builds a logical loop-free topology for Ethernet networks.

subnet
Subnet is the logical division of an IP network.

subscription
A business model where a customer pays a certain amount as subscription price to obtain access to a product or service.

SU-MIMO
Single-User Multiple-Input Multiple-Output. SU-MIMO allocates the full bandwidth of the AP to a single high-speed device during the allotted time slice.

SVP
SpectraLink Voice Priority. SVP is an open, straightforward QoS approach that has been adopted by most leading vendors of WLAN APs. SVP favors isochronous voice packets over asynchronous data packets when contending for the wireless medium and when transmitting packets onto the wired LAN.

SWAN
Structured Wireless-Aware Network. A technology that incorporates a Wireless Local Area Network (WLAN) into a wired Wide Area Network (WAN). SWAN technology can enable an existing wired network to serve hundreds of users, organizations, corporations, or agencies over a large geographic area. SWAN is said to be scalable, secure, and reliable.

TAC
Technical Assistance Center.

TACACS
Terminal Access Controller Access Control System. TACACS is a family of protocols that handles remote authentication and related services for network access control through a centralized server.

TACACS+
Terminal Access Controller Access Control System+. TACACS+ provides separate authentication, authorization, and accounting services. It is derived from, but not backward compatible with, TACACS.

TCP
Transmission Control Protocol. TCP is a communication protocol that defines the standards for establishing and maintaining network connection for applications to exchange data.

TCP/IP
Transmission Control Protocol/ Internet Protocol. TCP/IP is the basic communication language or protocol of the Internet.

TFTP
Trivial File Transfer Protocol. The TFTP is a software utility for transferring files from or to a remote host.

TIM
Traffic Indication Map. TIM is an information element that advertises if any associated stations have buffered unicast frames. APs periodically send the TIM within a beacon to identify the stations that are using power saving mode and the stations that have undelivered data buffered on the AP.

TKIP
Temporal Key Integrity Protocol. A part of the WPA encryption standard for wireless networks. TKIP is the next-generation Wired Equivalent Privacy (WEP) that provides per-packet key mixing to address the flaws encountered in the WEP standard.

TLS
Transport Layer Security. TLS is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections above the Transport Layer by using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

TLV
Type-length-value or Tag-Length-Value. TLV is an encoding format. It refers to the type of data being processed, the length of the value, and the value for the type of data being processed.

ToS
Type of Service. The ToS field is part of the IPv4 header, which specifies datagrams priority and requests a route for low-delay, high-throughput, or a highly reliable service.

TPC
Transmit Power Control. TPC is a part of the 802.11h amendment. It is used to regulate the power levels used by 802.11a radio cards.

TPM
Trusted Platform Module. TPM is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.

TSF
Timing Synchronization Function. TSF is a WLAN function that is used for synchronizing the timers for all the stations in a BSS.

TSPEC
Traffic Specification. TSPEC allows an 802.11e client or a QoS-capable wireless client to signal its traffic requirements to the AP.

TSV
Tab-Separated Values. TSV is a file format that allows the exchange of tabular data between applications that use different internal data formats.

TTL
Time to Live. TTL or hop limit is a mechanism that sets limits for data expiry in a computer or network.

TTY
TeleTypeWriter. TTY-enabled devices allow telephones to transmit text communications for people who are deaf or hard of hearing as well as transmit voice communication.

TXOP
Transmission Opportunity. TXOP is used in wireless networks supporting the IEEE 802.11e Quality of Service (QoS) standard. Used in both EDCA and HCF Controlled Channel Access modes of operation, TXOP is a bounded time interval in which stations supporting QoS are permitted to transfer a series of frames. TXOP is defined by a start time and a maximum duration.

UAM
Universal Access Method. UAM allows subscribers to access a wireless network after they successfully log in from a web browser.

U-APSD
Unscheduled Automatic Power Save Delivery. U-APSD is a part of 802.11e and helps considerably in increasing the battery life of VoWLAN terminals.

UCC
Unified Communications and Collaboration. UCC is a term used to describe the integration of various communications methods with collaboration tools such as virtual whiteboards, real-time audio and video conferencing, and enhanced call control capabilities.

UDID
Unique Device Identifier. UDID is used to identify an iOS device.

UDP
User Datagram Protocol. UDP is a part of the TCP/IP family of protocols used for data transfer. UDP is typically used for streaming media. UDP is a stateless protocol, which means it does not acknowledge that the packets being sent have been received.

UDR
User Derivation Rule. UDR is a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on MAC address, BSSID, DHCP-Option, encryption type, SSID, and the location of a user. For example, for an SSID with captive portal in the initial role, a UDR can be configured for scanners to provide a role based on their MAC OUI.

UHF
Ultra high frequency. UHF refers to radio frequencies between the range of 300 MHz and 3 GHz. UHF is also known as the decimeter band as the wavelengths range from one meter to one decimeter.

UI
User Interface.

UMTS
Universal Mobile Telecommunication System. UMTS is a third generation mobile cellular system for networks. See 3G.

UPnP
Universal Plug and Play. UPnp is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi APs, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

URI
Uniform Resource Identifier. URI identifies the name and the location of a resource in a uniform format.

URL
Uniform Resource Locator. URL is a global address used for locating web resources on the Internet.

USB
Universal Serial Bus. USB is a connection standard that offers a common interface for communication between the external devices and a computer. USB is the most common port used in the client devices.

UTC
Coordinated Universal Time. UTC is the primary time standard by which the world regulates clocks and time.

UWB
Ultra-Wideband. UWB is a wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance.

VA
Virtual Appliance. VA is a pre-configured virtual machine image, ready to run on a hypervisor.

VBR
Virtual Beacon Report. VBR displays a report with the MAC address details and RSSI information of an AP.

VHT
Very High Throughput. IEEE 802.11ac is an emerging VHT WLAN standard that could achieve physical data rates of close to 7 Gbps for the 5 GHz band.

VIA
Virtual Intranet Access. VIA provides secure remote network connectivity for Android, Apple iOS, Mac OS X, and Windows mobile devices and laptops. It automatically scans and selects the best secure connection to the corporate network.

VLAN
Virtual Local Area Network. In computer networking, a single Layer 2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them through one or more routers; such a domain is referred to as a Virtual Local Area Network, Virtual LAN, or VLAN.

VM
Virtual Machine. A VM is an emulation of a computer system. VMs are based on computer architectures and provide functionality of a physical computer.

VoIP
Voice over IP. VoIP allows transmission of voice and multimedia content over an IP network.

VoWLAN
Voice over WLAN. VoWLAN is a method of routing telephone calls for mobile users over the Internet using the technology specified in IEEE 802.11b. Routing mobile calls over the Internet makes them free, or at least much less expensive than they would be otherwise.

VPN
Virtual Private Network. VPN enables secure access to a corporate network when located remotely. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

VRD
Validated Reference Design. VRDs are guides that capture the best practices for a particular technology in field.

VRF
VisualRF. VRF is an AirWave Management Platform (AMP) module that provides a real-time, network-wide views of your entire Radio Frequency environment along with floor plan editing capabilities. VRF also includes overlays on client health to help diagnose issues related to clients, floor plan, or a specific location.

VRF Plan
VisualRF Plan. A stand-alone Windows client used for basic planning procedures such as adding a floor plan, provisioning APs, and generating a Bill of Materials report.

VRRP
Virtual Router Redundancy Protocol. VRRP is an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN.

VSA
Vendor-Specific Attribute. VSA is a method for communicating vendor-specific information between NASs and RADIUS servers.

VTP
VLAN Trunking Protocol. VTP is a Cisco proprietary protocol for propagating VLANs on a LAN.

walled garden
Walled garden is a feature that allows blocking of unauthorized users from accessing network resources.

WAN
Wide Area Network. WAN is a telecommunications network or computer network that extends over a large geographical distance.

WASP
Wireless Application Service Provider. WASP provides a web-based access to applications and services that would otherwise have to be stored locally and makes it possible for customers to access the service from a variety of wireless devices, such as a smartphone or Personal Digital Assistant (PDA).

WAX
Wireless abstract XML. WAX is an abstract markup language and a set of tools that is designed to help wireless application development as well as portability. Its tags perform at a higher level of abstraction than that of other wireless markup languages such as HTML, HDML, WML, XSL, and more.

W-CDMA
Wideband Code-Division Multiple Access. W-CDMA is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices.

web service
Web services allow businesses to share and process data programmatically. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

WEP
Wired Equivalent Privacy. WEP is a security protocol that is specified in 802.11b and is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN.

WFA
Wi-Fi Alliance. WFA is a non-profit organization that promotes Wi-Fi technology and certifies Wi-Fi products if they conform to certain standards of interoperability.

WIDS
Wireless Intrusion Detection System. WIDS is an application that detects the attacks on a wireless network or wireless system.

Wi-Fi
Wi-Fi is a technology that allows electronic devices to connect to a WLAN network, mainly using the 2.4 GHz and 5 GHz radio bands. Wi-Fi can apply to products that use any 802.11 standard.

WiMAX
Worldwide Interoperability for Microwave Access. WiMAX refers to the implementation of IEEE 802.16 family of wireless networks standards set by the WiMAX forum.

WIP
Wireless Intrusion Protection. The WIP module provides wired and wireless AP detection, classification, and containment. It detects Denial of Service (DoS) and impersonation attacks, and prevents client and network intrusions.

WIPS
Wireless Intrusion Prevention System. WIPS is a dedicated security device or integrated software application that monitors the radio spectrum of WLAN network for rogue APs and other wireless threats.

WISP
Wireless Internet Service Provider. WISP allows subscribers to connect to a server at designated hotspots using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers called stations, to access the Internet and the web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.

WISPr
Wireless Internet Service Provider Roaming. The WISPr framework enables the client devices to roam between the wireless hotspots using different ISPs.

WLAN
Wireless Local Area Network. WLAN is a 802.11 standards-based LAN that the users access through a wireless connection.

WME
Wireless Multimedia Extension. WME is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE) and background (AC_BK). See WMM.

WMI
Windows Management Instrumentation. WMI consists of a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification.

WMM
Wi-Fi Multimedia. WMM is also known as WME. It refers to a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK).

WPA
Wi-Fi Protected Access. WPA is an interoperable wireless security specification subset of the IEEE 802.11 standard. This standard provides authentication capabilities and uses TKIP for data encryption.

WPA2
Wi-Fi Protected Access 2. WPA2 is a certification program maintained by IEEE that oversees standards for security over wireless networks. WPA2 supports IEEE 802.1X/EAP authentication or PSK technology, but includes advanced encryption mechanism using CCMP that is referred to as AES.

WSDL
Web Service Description Language. WSDL is an XML-based interface definition language used to describe the functionality provided by a web service.

WSP
Wireless Service Provider. The service provider company that offers transmission services to users of wireless devices through Radio Frequency (RF) signals rather than through end-to-end wire communication.

WWW
World Wide Web.

X.509
X.509 is a standard for a public key infrastructure for managing digital certificates and public-key encryption. It is an essential part of the Transport Layer Security protocol used to secure web and email communication.

XAuth
Extended Authentication. XAuth provides a mechanism for requesting individual authentication information from the user, and a local user database or an external authentication server. It provides a method for storing the authentication information centrally in the local network.

XML
Extensible Markup Language. XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

XML-RPC
XML Remote Procedure Call. XML-RPC is a protocol that uses XML to encode its calls and HTTP as a transport mechanism. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

ZTP
Zero Touch Provisioning. ZTP is a device provisioning mechanism that allows automatic and quick provisioning of devices with a minimal or at times no manual intervention.