AOS-W 8.3.0.0

Alcatel·Lucent
Enterprise

Release Notes

Contents 3
Revision History 5
Release Overview 6
Chapter Overview 6
Related Documents 6
Supported Browsers 7
Contacting Support 7
New Features and Enhancements 8
Supported Hardware Platforms 18
Switch Platforms 18
AP Platforms 18
Regulatory Updates 21
Resolved Issues 22
Known Issues and Limitations 42
Upgrade Procedure 53
Migrating from AOS-W 6.x to AOS-W 8.x 53
Important Points to Remember and Best Practices 54
Memory Requirements 54
Backing up Critical Data 55
Upgrading 57
Downgrading 60
Before You Call Technical Support 62

Glossary of Terms 63

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

This release of AOS-W includes new features and enhancements, fixes to issues identified in previous releases as well as new known and outstanding issues.

Throughout this document, branch Switch and local Switch are termed as managed device.

Chapter Overview

Use the following links to navigate to the corresponding topics:

- New Features and Enhancements on page 8 describes the new features and enhancements introduced in this release.
- Supported Hardware Platforms on page 18 describes the hardware platforms supported in this release.
- Resolved Issues on page 22 lists the issues resolved in this release.
- Known Issues and Limitations on page 42 lists the issues identified in this release.
- Upgrade Procedure on page 53 describes the procedures for upgrading your WLAN network to the latest AOS-W version.
- Glossary of Terms on page 63 lists the acronyms and abbreviations.

Related Documents

The following guides are part of the complete documentation for the Alcatel-Lucent user-centric network:

- *AOS-W Getting Started Guide*
- *AOS-W User Guide*
- *AOS-W CLI Reference Guide*
- *AOS-W Migration Guide*
- *AOS-W API Guide*
- *Alcatel-Lucent Mobility Master Licensing Guide*
- *Alcatel-Lucent Virtual Appliance Installation Guide*
- *Alcatel-Lucent Mobility Master Hardware Appliance Installation Guide*

Supported Browsers

The following browsers are officially supported for use with the AOS-W WebUI:

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Firefox 48 and higher on Windows 7, Windows 8, Windows 10 and Mac OS
- Apple Safari 8.0 or later on Mac OS
- Google Chrome

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://support.esd.alcatel-lucent.com
Email	ebg_global_supportcenter@al-enterprise.com
Service & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

This chapter describes the features and/or enhancements introduced in AOS-W 8.3.0.0.

AirMatch

AirMatch Channel and Power Allocation

The following AirMatch commands are introduced in AOS-W 8.3.0.0:

- **show airmatch debug apinfo**
- **show airmatch debug pathloss history rep-radio**

The following AirMatch commands are modified in AOS-W 8.3.0.0:

- **airmatch ap freeze** and **airmatch ap unfreeze** support both single radio and dual-radio APs.
- **airmatch runnow** - The **eirp** and **opmode** parameters are introduced.

The following fields are introduced in the output of the **show airmatch debug feasibility** command:

- Current Opmode
- HW Supported Opmodes
- Configured Opmodes
- Feasible Opmodes
- Eirp Range Chan 20MHz
- Eirp Range Chan 40MHz
- Eirp Range Chan 80MHz
- Eirp Range Chan 160MHz

Dual 5 GHz / Dual Band Operating Mode Selection

When **Dual 5GHz Mode** is set to **Automatic**, AirMatch automatically determines the optimal settings for dual 5 GHz capable APs to be either dual band (5 GHz and 2.4 GHz) or dual 5 GHz (both radios operating in 5 GHz), depending on AP density and RF environment. If **Dual 5GHz Mode** is set to **Enabled**, then AirMatch sets the AP to operate in dual 5 GHz band, and if set to **Disabled**, then the AP is set to dual band.

AP-Platform

Loop Protection

The loop protection feature detects and avoids the formation of loops on the Ethernet ports of OAW-APs, OAW-RAPs, or Mesh APs. The loop protection feature can be enabled on all APs that have multiple Ethernet ports and it supports tunnel, split-tunnel, and bridge modes.

303 Series Wireless Access Points

The 303 Series access points are high-performance dual-radio wireless devices that support IEEE 802.11ac Wave 2 standard. These APs use MIMO technology to provide secure wireless connectivity for both 2.4 GHz 802.11a/b/g/n wireless services and 5 GHz 802.11a/n/ac Wi-Fi.

These APs provide the following capabilities:

- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor
- Compatibility with IEEE 802.3af PoE
- Integrated BLE radio

For complete technical details and installation instructions, refer to the *Alcatel-Lucent 303 Series Campus Access Points Installation Guide*.

AP-318 Wireless Access Points

The 318 Series wireless access points support IEEE 802.11ac Wave 2 standard, delivering high performance with the MU-MIMO technology, while also supporting 802.11a/b/g/n wireless services.

These APs provide the following capabilities:

- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor
- IEEE 802.11a/b/g/n/ac spectrum monitor
- Compatibility with IEEE 802.3at PoE

For complete technical details and installation instructions, refer to the *Alcatel-Lucent 318 Series Wireless Access Points Installation Guide*.

340 Series Access Points

The 340 Series access points (AP-344 and AP-345) are high-performance dual-radio wireless devices. These access points provide secure wireless connectivity for 2.4 GHz 802.11 b/g/n and 5 GHz 802.11a/n/ac Wi-Fi networks. The optional dual 5 GHz radio mode allows both radios to operate in the 5 GHz radio mode simultaneously, doubling the 5 GHz capacity of the access point. The 340 Series access points can be deployed in either a Switch-based (AOS-W) or Switchless (Instant) network environment.

These APs provide the following capabilities:

- Wireless access

- Wireless mesh
- AM
- SM
- Support for selected USB peripherals
- Integrated BLE radio
- MU-MIMO (Wave 2) support

For complete technical details and installation instructions, refer to the *Alcatel-Lucent 340 Series Access Points Installation Guide*.

370 Series Outdoor Access Wireless Access Points

The 370 Series outdoor wireless access points (AP-374, AP-375, and AP-377 access points) support IEEE 802.11ac Wave 2 standard. They also deliver high performance with the MU-MIMO technology, in addition to supporting 802.11a/b/g/n wireless services.

These APs provide the following capabilities:

- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor
- IEEE 802.11a/b/g/n/ac spectrum monitor
- Compatibility with IEEE 802.3at PoE

For complete technical details and installation instructions, refer to the *Alcatel-Lucent 370 Series Outdoor Access Points Installation Guide*.

AP Fast Recovery

Starting from AOS-W 8.3.0.0, Alcatel-Lucent APs provide support for the AP Fast Recovery feature. On detecting a firmware assert, the AP executes the fast recovery process in the affected radio. This avoids rebooting the AP unnecessarily, thereby reducing the downtime of the AP in the network. If the AP detects a core dump with valuable information during a firmware assert, then it transfers the core dump to the managed device and reboots. A new parameter, **recovery-mode**, is introduced in the **ap system-profile** command to configure this feature.

Support for Huawei K5150 4G Modem

AOS-W 8.3.0.0 supports Huawei K5150 4G modems on managed devices and OAW-RAPs. This modem can be provisioned so that managed devices and OAW-RAPs can choose the available network automatically.

Support for ZTE MF831 4G Modem

AOS-W 8.3.0.0 supports ZTE MF831 4G modems on managed devices and OAW-RAPs. This modem can be provisioned so that managed devices and OAW-RAPs can choose the available network automatically.

Support for New ZTE 4G Modems on OAW-RAPs

Starting from AOS-W 8.3.0.0, ZTE MF832S and ZTE MF825C 4G modems are supported on OAW-RAPs.

Support for Dual 5 GHz Mode on 340 Series Access Points

Starting from AOS-W 8.3.0.0, 340 Series access points support dual 5 GHz radio operation. This is applicable to AP-344 and AP-345 access points. You can set this feature to enable, disable, or automatic mode using the WebUI or the CLI.

The **automatic** mode is only supported in Mobility Master-Managed Device deployments and is used with AirMatch.

The automatic dual 5 GHz selection mode is not supported on AP-344 access points.

Support for 3G/4G Provisioning

Starting from AOS-W 8.3.0.0, APs support the use of 3G and 4G USB modems to provide Internet backhaul to a network.

Support for Hotspot 2.0 R2

Starting from AOS-W 8.3.0.0, the Hotspot 2.0 R2 feature support is extended to 300 Series, OAW-AP303H, OAW-AP310 Series, OAW-AP320 Series, OAW-AP330 Series, 340 Series, OAW-AP365, OAW-AP367, and 370 Series access points in both Switch-based and Switchless modes.

Support for IAP-VPN Termination on Mobility Controller Virtual Appliance

Starting from AOS-W 8.3.0.0, Mobility Controller Virtual Appliance supports IAP-VPN termination by using custom certificates.

AP-Wireless

Support for 802.3bz

Starting from AOS-W 8.3.0.0, OAW-AP330 Series access points are compliant with 802.3bz standard. This is an IEEE standard-based support for 2.5 Gbps or 5 Gbps.

ARM

Client Match Enhancement

Starting from AOS-W 8.3.0.0, a new output field, **AS**, is supported in the output of the **show ap arm client-match history** command that displays the actual radio signal strength of the target AP at steer completion.

Load Balancing Interval

Starting from AOS-W 8.3.0.0, a new parameter, **cm-lb-interval** is added to the **rf arm-profile** command to control the interval at which the Client Match performs load balancing. This parameter applies to both spectrum and MU-MIMO load balancing that is performed by the Client Match.

The default value of this parameter is 5 minutes and the valid range is 0-255, where 0 is used to disable load balancing.

To display the load balancing interval, a new output field, **LB Invl(minutes)** is added to the output of the **show ap arm client-match debug state** command.

Advanced Transmit Rate Statistics

Starting from AOS-W 8.3.0.0, the output of the following commands include MCS bucket mapping information with channel width, number of spatial streams, and guard interval information of 802.11ac APs:

- **show ap debug radio-stats**
- **show ap debug bss-stats**
- **show ap debug client-stats**

Authentication

Enhancements to SSH Ciphers and MAC Algorithms

Starting from AOS-W 8.3.0.0, administrators can configure SSH to enable or disable the following ciphers and MAC authentication algorithms:

- HMAC-SHA1-96
- HMAC-SHA1
- AES-CBC
- AES-CTR

This enhancement is only supported in the non-FIPS mode of operation.

Base OS Security

Support for ASCOM Device-Type

Starting from AOS-W 8.3.0.0, ASCOM device-type is supported while performing device classification.

VIA Connection-Profile Enhancement

This enhancement provides the ability to mark outgoing IKE and ESP packets with custom DSCP, which is configured in managed devices by using the VIA connection-profile.

This enhancement is specifically for Android clients. This is already available for Windows clients.

A new parameter, **tos_dscp**, for marking custom DSCP is available under VIA connection-profile. The range of values allowed for this parameter is 0 to 63. This parameter is part of the **aaa authentication via connection-profile <profile>** command. You can configure this parameter by using the WebUI or CLI.

BLE

ZF Openmatics Support for ZF BLE Tag Communication

Starting from AOS-W 8.3.0.0, you can manage ZF Tags and implement the BLE location service using the third-party ZF Openmatics. To support this feature, Alcatel-Lucent APs with built-in IoT-protocol radio (BLE) are required. You can configure the APs to support ZF Openmatics using the IoT profiles.

IoT Endpoints

Starting from AOS-W 8.3.0.0, APs contain a built-in IoT protocol that can send BLE information containing payload messages to the endpoints over a WebSocket or HTTPS connection. An IoT Transport Profile is a global profile similar to the management server profile. It is used to transport state and statistics data to endpoints. Administrators can also restrict unauthorized profiles from being applied to the stand-alone and cluster-based APs.

Switch-Datapath

New Counter for Standby Managed Devices in a Cluster

Starting from AOS-W 8.3.0.0, a new counter, **current standby entries**, is added to the **station** parameter of the **show datapath** command. This counter provides information on standby managed devices in a cluster.

Switch-Platform

Support for OAW-4850 Switch Platform

The OAW-4850 Switch is a wireless LAN Switch that connects, controls, and intelligently integrates wireless APs and AMs into a wired LAN system.

This Switch has the following port configuration:

- 2 x 40 GbE (QSFP+) ports
- 8 x 10 GBase-X (SFP+) ports
- USB 2.0 interface
- Console port
- Micro USB console port
- Management port

For technical specifications and installation instructions, refer to the *OAW-4850 Switch Installation Guide*.

Cluster

Active AP Load Balancing Enhancement

Starting from AOS-W 8.3.0.0, the APs are redistributed based on the Active AP count and the standby APs are not considered. This ensures that fewer APs fail over when a managed device fails over.

CPsec

Control Plane Security Enhancements

Starting from AOS-W 8.3.0.0, a configurable parameter, **timer**, is added to the **control-plane-security** command. The default value of this parameter is 2 hours. When an AP does not come up on the Switch within the configured or default value of the CPsec expiry timer, the CPsec entry is revoked and is moved to the **unapproved-no-cert** state in the whitelist database table. Use the following commands to configure the **timer** parameter:

```
(host) [md] (config) #control-plane-security
(host) [md] (Control Plane Security Profile) #timer <timer>
```

IPsec

TLS-RSA Cipher Suites

Ciphers are used to configure the strength of the cipher suites as high, medium, or low by executing the **web-server profile** command.

Starting from AOS-W 8.3.0.0, the following ciphers are not supported only in FIPS builds:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_192_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_192_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_192_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288

The feature components that act as TLS clients do not propose the discontinued ciphers as part of the client **Hello** message.

The following subsections provide cipher-related details for FIPS and non-FIPS builds:

In FIPS Builds

- The static-key ciphers and static RSA ciphers are not supported but the web-server ciphers are always set to the default value, high.
- WebUI does not support static-key ciphers.
- EAP-TLS/EAP-PEAP for 802.1X termination supports static RSA ciphers.
- For RadSec, server-side changes are required to support ECDHE/DHE ciphers.

In non-FIPS Builds

- In web-server, different ciphers can be selected based on their strengths.
  - High – ECDHE and DHE ciphers
  - Medium – DHE and static RSA ciphers
  - Low – Only static RSA ciphers
- The WebUI does not support static-key ciphers.

Licensing

Support for Flex ACR License (LIC-ACR)

AOS-W 8.3.0.0 provides support for Flex ACR License.

Logging

CEF Enhancement

Starting from AOS-W 8.3.0.0, the syntax of a CEF message is enhanced to provide additional information. This allows ArcSight to interpret the CEF information more accurately.

The **Device Event Class ID**, **Name**, and **Severity** parameters are introduced in the syntax of the CEF message. The following example shows the CEF format in which Switches can send syslog messages.

```
CEF: Version|Device Vendor|Device Product|Device Version|Device Event Class ID|Name|Severity|[Extension]
```

MultiZone

Client Match Support

Starting from AOS-W 8.3.0.0, the Client Match features such as sticky-client and band steering are supported in a MultiZone deployment for Campus APs. Client Match in each zone functions independently by controlling clients that are associated to the Virtual APs owned by that zone.

Decrypt Tunnel Support

Starting from AOS-W 8.3.0.0, MultiZone supports Decrypt Tunnel forwarding mode on the data zone Virtual APs.

RSDB and Dual 5 GHz Bands Support for MultiZone

Starting from AOS-W 8.3.0.0, MultiZone supports RSDB on OAW-AP203R, OAW-AP203RP, and OAW-AP203H access points. Also, MultiZone supports Dual 5 GHz on AP-344 and AP-345 access points.

RADIUS

Support for RADIUS Accounting Session ID in RADIUS Access Request

Starting from AOS-W 8.3.0.0, the RADIUS access request, if configured, includes the RADIUS accounting session ID. Allow the RADIUS access-request to include the RADIUS accounting session ID by enabling the **radius-acct-session-id-in-access** parameter in the **aaa profile** command.

```
(host) [mynode] (config) #aaa profile default
(host) [mynode] (AAA Profile "default") #radius-acct-session-id-in-access
```

Tunnel Node

Support for Downloadable Roles for Per-user Tunneled Node Users

Starting from AOS-W 8.3.0.0, this feature allows the managed device to get the user role from the Alcatel-Lucent ClearPass Policy Manager server while tunneling wired user's traffic to the managed device.

Web Server

Supported SSL/TLS Protocol in FIPS Mode of Operation

Starting from AOS-W 8.3.0.0, the SSL or TLS protocol of the FIPS version supports only TLSv1.2 for secure communication with the web server. Use the **show web-server profile** command to display the configured TLS version. The output on execution of this command is as follows:

```
(host) [mynode]# show web-server profile

Web Server Configuration
------------------------
Parameter                                       Value
---------                                       -----
SSL/TLS Protocol Config                         tlsv1.2
Switch Certificate                              default
Captive Portal Certificate                      default
IDP Certificate                                 default
Management user's WebUI access method           username/password
User absolute session timeout <30-3600> (seconds)  0
User session timeout <30-3600> (seconds)        900
Maximum supported concurrent clients <25-320>   75
```

WebUI

WebUI Enhancements to Support Dual 5 GHz Mode

Starting from AOS-W 8.3.0.0, you can find the new **Dual 5GHz mode** option in the following paths:

- Configuration > System > Profiles > AP > AP system profile.
- Configuration > AP Groups > Profiles > AP > AP system > AP system profile: <profile-name> (make sure the Username > Preference > show advanced profiles option in the WebUI is enabled).

For a stand-alone Switch or a master Switch, the **Dual 5GHz mode** option is available in the **Configuration > AP Groups > <AP group profile-name> > Radio > Advanced** path.

When you select an AP-344 access point model in the Access Points table, you can see two additional gain parameters to set for Radio 0 and Radio 1 for Dual 5 GHz mode. Find these parameters in the following paths:

- Configuration > Access Points > Campus APs.
- Configuration > Access Points > Remote APs.
- Configuration > Access Points > Mesh APs.

The **Dashboard** page now displays graphs for details on the radios of Dual 5 GHz mode APs. To view the lower band radio and upper band radio details of a Dual 5 GHz mode AP, navigate to **Dashboard > Access Points > Access Points table** and select a 340 Series AP.

Support for Viewing Inheritance History

Starting from AOS-W 8.3.0.0, the WebUI allows you to view the inheritance details of any configuration at any group or node level. This feature is supported only for configurations that can be overridden. A blue color information icon is displayed in the respective rows of the configuration table under which some configurations are overridden. Clicking the icon displays the details of the inheritance with a link to the parent node. You can click on the parent node link to navigate to the parent node level. You can choose to remove all the overrides under the selected node level from the pop-up window by clicking the **Remove Overrides** button. Else, you can choose to remove the individual configuration overrides at the field level.

Support for WLAN Forwarding Mode Options

Starting from AOS-W 8.3.0.0, new WebUI options, **Split-Tunnel** and **Bridge** modes, are added to the **Forwarding mode** drop-down list in the **WLANs > General** page.

WebUI Support for Called Station ID in RADIUS Server Profile

Starting from AOS-W 8.3.0.0, Mobility Master provides WebUI support for configuring the **Called Station ID** parameters, such as **Station ID type**, **Station ID delimiter**, and **Include SSID** for a RADIUS server under the **Configuration** > **Authentication** > **Auth Servers** page of the WebUI.

This chapter describes the hardware platforms supported in AOS-W 8.3.0.0.

Switch Platforms

The following table displays the Switch platforms that are supported in AOS-W 8.3.0.0.

Table 3: *Supported Switch Platforms in AOS-W 8.3.0.0*

Switch Family	Switch Model
OAW-40xx Series	OAW-4005, OAW-4008, OAW-4010, OAW-4024, OAW-4030
OAW-4x50 Series	OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM, OAW-4850

AP Platforms

The following table displays the AP platforms that are supported in AOS-W 8.3.0.0.

Table 4: *Supported AP Platforms in AOS-W 8.3.0.0*

AP Family	AP Model
—	OAW-AP103, OAW-AP103H
OAW-AP100 Series	OAW-AP104, OAW-AP105
OAW-AP110 Series	OAW-AP114, OAW-AP115
OAW-AP130 Series	OAW-AP134, OAW-AP135
OAW-AP 170 Series	OAW-AP175AC, OAW-AP175AC-F1, OAW-AP175DC, OAW-AP175DC-F1, OAW-AP175P, OAW-AP175P-F1
OAW-AP200 Series	OAW-AP204, OAW-AP205

Table 4: *Supported AP Platforms in AOS-W 8.3.0.0*

AP Family	AP Model
—	OAW-AP203H
—	OAW-AP205H
—	OAW-AP207
203R Series	OAW-AP203R, OAW-AP203RP
OAW-AP210 Series	OAW-AP214, OAW-AP215
OAW-AP 220 Series	OAW-AP224, OAW-AP225
—	OAW-AP228
OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277
300 Series	OAW-AP304, OAW-AP305
—	AP-303
—	OAW-AP303H
OAW-AP310 Series	OAW-AP314, OAW-AP315
—	AP-318
OAW-AP320 Series	OAW-APAP-324, OAW-AP325
OAW-AP330 Series	OAW-AP334, OAW-AP335
340 Series	AP-344, AP-345
360 Series	OAW-AP365, OAW-AP367
370 Series	AP-374, AP-375, AP-377

Table 4: *Supported AP Platforms in AOS-W 8.3.0.0*

AP Family	AP Model
	OAW-RAP155, OAW-RAP155P
OAW-RAP100 Series	OAW-RAP108, OAW-RAP109
—	OAW-RAP3WN, OAW-RAP3WNP

Chapter 4
Regulatory Updates

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 Switch Command Line Interface (CLI) and execute the **show ap allowed-channels country-code <country-code> ap-type <ap-model>** command.

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 service.esd.alcatel-lucent.com.

The following default DRT file version is part of AOS-W 8.3.0.0:

- DRT-1.0_64450

This chapter describes the issues resolved in AOS-W 8.3.0.0.

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
114524	**Symptom:** Some APs displayed 270% channel utilization in the AP tables. The fix ensures that the APs do not display excessive utilization. **Scenario:** This issue was observed in APs running AOS-W 8.2.0.0.	AP-Wireless	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0
137108	**Symptom:** Users were unable to log in to VIA when they used special characters in the authentication password. This issue is resolved by configuring different encoding format types. **Scenario:** This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	RADIUS	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0
156908	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as **Kernel panic - not syncing: softlockup: hung tasks**. The fix ensures that the frames with sequence number 0 are inserted at the tail of the frames. **Scenario:** The issue occurred as the frames with sequence number 0 were inserted in an incorrect position. The issue was observed in APs running AOS-W 8.0.0.0 or later versions.	AP-Wireless	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0
161383 173575 176409	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Rebooting the AP because of FW HANG**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP305 and OAW-AP320 Series access points running AOS-W 8.2.0.0 or later versions.	AP-Wireless	OAW-AP305 and OAW-AP320 Series access points	AOS-W 8.2.0.1	AOS-W 8.3.0.0
162272	**Symptom:** A Mobility Master Virtual Appliance was unresponsive. This issue is resolved by disabling the serial console redirect. **Scenario:** This issue occurred during a kernel crash with the serial console redirect. This issue was observed in Mobility Master Virtual Appliances running AOS-W 8.2.0.0 on Hyper-V.	Switch-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
162735	**Symptom:** The **datapath** process in a managed device crashed and the managed device rebooted unexpectedly. The fix ensures that the managed device 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 managed devices running AOS-W 8.2.0.0.	Switch-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
164253	**Symptom:** The Remote AP console page, rapconsole.arubanetworks.com, displayed the old Alcatel-Lucent logo for a stand-alone Remote AP. The fix ensures that the new HPE-Alcatel-Lucent logo is displayed. **Scenario:** This issue was observed in Remote APs running AOS-W 8.2.0.0.	Remote AP	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
165595	**Symptom:** A managed device 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 these incorrect error messages are not displayed in the logs. **Scenario:** This issue occurred when a backup Virtual AP was configured for another AP. This issue was observed in APs running AOS-W 8.2.0.0.	Air Management-IDS	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
165788	**Symptom:** A user was unable to remove stale entries from a standby Mobility Master. The fix allows the user to delete stale entries from the standby Mobility Master. **Scenario:** This issue was observed in a standby Mobility Masters running AOS-W 8.2.0.0 or later versions in a master-standby topology.	Station Management	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
166272 173020	**Symptom:** Clients were unable to connect to virtual IPs through the Hot Standby Router Protocol (HSRP) or Gateway Load Balancing Protocol (GLBP). The fix ensures that clients are able to connect to virtual IPs. **Scenario:** This issue occurred when clients used the L2 GRE tunnel to connect to virtual IPs, and Broadcast and Multicast Optimization was enabled on the VLAN. This issue was observed in managed devices running AOS-W 8.1.0.0 or later versions.	Routing	All platforms	AOS-W 8.1.0.0	AOS-W 8.3.0.0
167028	**Symptom:** The SNMP walk reported that an AP's port speed was greater than 1 Gbps on a 1 Gbps Ethernet Port. The fix ensures that the correct AP port speed is displayed. **Scenario:** This issue occurred because the **STM** process incorrectly calculated the Ethernet port speed. This issue was observed in APs running AOS-W 8.0.1.0 or later versions.	Air Management - IDS	All platforms	AOS-W 8.0.1.0	AOS-W 8.3.0.0
167198 177034	**Symptom:** An AP crashed and rebooted. The log file listed the reason for the event as **Reboot caused by kernel panic: softlockup: hung tasks**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred due to an interruption while sending multicast data to the AP. This issue was observed in OAW-AP303H, OAW-AP304, OAW-AP305, OAW-AP365, and OAW-AP367 access points running AOS-W 8.2.0.0.	AP Datapath	OAW-AP303H, OAW-AP304, OAW-AP305, OAW-AP365, and OAW-AP367 access points	AOS-W 8.2.0.0	AOS-W 8.3.0.0
167572	**Symptom:** A correct role was not assigned to a user. The fix ensures that a correct role is assigned to the user. **Scenario:** This issue occurred when a user role was configured in uppercase but the managed device identified the user role in lowercase. This issue was observed in managed devices running AOS-W 8.1.0.1 or later versions.	Role/VLAN Derivation	All platforms	AOS-W 8.1.0.1	167572
167706	**Symptom:** A managed device 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 managed device works as expected. **Scenario:** This issue occurred when few leaked packets were not handled properly in SOS. This issue was observed in OAW-4x50 Series Switches running AOS-W 8.0.0.0 or later versions.	Switch-Datapath	OAW-4x50 Series Switches	AOS-W 8.0.0.0	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
168146	**Symptom:** A Mobility Master Hardware Appliance failed to download the Activate whitelist from a managed device. The fix ensures that the Mobility Master Hardware Appliance successfully downloads the whitelist from a managed device. **Scenario:** This issue was observed in Mobility Master Hardware Appliances running AOS-W 8.1.0.2 or later versions.	Switch-Platform	All platforms	AOS-W 8.1.0.2	AOS-W 8.3.0.0
168457	**Symptom:** The ACR license count was not updated to the applications running on a standby Mobility Master until a failover happened. The fix ensures that the ACR license limits are updated to the applications as soon as the database synchronizes. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions in a master-standby topology.	Licensing	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0
168485	**Symptom:** The AeroScout Location Engine was unable to receive Wi-Fi tags from the server. The fix ensures that the AeroScout Location Engine is able to 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 APs running AOS-W 8.2.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
168789	**Symptom:** APs with an 802.1X supplicant configuration failed to boot. The fix ensures that APs with the 802.1X configuration are able to boot. **Scenario:** This issue occurred when an ACL denied DNS response from a DNS server. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
168971 169581 169880 171920 173550	**Symptom:** An AP stopped responding and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: Fatal exception in interrupt**. Improvements to the AP wireless driver resolved the issue. **Scenario:** This issue occurred due to a memory corruption of the AP. This issue was observed in 300 Series, OAW-AP303H, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points running AOS-W 8.1.0.0 in Mesh mode.	Mesh	300 Series, OAW-AP303H, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series points	AOS-W 8.1.0.0	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169010 169073 173330 175788	**Symptom:** An AP failed to respond and rebooted unexpectedly. The log file listed the reason for the event as **Unhandled fault: external abort on non-linefetch (0x1008) at 0xe6000000**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in 300 Series access points running AOS-W 8.2.0.0.	AP-Platform	300 Series access points	AOS-W 8.2.0.0	AOS-W 8.3.0.0
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 OAW-AP275 access points running AOS-W 8.2.0.0.	Mesh	OAW-AP275 access points	AOS-W 8.2.0.0	AOS-W 8.3.0.0
169151	**Symptom:** Some Windows clients detected IP address conflict with a Mobility Master. The fix ensures that Windows clients do not detect IP address conflicts when OpenFlow is enabled. **Scenario:** This issue occurred if the client sent an ARP probe when OpenFlow was enabled on the Mobility Master. This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	Switch-Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
169327	**Symptom:** A Mobility Master displayed the **An internal system error has occurred at file server_group.c function cfg_server_group_item_int line 384 error Error: unknown server** error. The fix ensures that the repositioned server configurations are sent to the managed device. **Scenario:** This issue occurred when the authentication server in the server group was repositioned, but the new position was not sent to the managed device. This issue was observed in Mobility Masters running AOS-W 8.1.0.3 or later versions.	Base OS Security	All platforms	AOS-W 8.1.0.3	AOS-W 8.3.0.0
169540 175490	**Symptom:** The **STM** process in a managed device crashed multiple times. The fix ensures that the number of virtual APs is set after validating 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 the maximum number of SSIDs. This issue was observed in managed devices running AOS-W 8.2.0.0.	Switch- Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169749	**Symptom:** A client was unable to connect to 5 GHz radio on some APs. Improvements to the wireless driver resolved this issue. **Scenario:** This issue occurred because radio 0 did not transmit traffic. This issue was observed in OAW-AP325 access points running AOS-W 8.0.0.0 or later versions.	AP-Wireless	OAW-AP325 access points	AOS-W 8.0.0.0	AOS-W 8.3.0.0
170037	**Symptom:** APs configured with static IP addresses failed to discover the WLAN Switch through ADP or DNS. The fix ensures that APs are able to discover the WLANs accurately. **Scenario:** This issue occurred when an ACL denied Tx ADP packets. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
170111 177361	**Symptom:** The **STM** process in a Mobility Master stopped responding after executing the **clear gap-db stale** command. The fix ensures that the **STM** process works as expected upon executing the command. **Scenario:** This issue occurred in a cluster topology with load balancing enabled. This issue was observed in Mobility Masters running AOS-W 8.1.0.2 or later versions.	AP-Platform	All platforms	AOS-W 8.1.0.2	AOS-W 8.3.0.0
170171	**Symptom:** A **web server** process that handles captive portal requests crashed intermittently in a managed device. The fix ensures that the **web server** process does not crash. **Scenario:** This issue occurred when there was an increase in the captive portal requests sent to the managed device. This issue was observed in managed devices running AOS-W 8.2.0.0.	Captive Portal	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
170346	**Symptom:** Some clients were unable to connect to an AP. The fix ensures that the clients connect to the APs without service interruption. **Scenario:** This issue occurred because the whitelist database of Campus AP was missing in the managed device and when irrelevant log messages in the log file consumed memory. This resulted in missing whitelist database entries. This issue was observed in managed devices running AOS-W 8.2.0.0.	Database	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
170457	**Symptom:** A managed device dropped VLAN probe requests causing the cluster to remain in L3 connected state. The fix ensures that the managed device does not drop VLAN probe requests when the **bcmc-optimization** parameter is enabled. **Scenario:** This issue occurred when **bcmc-optimization** parameter was enabled on the VLAN interface after reloading the managed device in the cluster. This issue was observed in cluster setups running AOS-W 8.2.0.0 or later versions.	Cluster Manager	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
170803 171109	**Symptom:** A managed device stopped responding and rebooted. The log file listed the reason for the event as **Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred due to a memory leak on the managed device. This issue was observed in managed devices running AOS-W 8.2.0.0.	Switch-Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
171113	**Symptom:** Bandwidth contracts in the target role were not applied to a split-tunnel user. The fix ensures that bandwidth contracts are applied to the split-tunnel user. **Scenario:** This issue occurred when RFC 3576 CoA was used to change the role of the split-tunnel user. This issue was not limited to any specific platform or AOS-W version.	AP Datapath	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0
171316	**Symptom:** A managed device displayed the **dot1x_gsm_set_ pmkcache(): GSM: Failed to publish PMK-cache object. Error:error_no_free_slots** error. The fix ensures that the managed device does not display the error. **Scenario:** This issue occurred when the PMK cache GSM channel was full. This issue was observed in cluster setups running AOS-W 8.2.0.1.	Base OS Security	All platforms	AOS-W 8.2.0.1	AOS-W 8.3.0.0
171379	**Symptom:** Multiple core dumps were observed in OAW-AP325 access points. The fix ensures that the packets with invalid lengths are not processed. **Scenario:** This issue occurred when the wireless driver sent packets with invalid lengths to the AP. This issue was observed in OAW-AP325 access points running AOS-W 8.0.0.0 or later versions.	Air Management - IDS	OAW-AP325 access points	AOS-W 8.0.0.0	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171521 175748	**Symptom:** The captive portal redirect was not triggered for a Linux-based client. The fix ensures that the captive portal redirect for Linux-based clients is successful. **Scenario:** This issue occurred when Linux-based clients used the additional Resource Record (RR) options in the DNS request and DNS response returned **no such name** instead of the IP address of the managed device. This issue was observed in managed devices running AOS-W 8.2.0.0.	Switch-Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
171611	**Symptom:** Static route entries were missing in the managed device. Hence the managed device was disconnected from the Mobility Master. The fix ensures that the **ISAMKPD** process uses the correct crypto map during IKE or IPsec tunnel initiation. **Scenario:** This issue occurred when **masterip, vpnip,** and **vpn-peer peer-mac** commands pointed to the same MAC address and the **ISAMKPD** process used a wrong crypto map during IKE or IPsec tunnel initiation. This issue was observed in managed devices running AOS-W 8.1.0.4 or later versions.	IPsec	All platforms	AOS-W 8.1.0.4	AOS-W 8.3.0.0
171614 172310 174525 175401	**Symptom:** The **Datapath** process on a managed device crashed. 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 process does not crash due to invalid memory access. **Scenario:** This issue occurred due to an invalid memory access. This issue was observed in managed devices running AOS-W 8.1.0.4 or later versions.	Switch-Datapath	All platforms	AOS-W 8.1.0.4	AOS-W 8.3.0.0
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 unable to send or receive traffic. The fix ensures that the client obtains an IP address and can send or receive traffic. **Scenario:** This issue occurred because both wired and wireless clients had a common VLAN. This issue was observed in APs running AOS-W 8.0.0.0 or later versions.	AP Datapath	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
172534	**Symptom:** WEP clients were unable to pass traffic after a cluster failover. The fix ensures that the clients are able to pass traffic after the cluster failover. **Scenario:** This issue occurred when dynamic WEP keys were not synchronized in a cluster. This issue was observed in cluster setups running AOS-W 8.1.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.1.0.0	AOS-W 8.3.0.0
172665	**Symptom:** A managed device did not clear the stale internal-user entries of IPsec tunnels from an HPE switch. The **aaa user delete** command displayed the following error message: **User delete for HP switches is not supported**. This issue is resolved by allowing deletion of the HPE switch user entries. **Scenario:** This issue occurred when a managed device included the HPE switch users as trusted users but omitted them from ageout user deletion. The HPE switch users were retained as stale internal-user entries even after IPsec sessions between users and the managed device were terminated. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	IPsec	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0
172801 175444 176229	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as, **kernel panic: Fatal exception**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP225 access points running AOS-W 8.0.0.0 or later versions.	AP-Wireless	OAW-AP225 access points	AOS-W8.0.0.0	AOS-W 8.3.0.0
173083	**Symptom:** The WebUI displayed the OmniAccess Mobility Controller label for a standby Mobility Master. The fix ensures that the WebUI displays the Mobility Master label for the standby Mobility Master. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.2.0.1 or later versions.	WebUI	All platforms	AOS-W 8.2.0.1	AOS-W 8.3.0.0
173230	**Symptom:** A OAW-RAP rebooted unexpectedly. The log file listed the reason for this event as **Missed heartbeats**. The fix ensures that the OAW-RAP works as expected. **Scenario:** This issue occurred when **Tx queue** in the **IPsec** process was stuck. This issue was observed in OAW-RAP155 access points running AOS-W 8.0.0.0.	AP-Platform	OAW-RAP155 access points	AOS-W 8.0.0.0	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
173328	**Symptom:** The **block-redirect-url** configuration on an active Mobility Master did not synchronize with the standby Mobility Master. The fix ensures that the **block-redirect-url** configuration is updated on the standby Mobility Master. **Scenario:** This issue occurred in Mobility Masters running AOS-W 8.0.0.0 or later versions in an active-standby topology.	WebCC	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
173422 173483 173576	**Symptom:** The **Dashboard** page of a Mobility Master incorrectly displayed the status of some APs as DOWN although the APs were UP. The fix ensures that the Mobility Master correctly displays the status of APs. **Scenario:** This issue occurred when all SSIDs in an AP group were disabled. This issue was observed in Mobility Masters running AOS-W 8.2.0.1 or later versions.	Monitoring	All platforms	AOS-W 8.2.0.1	AOS-W 8.3.0.0
173441	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as, **kernel panic**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in APs running AOS-W 8.0.0.0 or later versions.	AP-Wireless	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0
173554	**Symptom:** The IDS logs and SNMP traps included WVE ID hyperlinks that were invalid. The fix ensures that the WVE information is removed from all IDS logs. **Scenario:** This issue was not limited to any specific Switch model or AOS-W release version.	Air Management-IDS	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0
173772	**Symptom:** When a user tried to map a VLAN name to a user role the CLI displayed **Invalid Named VLAN**. The fix ensures that the user is able to map the VLAN name to the user role. **Scenario:** This issue occurred when a VLAN name was automatically stored in lowercase. This issue was observed in managed devices running AOS-W 8.1.0.4 or later versions.	VLAN	All platforms	AOS-W 8.1.0.4	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
173868	**Symptom:** Users with the same static IP address failed to pass traffic when connected to an SSID. The fix ensures that the static IP address successfully passes traffic when connected to the SSID. **Scenario:** This issue occurred when **prohibit-ip-spoofing** parameter was disabled in the firewall settings. This issue was observed in managed devices running AOS-W 8.1.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.1.0.0	AOS-W 8.3.0.0
173993	**Symptom:** IDS incorrectly detected rogue APs on a secure network. The fix ensures that wired clients do not introduce invalid wired MAC addresses into the Ethernet MAC list. **Scenario:** This issue occurred when a client moved from an external wireless network to a wired corporate network. This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	Air Management-IDS	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0
174001	**Symptom:** A Mobility Master failed to send SNMPv3 **INFORM** traps to OmniVista 3600 Air Manager. The fix ensures that the Mobility Master sends SNMPV3 **INFORM** traps to OmniVista 3600 Air Manager. **Scenario:** This issue occurred after the Mobility Master rebooted. This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	SNMP	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0
174287	**Symptom:** An AP incorrectly operated in restricted mode (indicated by a flashing system LED) though the uplink speed was set to an optimal value. The fix ensures that the AP operates in the correct mode. **Scenario:** This issue was observed in OAW-AP330 Series access points running AOS-W 8.0.0.0 or later versions.	AP Platform	OAW-AP330 Series access points	AOS-W 8.2.0.1	AOS-W 8.3.0.0
174336	**Symptom:** APs crashed and rebooted intermittently. The log file listed the reason for the event as **External watchdog reset** and **kernel panic: Fatal exception**. The fix ensures that APs do not crash and reboot. **Scenario:** This issue was observed in OAW-AP200 Series access points running AOS-W 8.2.0.0 or later versions.	AP-Wireless	OAW-AP200 Series access points	AOS-W 8.2.0.0	AOS-W 8.3.0.0
174337	**Symptom:** IDS tarpit containment was inconsistent in access points. The issue is resolved by ensuring that tarpit frames are sent on the same channel as that of the target device. **Scenario**: This issue occurred when APs were configured in AM mode and the tarpit frames were sent out on the wrong channel. This issue was observed in APs, but is not restricted to any AOS-W version.	Air Management - IDS	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
174495 176334	**Symptom:** The **show configuration effective** command output displayed **inherited from [/sc]** for some configuration details. This issue is resolved by fixing the command output to display **inherited from [/mm]**. **Scenario:** This issue occurred because **/sc** was not replaced with **/mm** in some file instances. This issue was observed in a Managed Device - Mobility Master Virtual Appliance topology.	Configuration	All platforms	AOS-W 8.2.1.0	AOS-W 8.3.0.0
174533	**Symptom:** SNMP traps with interface name and interface description were not available as part of **wlsxPortDown** and **wlsxPortUp**. The fix ensures that SNMP traps with the interface name and interface description are available. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.0.	SNMP	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
174615	**Symptom:** Cluster VRRP flapping was observed when threshold values on a managed device were modified. This issue is resolved by retaining VRRP flaps when the cluster parameters are modified. **Scenario:** This issue occurred when the cluster manager added or deleted the VRRP instances multiple times. This issue was observed in managed devices running AOS-W 8.2.0.2 or later versions.	VRRP	All platforms	AOS-W 8.2.0.2	AOS-W 8.3.0.0
174644 174925	**Symptom:** AirGroup lost all the learned server and user details and also failed to learn any new user or server. The fix ensures that AirGroup learns all users and servers appropriately. **Scenario:** This issue occurred whenever an AirGroup service or profile was modified. This issue was observed in AOS-W 8.2.0.0 or later versions.	AirGroup	All platforms	AOS-W 8.2.0.2	AOS-W 8.3.0.0
174670	**Symptom:** An LACP port channel received multiple warning messages, **LACP: Disabling Collection and Distribution on port 0/0/0 LAG 0**. The fix ensures that the port channel does not receive these warning messages. **Scenario:** This issue occurred when the port channel was in trusted mode and trusted VLAN list for the port channel did not have default VLAN in its list. This issue was observed in stand-alone Switches running AOS-W 8.2.0.2 or later versions.	Port-Channel	All platforms	AOS-W 8.2.0.2	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
174788	**Symptom:** Mobility Masters incorrectly allowed users to execute the **aaa user delete** command from the **/mm** or **/mm/mynode** levels. However, the command was not effective because it was applicable only at the managed device level (**/md/<device>**). The fix ensures that an error message is displayed when executing the command from the **/mm** or **/mm/mynode** levels. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.2.0.2	AOS-W 8.3.0.0
174823 175163	**Symptom:** The **Authentication** process in a managed device crashed unexpectedly. The fix ensures that the **Authentication** process does not crash. **Scenario:** This issue occurred when the **aaa test-server verbose** command was executed. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0
174865	**Symptom:** Some clients moved to 802.1X authentication although they failed MAC authentication. This issue is resolved by not allowing clients that fail MAC authentication to move to 802.1X authentication. **Scenario:** This issue occurred when L2 fail-through was disabled. This issue was observed in Mobility Masters running AOS-W 8.0.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0
174955	**Symptom:** The **Dashboard** > **UCC** > **Calls Per Device Type** > **Table** tab displayed **0** call records under the **Last Hr** column. The fix ensures that the call records are displayed correctly. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.2.1.0 or later versions.	WebUI	All platforms	AOS-W 8.2.1.0	AOS-W 8.3.0.0
174979	**Symptom**: The size of the **ale.log** file on a Mobility Master was large. This issue is resolved by updating only the consolidated data to the **ale.log** file once a day. **Scenario**: This issue occurred due to frequent processing of AMON messages. This issue was observed in Mobility Masters running AOS-W 8.2.0.0 or later versions.	NBAPI	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
175061	**Symptom:** The system time of a managed device was displayed incorrectly. The fix ensures that correct time is displayed on the managed device. **Scenario:** This issue occurred when the **NTPD** process in a managed device used a local interface during boot time. The local interface did not have a route to the NTP server and hence the system time of the managed device was not synchronized. This issue was observed in a managed devices running AOS-W 8.2.0.0 or later versions.	Switch-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
175268	**Symptom:** The output of **show ap debug client-table** command displayed incorrect Tx-Retries. The fix ensures that accurate Tx-Retries are displayed. **Scenario:** This issue was observed in 300 Series access points connected to managed devices running AOS-W 8.0.0.0.	AP Datapath	300 Series access points	AOS-W 8.0.0.0	AOS-W 8.3.0.0
175333	**Symptom:** Clients were unable to pass traffic. The fix ensures that clients can pass traffic. **Scenario:** This issue was observed in OAW-AP325 access points running AOS-W 8.0.0.0.	AP-Platform	OAW-AP325 access points	AOS-W 8.0.0.0	AOS-W 8.3.0.0
175340	**Symptom:** The AP logs for a OAW-RAP displayed the error message, **connect-debounce failed, port 1 disabled**. The fix ensures that this error is not displayed. **Scenario:** This issue was observed in OAW-RAP3WNP access points running AOS-W 8.0.0.0.	AP-Platform	OAW-RAP3WNP access points	AOS-W 8.0.0.0	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
175387	**Symptom:** APs blocked ARP requests which had the same IP address as that of local DHCP server of AP. The fix ensures the following: ■ AP datapath does not block the ARP request from the AP with the DHCP VLAN address. ■ If there is a wired or wireless client connected to AP and has the same IP address, the ARP reply is dropped by ARP as an ARP spoof. But, if this IP address does not belong to a client that is connected to AP, the ARP reply is forwarded. **Scenario:** This issue occurred when a route-cache entry was added with the AP local DHCP address and VLAN. But, when an ARP request which was with the same IP address as that of the AP's DHCP server was received by the AP, the AP datapath dropped the ARP request due to a mismatch in VLAN information. This issue was observed in APs running AOS-W 8.0.0.0 or later versions.	AP Datapath	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0
175741	**Symptom:** LLDP-MED did not get enabled on the ports E1 through E3 of an AP although the configuration was applied on all ports. The fix ensures that LLDP-MED gets enabled on the ports E1 through E3. **Scenario:** This issue was observed in OAW-AP203R and OAW-AP203RP access points running AOS-W 8.2.0.0 or later versions.	AP Datapath	OAW-AP203R and OAW-AP203RP access points	AOS-W 8.2.0.0	AOS-W 8.3.0.0
175763	**Symptom:** The **mDNS** process crashed and rebooted frequently on a managed device. The fix ensures that the crash does not occur. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.1 or later versions.	AirGroup	All platforms	AOS-W 8.2.0.1	AOS-W 8.3.0.0
175841	**Symptom:** An AirGroup server table or AirGroup user table displayed stale entries. The fix ensures that the AirGroup server table or AirGroup user table does not display stale entries. **Scenario:** This issue was observed in Mobility Masters running AOS-W 8.2.0.2.	AirGroup	All platforms	AOS-W 8.2.0.1	AOS-W 8.3.0.0
175852	**Symptom:** A managed device displayed the **Save failed: Module Authentication is busy. Please try later** error when the user attempted to save the configuration. The fix ensures that users are able to save the configuration changes in the managed device. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
175945	**Symptom:** A stand-alone Switch acting as a DHCP server for multiple VLAN pools tagged DHCP-offer packets with the wrong VLAN. The fix ensures that the DHCP-offer packets are tagged with the correct VLAN. **Scenario:** This issue was observed in stand-alone Switches running AOS-W 8.0.0.0.	VLAN	All platforms	AOS-W 8.0.0.0	AOS-W 8.3.0.0
175974 176628	**Symptom:** The jumbo configuration on port channel did not apply to a 40 gibabitethernet member interface after a reload of the managed device. This issue is resolved by ensuring that the jumbo configuration to member ports is applied when ports are added. **Scenario:** This issue occurred because FPAPPS received the port channel configuration earlier than the member ports information from LAGM. After the managed device reloaded, the MTU size was 1752 bytes instead of 9216 bytes. This issue was observed in OAW-4850 managed devices running AOS-W 8.2.1.0.	Port-Channel	All platforms	AOS-W 8.2.1.0	AOS-W 8.3.0.0
176001	**Symptom:** The output of the **show amon-receiver interest-table** command did not display AMON message registrations although the **nbapi_publish** parameter was enabled in the **ale-configuration** command. The fix ensures that AMON message registrations are displayed. **Scenario:** This issue occurred when a Mobility Master was reloaded immediately after enabling the **nbapi_publish** parameter. This issue was observed in Mobility Masters running AOS-W 8.2.1.0 or later versions.	NBAPI	All platforms	AOS-W 8.2.1.0	AOS-W 8.3.0.0
176029	**Symptom:** The CLI help text for the **tunnel** parameter in the **via connection-profile** command did not show the maximum number of VIA tunneled networks that can be configured. This issue is resolved by modifying the CLI help text so that users are aware of the maximum limits. **Scenario:** Without this help text, users were unable to know the maximum number of allowed VIA tunneled network configurations. This issue was not limited to any specific platform or AOS-W version.	CLI	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
176118	**Symptom:** Users were unable to save the changes that were made in the **Guest Email** tab under **Mobility Master** > **Configuration** > **Services** > **Guest Provisioning** > **Guest Email** page. The fix ensures that users are able to save the changes. **Scenario:** This issue occurred when users attempted to edit and save the changes that were already configured in the WebUI. This issue was observed in Mobility Masters running AOS-W 8.2.0.2 or later versions.	WebUI	All platforms	AOS-W 8.2.0.2	AOS-W 8.3.0.0
176322	**Symptom:** An AP received the IP address from an incorrect VLAN although the VLAN was changed through **device-profile** on the switch. This issue is resolved by ensuring that the AP receives the IP address from the correct VLAN. **Scenario:** This issue occurred because the switch VLAN configuration did not change before the AP sent the DHCP information. This issue was observed in APs running AOS-W 8.1.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.1.0.0	AOS-W 8.3.0.0
176344	**Symptom:** The cached ACR licenses were not preserved on the licensing server after upgrading a Mobility Master. The fix ensures that the cached ACR licenses are preserved. **Scenario:** This issue occurred when a Mobility Master was upgraded to AOS-W 8.2.0.0 or later versions. This issue was not limited to any specific platform.	Licensing	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
176404	**Symptom:** An AP did not send GARP, when initialization was in progress. The fix ensures that the AP sends GARP when an interface is UP. **Scenario:** This issue occurred when an IP address was assigned to the interface. So, when a new AP was statically allocated with an old AP's IP address, the devices on the LAN were not notified and the ARP table was not updated. As a result, devices had to wait for the ARP entry to expire or for the new AP to send a message. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AP Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
176430	**Symptom:** Some APs sent ARP requests for a gateway with an incorrect IP address. The fix ensures that the APs send correct IP addresses for ARP request. **Scenario:** The issue occurred in the following scenarios: ■ When APs disconnected from the managed device. ■ When the DHCP server was unreachable. ■ When the gateway was unreachable. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AP Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
176444	**Symptom:** The startup wizard did not allow adding licenses to a stand-alone Switch. The fix ensures that the licenses are added successfully. **Scenario:** This issue was observed in stand-alone Switches running AOS-W 8.2.1.0.	Switch - Platform	All platforms	AOS-W 8.2.1.0	AOS-W 8.3.0.0
176607	**Symptom:** A client that was connected to an AP failed to obtain an IP address. The fix ensures that the client obtains an IP address. **Scenario:** This issue occurred due to a memory leak in the APs with onboard or USB-based BLE radios. This issue was observed in OAW-AP203H, 203R Series, OAW-AP205H, OAW-AP210 Series, OAW-AP 220 Series, 300 Series, OAW-AP310 Series, OAW-AP320 Series, OAW-AP330 Series, 340 Series, 360 Series, and 370 Series access points running AOS-W 8.2.0.0 or later versions.	BLE	OAW-AP203H, 203R Series, OAW-AP205H, OAW-AP210 Series, OAW-AP 220 Series, 300 Series, OAW-AP310 Series, OAW-AP320 Series, OAW-AP330 Series, 340 Series, 360 Series, and 370 Series access points	AOS-W 8.2.0.0	AOS-W 8.3.0.0
176801	**Symptom:** The LMS Preemption did not work in a cluster setup. This issue is resolved by configuring the LMS and Backup LMS correctly. **Scenario:** This issue was observed when a backup LMS was configured as master and **active load balance** was enabled on the backup cluster. This issue was observed in a cluster setup running AOS-W 8.1.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.2.0.2	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
176885	**Symptom:** The syslog server displayed the **problem retrieving http_session from db: PGRES_FATAL_ERROR** error that originated from a Mobility Controller Virtual Appliance. This issue is resolved by performing the following actions: ■ Clearing inactive WebUI sessions at the expiry of idle timeout. ■ Sending an enhanced error message to the syslog server. **Scenario:** This issue was observed in Mobility Controller Virtual Appliances running AOS-W 8.2.0.1.	Web Server	Mobility Controller Virtual Appliance	AOS-W 8.2.0.1	AOS-W 8.3.0.0
177009 177268 177336 178427	**Symptom:** The output of the **show memory lagm** command displayed a loss of memory in the LACP component of the **LAGM** process. The issue is resolved by fixing a memory leak in the **LAGM** process. **Scenario:** This issue occurred when LACP was enabled on any interface. This issue was observed in managed devices running AOS-W 8.2.0.2 or later versions.	Port-Channel	All platforms	AOS-W 8.2.0.0	AOS-W 8.3.0.0
177199	**Symptom:** The ZTP port was not defined for a managed device. This issue is fixed by adding the ZTP port definitions for the managed device. **Scenario:** This issue was observed in OAW-4x50 Series Switches running AOS-W 8.2.0.2 or later versions.	Configuration	OAW-4x50 Series Switches	AOS-W 8.2.0.2	AOS-W 8.3.0.0
177204	**Symptom:** The following streaming API and the CLI command on a managed device returned a value of 0 for Minimum RTT: ■ The **stats_ip_probe_uplink** streaming API ■ The **show ip health-check verbose** CLI command This issue is resolved by setting the Minimum RTT value to the lowest measured latency. **Scenario:** This issue occurred in managed devices with the **Uplink Health-check** configuration enabled. This issue was observed in OAW-40xx Series and OAW-4x50 Series managed devices running AOS-W 8.0.1.0.	Switch-Datapath	OAW-40xx Series and OAW-4x50 Series managed devices	AOS-W 8.0.1.0	AOS-W 8.3.0.0
177052	**Symptom:** An **mDNS** process memory leak occurred on a Mobility Master. The fix ensures that there is no memory leak. **Scenario:** This issue occurred when an AirGroup client changed the IP address. This issue was observed in Mobility Masters running AOS-W 8.2.0.0 or later versions.	AirGroup	All platforms	AOS-W 8.2.0.2	AOS-W 8.3.0.0

Table 5: *Resolved Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
177522	**Symptom:** The **Controller discovery** field in **Campus APs** and **Remote APs** pages of the WebUI displayed an irrelevant option. The issue is resolved by changing the **DHCP** option to **Use AP discovery protocol (ADP)** under **Configuration** > **Access Points** > **Campus APs** page of the WebUI. **Scenario:** This issue occurred when users tried to provision APs by using the **Controller discovery** field in **Campus APs** or **Remote APs** page of the WebUI. This issue was observed in managed devices running AOS-W 8.2.0.2 or later versions.	WebUI	All platforms	AOS-W 8.2.0.2	AOS-W 8.3.0.0
177575	**Symptom:** The output of the **show interface gigabitethernet <slot/module/port> counters** command displayed incorrect count of unicast and multicast packets. The fix ensures that the following show commands work appropriately: ■ The output of the **show interface gigabitethernet <slot/module/port> counters** command displays the correct count of unicast packets on 40 Gbps ports. ■ The **show interface gigabitethernet <slot/module/port> counters** command and any other command do not display the count of unicast packets on the 1 Gbps and 10 Gbps ports. **Scenario:** This issue was observed in OAW-4850 managed devices running AOS-W 8.3.0.0.	Switch-Platform	OAW-4850 managed devices	AOS-W 8.3.0.0	AOS-W 8.3.0.0
178438	**Symptom:** Temporary folder was full. This issue is resolved by disabling the debug logs to a file in /tmp location. **Scenario:** This issue occurred due to **ctrlmgmtdbg** log files getting too large. This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	Configuration	All platforms	AOS-W 8.2.1.0	AOS-W 8.3.0.0

This chapter describes the known issues and limitations identified in AOS-W 8.3.0.0.

Limitations

This section describes the limitations in AOS-W 8.3.0.0.

IOS Device Connectivity Issue

The iPad gets disconnected when the channel is changed from one frequency to another on a Mobility Master.

This issue is observed only in the latest IOS version, iOS 11.3.

No Support for Cell Size Reduction

Starting from AOS-W 8.3.0.0, the **cell-size-reduction** parameter in **rf dot11a-radio-profile** and **rf dot11g-radio-profile** commands does not take effect for 300 Series access points. If the **cell-size-reduction** parameter has any configured value, the 300 Series access points disregard the value.

Known Issues

The following known issues are observed in AOS-W 8.3.0.0.

Table 6: *Known Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
143800 156149 161721 162902 166512 170300 172955 172967 174101 177773	**Symptom:** The **OFA** process in a managed device crashes unexpectedly. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	SDN	All platforms	AOS-W 8.2.0.0
149222	**Symptom:** The WebUI of a Mobility Master does not display any devices. **Scenario:** This issue occurs when a user configures a managed device from the **/mm/mynode** node hierarchy by using the CLI. This issue is observed in the WebUI of a Mobility Master running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	IPsec	All platforms	AOS-W 8.0.0.0
151952	**Symptom:** When a managed device reboots, APs and clients boot without IP address and other fields. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.1.0. **Workaround:** None.	Monitoring	All platforms	AOS-W 8.0.1.0
154893	**Symptom:** The **Postgres** process in a managed device that is deployed in the cluster topology crashes unexpectedly. **Scenario:** This issue is observed in OAW-4x50 Series Switches running AOS-W 8.1.0.0 or later versions. **Workaround:** None.	Database	OAW-4x50 Series Switches	AOS-W 8.1.0.0
159973	**Symptom:** Certificates loaded on a managed device do not synchronize between Mobility Master and the standby Mobility Master. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.1.0.0 or later versions. **Workaround:** Load these certificates on the Mobility Master.	Certificate Manager	All platforms	AOS-W 8.1.0.0

Table 6: *Known Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
160281	**Symptom:** A managed device stops forwarding packets on 40 Gbps ports unexpectedly. **Scenario:** This issue occurs when both 40 Gbps and 10 Gbps ports are enabled for jumbo traffic in the OAW-4850 managed device. The network engine in the managed device stalls when jumbo packets (frame size larger than 1380) egress on 40 Gbps and 10 Gbps ports simultaneously. This issue is observed in OAW-4850 managed devices running AOS-W 8.2.0.0 or later versions. **Workaround:** Avoid simultaneous jumbo packets egress on 40 Gbps and 10 Gbps ports of the OAW-4850 managed devices.	Switch-Datapath	OAW-4850 managed devices	AOS-W 8.2.0.0
160432	**Symptom:** VIA clients are not displayed in the **Dashboard > Clients** page of the WebUI. **Scenario:** This issue is observed on VIA clients that are connected to stand-alone Switches running AOS-W 8.1.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W8.1.0.0
164530	**Symptom:** The APPRF feature does not block the traffic that originates from Android-based mobile phones. **Scenario:** This issue is observed in managed devices running AOS-W 8.1.0.1. **Workaround:** None.	DPI	All platforms	AOS-W 8.1.0.1
165908 170224 171074 171396 173372 174322 174370 174917 177151 177457 177662 178307	**Symptom:** The **kernel** process in a managed device crashes and the managed device reboots unexpectedly. The log file lists the reason for the event as **control processor kernel panic**. **Scenario:** This issue is observed in OAW-4x50 Series managed devices running AOS-W 8.2.0.0. **Workaround:** None.	Switch-Platform	OAW-4x50 Series managed devices	AOS-W 8.2.0.0
165943	**Symptom:** The **Dashboard** > **Info** page in the WebUI of a Mobility Master displays incorrect country information. **Scenario:** This issue occurs when **global-geolocation-acl** is configured on the Mobility Master. This issue is observed in Mobility Masters running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 8.0.0.0

Table 6: *Known Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
167110	**Symptom:** An AP fails to establish an IPsec tunnel when LMS is set to the VRRP IP address. **Scenario:** This issue occurs due to a race condition between **IKE** and **FPAPPS**. This issue is observed in a managed device running AOS-W 8.1.0.2 or later versions. **Workaround:** Restart the **ISAKMPD** process using the **process restart isakmpd core** command.	VRRP	All platforms	AOS-W 8.1.0.2
168725 168727	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.0.0. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 8.0.0.0
169216	**Symptom:** Data transfer from a Mobility Master Virtual Appliance setup to a Hyper-V switch stops unexpectedly. **Scenario:** When the throughput rate exceeds the threshold rate, the Hyper-V switch runs out of memory due to unlimited packets getting queued. This issue is observed in Switches running AOS-W 8.2.0.0 or later versions. **Workaround**: None	Switch- Datapath	All platforms	AOS-W 8.2.0.0
170058	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in OAW-4x50 Series Switches running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	Switch-Datapath	OAW-4x50 Series Switches	AOS-W 8.0.0.0
170249 175830	**Symptom:** Clients are unable to connect to some APs as the APs report 100% CPU utilization. **Scenario:** This issue is observed in OAW-AP100 Series access points running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP100 Series access points	AOS-W 8.0.0.0
171719	**Symptom:** A managed device fails to send the EAP-TLS request to its clients. **Scenario:** This issue occurs when the TLS exchange takes more than 10 seconds to complete. This issue is observed in managed devices running AOS-W 8.1.0.4 or later versions. **Workaround:** None.	802.1X	All platforms	AOS-W 8.1.0.4

Table 6: *Known Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
171839	**Symptom:** A managed device stops responding and reboots. The log file for the event lists the reason as **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:2).** **Scenario:** This issue occurs due to a session table corruption. This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 8.1.0.0
172464 175355	**Symptom:** A managed device has high CPU utilization and APs get disconnected. **Scenario:** This issue is observed in OAW-4x50 Series Switches running AOS-W 8.3.0.0. **Workaround:** None.	Web Server	OAW-4x50 Series Switches	AOS-W 8.3.0.0
172862	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 8.0.0.0
172942	**Symptom:** A managed device reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2**. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 8.0.0.0
173070	**Symptom:** The role and count of clients that are displayed in the **AppRF** dashboard are different from those that are displayed in the CLI command output. **Scenario:** This issue is observed in a Mobility Master running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	Firewall Visibility	All platforms	AOS-W 8.0.0.0
173283	**Symptom:** A managed device reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert).** **Scenario:** This issue is observed in managed devices running AOS-W 8.1.0.4 or later versions. **Workaround:** Upgrade to AOS-W 8.2.1.0.	Switch-Datapath	All platforms	AOS-W 8.1.0.4

Table 6: *Known Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
173395	**Symptom:** Some APs terminating on a managed device stop responding to pings randomly. **Scenario:** This issue occurs when some ICMP echo packets are dropped by the AP Ethernet driver. This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions. **Workaround:** Reboot the AP.	AP-Wireless	All platforms	AOS-W 8.0.0.0
173580	**Symptom**: The **Date and time** field in the **Configuration** > **General** > **Clock** page of the WebUI does not display values even though the NTP server is configured and synchronized with the system clock. **Scenario**: This issue is observed in managed devices running AOS-W 8.2.0.1 or later versions. **Workaround**: None.	WebUI	All platforms	AOS-W 8.2.0.1
173645	**Symptom:** False detections of type-5 radars are triggered in the FCC domain. **Scenario:** This issue is observed in OAW-AP200 Series, OAW-AP210 Series, and OAW-AP 220 Series access points running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 8.0.0.0
173746	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 8.0.0.0
173799	**Symptom:** An AP reboots continuously. The log file lists the reason for the event as **AP rebooted Wed Dec 27 11:23:51 EST 2017; Critical process /aruba/bin/meshd [pid 2413] DIED, process marked as RESTART**. **Scenario:** This issue occurs because **WPA Hexkey** values of the mesh recovery profile are incorrectly set. This issue is observed when APs operate in the mesh portal mode. This issue is not limited to any specific AP model or AOS-W release version. **Workaround:** Perform one of the following actions: ■ Set **WPA Hexkey** parameter values correctly in the **ap mesh-recovery-profile** command in support mode. ■ Reprovision the AP.	Mesh	All platforms	AOS-W 8.0.0.0

Table 6: *Known Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
173825 175778	**Symptom:** The client count does not get updated in OmniVista 3600 Air Manager. **Scenario:** This issue occurs because a managed device sends a value of 0.0.0.0 for **lms_ip**. This results in OmniVista 3600 Air Manager not updating the client count. This issue is not limited to any specific platform or AOS-W version. **Workaround:** None.	Activate/OmniVista 3600 Air Manager	All platforms	AOS-W 8.2.0.0
173885 173887	**Symptom:** An AP rebootstraps because managed devices fail to retain the VRRP master state. **Scenario:** This issue occurs when the LACP link flaps on the managed device. This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions. **Workaround:** Reboot the managed device.	Port-Channel	All platforms	AOS-W 8.0.0.0
174010	**Symptom:** The captive portal page is not displayed for the clients in split-tunnel forwarding mode. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.0.1 or later versions. **Workaround:** None.	Captive Portal	All platforms	AOS-W 8.2.0.1
174445	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 8.2.0.0
174725	**Symptom:** A managed device stops responding and reboots. The log file lists the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2).** **Scenario:** This issue occurs due to a memory corruption. This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions. **Workaround:** Disable AMSDU.	Switch-Datapath	All platforms	AOS-W 8.1.0.0
174856	**Symptom:** The output of the **show firewall dns-names** command displays the error, **Module Authentication is busy. Please try later**, along with an outdated IP address list. **Scenario:** This issue occurs when users execute the **netdestination wechat** command to define destination hosts. This issue is observed in a cluster setups running AOS-W 8.1.0.2 version. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.1.0.2

Table 6: *Known Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
174898	**Symptom:** Multiple APs crash and reboot unexpectedly. The log file lists the reason for the event as **kernel panic: NSS FW coredump: bringing system down**. **Scenario:** This issue is observed in OAW-AP310 Series and OAW-AP320 Series access points running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP310 Series and OAW-AP320 Series access points	AOS-W 8.3.0.0
174943	**Symptom:** The **tx rate** value is displayed incorrectly when the **show ap debug radiostats** command is executed. **Scenario:** This issue is observed in 300 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points running AOS-W 8.2.0.1 or later versions. **Workaround:** None.	AP-Wireless	300 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points	AOS-W 8.2.0.1
174989	**Symptom:** A stand-alone Switch crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue occurs due to a POE stall caused by overutilization of the forwarding plane. This issue is observed in stand-alone Switches running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 8.0.0.0
175391	**Symptom:** After exchanging VoIP packets, an AP delays the scanning of data packets by 1 second, instead of the intended 30 milliseconds. **Scenario:** This issue occurs when the VoIP-aware scanning feature is enabled and the voice call has been completed. This issue is observed in APs running AOS-W 8.3.0.0. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 8.3.0.0
175589	**Symptom:** Users are disconnected from APs due to insufficient resources on both 802.11a and 802.11g radios. **Scenario:** This issue is observed in OAW-AP365 access points running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP365 access points	AOS-W 8.2.0.0
175610	**Symptom:** The log file of a managed device frequently displays the following error message: **0:<4>__ratelimit: 596 callbacks suppressed**. **Scenario:** This issue is observed in a cluster setup running AOS-W 8.2.0.2 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 8.2.0.2

Table 6: *Known Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
175660	**Symptom:** VRRP MACs overlap multiple two-node clusters when configured in the same L2 domain with CoA. **Scenario:** This issue is observed in cluster setups running AOS-W 8.2.0.0 or later versions. **Workaround:** Use different VLAN IDs during VRRP configuration.	Cluster-Manager	All platforms	AOS-W 8.2.0.0
175714	**Symptom:** The **D** flag (indicates dirty mode) is displayed against an AP in the WebUI and clients lose connectivity. **Scenario:** This issue is observed during an upgrade, when an AP moves to a different managed device while the original managed device reboots. This issue is observed in access points running AOS-W 8.2.0.2. **Workaround:** None.	AP-Platform	All platforms	AOS-W 8.2.0.2
175928	**Symptom:** A managed device reboots unexpectedly. The log files lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in OAW-4650 Switches running AOS-W 8.2.0.1. **Workaround:** None.	Switch-Datapath	OAW-4650 Switches	AOS-W 8.2.0.1
176062	**Symptom:** A configured port is not displayed in the static port channel mode when a stand-alone Switch is rebooted. **Scenario:** This issue occurs when the user executes the **show running config** or **interface port-channel** command after rebooting the Switch. This issue is observed in OAW-4550 Switches running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	Port-Channel	OAW-4550 Switches	AOS-W 8.2.0.0
176207	**Symptom:** A managed device is unable to apply bandwidth contract to wired users. **Scenario:** This issue occurs when multiple IP addresses are used for each MAC address. This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.0.0.0
176330 177428	**Symptom:** The **Diagnostics > Technical Support > Copy Files** page in the WebUI displays success message although the TFTP file transfer fails. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.2.0.0

Table 6: *Known Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
178016	**Symptom:** Some APs detect false radar signals and change radio channels frequently. **Scenario:** This issue occurs when the false radar typeid is 36. This issue is observed in OAW-AP105 access points running AOS-W 8.3.0.0. **Workaround:** None.	AP-Wireless	OAW-AP105 access points	AOS-W 8.3.0.0
178297	**Symptom:** Users get the **Name of the country needs to be matching one of the countries listed under 'show ip-geolocation countries'** error when they enter country name with spaces in the name in the CLI. **Scenario:** This issue occurs when users try to configure a country by using the **ip access-list geolocation global-geolocation-acl** command and the country name includes spaces in it. This issue is observed in OAW-4008 stand-alone controllers running AOS-W 8.3.0.0. **Workaround:** For a country name that includes a space, enclose the country name within double quotes while configuring through the CLI.	Switch-Platform	OAW-4008 Switches	AOS-W 8.3.0.0
178839	**Symptom:** When an AP with static channel or EIRP is rebooted, the opmode changes on other Dual-5 GHZ APs as well. This results in 2.4 GHz APs getting EIRP computed for 5 GHz AP and vice-verse. **Scenario:** This issue occurs when the following conditions are met: ■ The Dual-5G APs are configured with static channels or EIRP. ■ The AP is rebooted. ■ The value of **dual-5ghz-mode** is set to **automatic** in the **ap system-profile**. This issue is observed in APs running AOS-W 8.3.0.0. **Workaround:** ■ Do not have static channel or EIRP for Dual-5G AP. ■ If static channel or EIRP configuration is needed, then once the AP is rebooted, remove the static configuration and redo the configuration.	AirMatch	All platforms	AOS-W 8.3.0.0

Table 6: *Known Issues in AOS-W 8.3.0.0*

Bug ID	Description	Component	Platform	Reported Version
179000	**Symptom:** A reduction of power is observed in AP-345 access points. **Scenario:** This issue occurs as the antenna polarization is incorrectly programmed to calculate maximum TX power. This issue is observed in AP-345 access points running AOS-W 8.3.0.0. **Workaround:** None.	AP-Wireless	AP-345 access points	AOS-W 8.3.0.0
179047	**Symptom:** An AP crashes due to configuration changes. The log files lists the reason for the event as **PC is at wlc_apps_bss_ps_off_done+0x54/0x118 [wl] and LR is at wlc_mbss_shm_ssid_upd+0x2f8/0x330 [wl]**. **Scenario:** This issue is observed in AP-345 access points running AOS-W 8.3.0.0. **Workaround:** None.	AP-Wireless	AP-345 access points	AOS-W 8.3.0.0
179064	**Symptom:** The status of the Virtual AP is temporarily DOWN, resulting in clients getting disconnected. **Scenario:** This issue occurs when the radio band of the AP changes. This issue is observed in managed devices running AOS-W 8.3.0.0. **Workaround:** None.	Station Management	All platforms	AOS-W 8.3.0.0

This chapter details software upgrade procedures. Alcatel-Lucent best practices recommend that you schedule a maintenance window for the upgrade.

Read all the information in this chapter before upgrading your Mobility Master, managed device, master Switch, and/or stand-alone Switch.

Topics in this chapter include:

- Migrating from AOS-W 6.x to AOS-W 8.x on page 53
- Important Points to Remember and Best Practices on page 54
- Memory Requirements on page 54
- Backing up Critical Data on page 55
- Upgrading on page 57
- Downgrading on page 60
- Before You Call Technical Support on page 62

Migrating from AOS-W 6.x to AOS-W 8.x

If you are migrating from AOS-W 6.x to AOS-W 8.x, take a note of the following points:

- Use the interactive migration tool provided on the customer support site to migrate any AOS-W 6.x deployments to one of the following AOS-W 8.x deployments:
  - Master-Local setup to Mobility Master
  - All-Master setup to Mobility Master
  - Master-Local setup to Master Switch Mode in AOS-W 8.x
  - Stand-alone Switch running AOS-W 8.x

For more information, refer to the *AOS-W 8.x Migration Guide*.

Licenses are not migrated by the migration tool from any of the devices to Mobility Master. However, the licenses are preserved when migrating to AOS-W 8.x Master Switch Mode or stand-alone Switches. For more information on License migration, refer to *Alcatel-Lucent Mobility Master Licensing Guide*.

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 managed device? Verify this information by navigating to the **Dashboard > 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 managed device (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W is currently on the managed device?
  - Are all managed devices running the same version of software?
  - Which services are used on the managed device (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 managed device. 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 AOS-W, assess your software license requirements and load any new or expanded licenses you may require. For a detailed description of these new license modules, see the "Software Licenses" chapter in the *AOS-W 8.x.0.0 User Guide*.

Memory Requirements

All Alcatel-Lucent managed devices store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the managed device. 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 100 MB of free memory available for an upgrade using the WebUI or CLI. Execute the **show memory** command to identify the amount of free memory available using the CLI. Do not proceed unless this much free memory is available. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Confirm that there is at least 150 MB of flash space available for an upgrade using the WebUI or CLI. Execute the **show storage** command to identify the amount of flash space available using the CLI.

In certain situations, a reboot or a shutdown could cause the managed device 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 managed device logs, crash data, or flash backups should be copied to a location off the managed device, then deleted from the managed device to free up flash space. You can delete the following files from the managed device 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 55 to copy the **crash.tar** file to an external server, and then execute the **tar clean crash** command to delete the file from the managed device.
- **Flash Backups:** Use the procedures described in Backing up Critical Data on page 55 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 managed device.
- **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 55 to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the managed device.

The following procedure deletes a file.

In the WebUI

From the Mobility Master, navigate to **Diagnostic > Technical Support > Delete Files** and remove any aging log files or redundant backups which may have been created by administrator.

In the CLI

```
(host) #delete filename <filename>
```

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
- Custom captive portal pages
- x.509 certificates
- Logs

- Flashbackup

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 managed device:

1. In the Mobility Master node hierarchy, navigate to the **Maintenance > Configuration Management > Backup** page.
2. Click **Create Backup** to backup the contents of the compact flash file system to the **flashbackup.tar.gz file**.
3. Click **Copy Backup** to copy the file to an external server.

   You can later copy the backup file from the external server to the compact flash file system using the file utility in the **Diagnostics > Technical Support > Copy Files** page.
4. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > Configuration Management > Restore** 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 command line:

1. Make sure you are in the **enable** mode in the 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 take the flash backup.......
   File flashbackup.tar.gz created successfully on flash.
   Please copy it out of the controller and delete it when done.
   ```
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
   Please wait while we restore the flash backup........
   Flash restored successfully.
   Please reload (reboot) the controller for the new files to take effect.
   ```

Upgrading

The following sections provide the procedures for upgrading your WLAN network to the latest AOS-W version using the WebUI or CLI.

AOS-W 8.3.0.0 Upgrade Notes

Before you upgrade Mobility Master from AOS-W 8.0.0.0 to AOS-W 8.3.0.0, take a note of the following points:

- AOS-W 8.3.0.0 supports only a maximum of 3 network adapters for Mobility Master and 4 network adapters for Mobility Master Virtual Appliance. If you have 4 network adapters on your AOS-W 8.0.0.0 Mobility Master Virtual Appliance, you must remove one before upgrading to AOS-W 8.3.0.0 to avoid upgrade failure. To remove a network adapter from AOS-W 8.0.0.0 Mobility Master Virtual Appliance:

Before you remove the additional network adapter from the Mobility Master Virtual Appliance, ensure that you copy the AOS-W 8.0.0.0 image on the system partition of Mobility Master Virtual Appliance.

  1. Log in to the vSphere client.
  2. Select the Mobility Master VM instance and click **Shut down the virtual machine**.
  3. Click **Edit Virtual machine settings**.
  4. From the **Hardware** tab, select and remove a network adapter that is not active.
- Before upgrading to AOS-W 8.3.0.0 from AOS-W 8.0.0.0, ensure that you configure the MAC address of the management interface as the peer MAC address, if the peer is a Mobility Master Virtual Appliance or Mobility Master. Before reloading the new image on Mobility Master, alter the peer MAC address using the following procedure in the WebUI:
  1. From the **Managed Network** node hierarchy, select the managed device.
  2. Navigate to **Configuration > Controllers** and enter the management interface MAC address in the **Peer MAC address of master** field.
  3. Click **Submit** and click **Continue** in the reload popup.
  4. Click **Pending Changes**.
  5. In the **Pending Changes** window, select the check box and click **Deploy changes**.

  Alternatively, you can execute the following CLI command on Mobility Master at the device level:

  ```
  (host) [<device-mac-address>] (config) #masterip <ipaddr> ipsec <key> peer-mac-1 <mgmt-interface-mac> peer-mac-2 <mgmt-interface-mac> interface vlan <id>
  ```
- Before upgrading to AOS-W 8.3.0.0, you must share the licenses within the global licensing pool by executing the **license-pool-profile-root** command:

  ```
  (host) [mm](config) #license-pool-profile-root
  (host) [mm](License root(/) pool profile) #acr-license-enable
  ```

In 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 54.

NOTE

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

You can install the software image from a TFTP or FTP server using the same WebUI page.

1. Download AOS-W 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 **Alcatel.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.

NOTE

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

4. Log in to the AOS-W WebUI from the Mobility Master.
5. Navigate to the **Maintenance > Software Management > Upgrade** page.
   a. Select the **Local File** option from the **Upgrade using** drop-down list.
   b. Click **Browse** from the **Image file name** field to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Choose the partition from the **Partition to Upgrade** option.
8. Enable the **Reboot Controller After Upgrade** toggle switch to automatically reboot after upgrading. Disable the same, if you do not want to reboot immediately.

NOTE

Note that the upgrade will not take effect until you reboot.

9. Select the **Save Current Configuration** option.
10. Click **Upgrade**.

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

11. Click **OK**.

    If you chose to automatically reboot 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 **Dashboard > WLANs** page to verify the upgrade.

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

1. Log in to the WebUI to verify all your Switches are up after the reboot.
2. Navigate to the **Dashboard > Access Points** 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 55 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.

In 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 54.

Upgrading From a Recent Version of AOS-W

To install the AOS-W software image from a PC or workstation using the CLI:

1. Download AOS-W from the customer support site.
2. Open an SSH session on your master (and local) Switches.
3. Execute the **ping** command to verify the network connection from the target Switch 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 AOS-W images are loaded on the Switch'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**.

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

5. Execute the **copy** command to load the new image onto the non-boot 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>
```

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

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

7. Reboot the Switch.

   ```
   (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 Switch is functioning as expected.

1. Log in to the CLI to verify that all your Switches 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 55 for information on creating a backup.

Downgrading

If necessary, you can return to your previous version of AOS-W.

Before You Begin

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

1. Back up your Switch. For details, see Backing up Critical Data on page 55.
2. Verify that the control plane security is disabled.
3. Set the Switch to boot with the previously saved pre-AOS-W configuration file.
4. Set the Switch to boot from the system partition that contains the previously running AOS-W 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 Switch 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 Switch, perform the following steps:
   - Restore pre-AOS-W flash backup from the file stored on the Switch. Do not restore the AOS-W 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 AOS-W, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W, you need to reinstall the certificates in the downgraded AOS-W version.

Downgrading Using the WebUI

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

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the Switch by navigating to the **Diagnostics > Technical Support > Copy Files** page.
   a. For **Select source file** option, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.
   b. For **Select destination file** option, enter a file name (other than default.cfg) for Flash File System.
2. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Software Management > Upgrade** 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**.
3. Navigate to the **Maintenance > Software Management > Boot Parameters** page.
   a. Select the system partition that contains the pre-upgrade image file as the boot partition.
   b. Click **Apply**.
4. Navigate to the **Maintenance > Software Management > Reboot** page. Select **Save configuration before reboot** option and click **Reboot**. The Switch reboots after the countdown period.
5. When the boot process is complete, verify that the Switch is using the correct software by navigating to the **Maintenance > Software Management > About** page.

Downgrading Using the CLI

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

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

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

   or

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

2. Set the Switch to boot with your pre-upgrade 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).
   ```
   #show image version
   ```
4. Set the backup system partition as the new boot partition.
   ```
   (host) # boot system partition 1
   ```
5. Reboot the Switch.
   ```
   (host) # reload
   ```
6. When the boot process is complete, verify that the Switch 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 Alcatel-Lucent device 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 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 at the time of the problem. Alcatel-Lucent strongly recommends that you consider adding a syslog server if you do not already have one to capture the logs.
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 Alcatel-Lucent device) or any recent changes to your Alcatel-Lucent device 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 Alcatel-Lucent device 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.