AOS-W 6.5.2.0

Alcatel·Lucent
Enterprise

Release Notes

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.
Revision 02	Added a section, **Support for Cisco-AvPair VSA** under New Features on page 8.

AOS-W 6.5.2.0 is a software release that includes new features and enhancements introduced in this release, and fixes to issues identified in previous releases.

NOTE

See the Upgrade Procedure on page 46 for instructions on how to upgrade your switch to this release.

Chapter Overview

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

NOTE

For information regarding prior releases, refer to the corresponding Release Notes on https://support.esd.alcatel-lucent.com/.

Supported Browsers

The following browsers are officially supported for use with AOS-W 6.5.2.0 WebUI:

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

Contacting Support

Table 2: *Contact Information*

Contact Center Online	
Main Site	http://enterprise.alcatel-lucent.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 new features, enhancements, and hardware introduced in AOS-W 6.5.2.0. For more information about these features, refer to the *AOS-W 6.5.2.x User Guide*.

OV3600 Management

Inline Monitoring

Starting with AOS-W 6.5.2.0, inline monitoring feature is supported for Remote APs.

AMON

AirMatch Monitoring Information in AMON Messages

When AirMatch monitoring is enabled via the AP system profile, each AP measures its RF environment for a configurable duration (every 30 minutes by default). The switch uses this information to analyze its RF neighborhood, and can send this information in AMON messages to OV3600 or a mobility manager server.

The AirMatch feature in AOS-W 6.5.2.0 is used only to send monitoring messages to OV3600. AOS-W 6.5.x uses the ARM feature to dynamically and intelligently choose the best 802.11 channel and transmit power for each Alcatel-Lucent AP in its current RF environment.

AP Configuration

AP Health Checks

The AP Health check feature uses ping probes to check reachability and latency levels for the connection between the AP and the switch. The recorded latency information appears in the output of the **show ap ip health-check** command. If the switch IP address becomes unreachable from the AP uplink, this feature records the time that the connection failed, and saves that information in a log file on the AP.

AP-Platform

BLE

Starting with AOS-W 6.5.2.0, the BLE firmware image is part of AOS-W. The BLE firmware will be upgraded automatically when AOS-W is upgraded.

Mesh Support

Starting with AOS-W 6.5.2.0, mesh support is introduced for OAW-AP303H, OAW-AP300 Series, OAW-AP330 Series, and OAW-AP360 Series access points.

Support for OAW-AP203H Access Point

The OAW-AP203H access point is an IEEE 802.11ac standard high-performance flex-radio wireless device ideal for hospitality and branch deployments. The AP is software configurable as either a single radio dual band or dual radio. MIMO technology allows the AP to deliver high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a, b, and g wireless services. The AP works in conjunction with a switch.

The AP provides the following capabilities:

- IEEE 802.11a, b, g, n, or ac operation as a wireless access point
- IEEE 802.11a, b, g, n, or ac operation as a wireless air monitor
- Compatible with IEEE 802.3af PoE
- Centralized management configuration

For technical specifications, see the OAW-AP203H data sheet. For installation instructions, see the *OAW-AP203H Access Point Installation Guide*.

OAW-AP203H Access Point Limitations

The unique private keys for OAW-AP203H access points are stored in flash because these access points do not have TPM chip unlike most other APs. Therefore, OAW-AP203H access points cannot use certificates in AOS-W 6.5.2.0 release.

To convert an OAW-AP203H Campus AP to a Remote AP, use PSK or locally generated certificates.

The future releases of AOS-W will provide support for using certificates with OAW-AP203H.

In addition to the certificate issue, the OAW-AP203H access points have the following limitations:

- No support for Spectrum Monitoring.
- No support for on-board BLE. However, you can avail the BLE support by using an external USB.

Support for OAW-AP203R Series Remote Access Points

The OAW-AP203R Series (OAW-AP203R and OAW-AP203RP) Remote APs are IEEE 802.11ac standard high-performance Remote APs ideal for home and branch deployments. MIMO technology allows these Remote APs to deliver high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a, b, and g wireless services. The Remote APs work in conjunction with a switch.

The Remote APs provides the following capabilities:

- IEEE 802.11a, b, g, n, or ac operation as a wireless access point

- IEEE 802.11a, b, g, n, or ac operation as a wireless air monitor
- Compatible with IEEE 802.3at PoE
- Centralized management configuration
- Support for PoE-in (E0 port)/PoE-out (E2 port)
- Support for selected USB peripherals
- Integrated BLE radio

For technical specifications, see the OAW-AP203R Series data sheet. For installation instructions, see the *OAW-AP203R Series Remote Access Points Installation Guide*.

Support for OAW-AP303H Access Point

The OAW-AP303H access point is an IEEE 802.11ac standard high-performance wireless device ideal for hospitality and branch deployments. MIMO technology allows the AP to deliver high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a, b, and g wireless services. The AP works in conjunction with a switch.

The AP provides the following capabilities:

- IEEE 802.11a, b, g, n, or ac operation as a wireless access point
- IEEE 802.11a, b, g, n, or ac operation as a wireless air monitor
- Compatible with IEEE 802.3af PoE and 802.3at PoE+
- Centralized management configuration
- Support for PoE-in (E0 port)/PoE-out (E3 port)
- Support for selected USB peripherals
- Integrated BLE radio

For technical specifications, see the OAW-AP303H data sheet. For installation instructions, see the *OAW-AP303H Access Point Installation Guide*.

Support for OAW-AP360 Series Outdoor Access Points

The OAW-AP360 Series (OAW-AP365 and OAW-AP367) outdoor APs support IEEE 802.11ac standard for high performance WLAN, and are equipped with two radios, which provide network access and monitor the network simultaneously. MIMO technology allows these APs to deliver high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a, b, and g wireless services. The outdoor APs work in conjunction with a switch.

The outdoor APs provide the following capabilities:

- IEEE 802.11a, b, g, n, or ac operation as a wireless access point
- IEEE 802.11a, b, g, n, or ac operation as a wireless air monitor
- IEEE 802.11a, b, g, n, or ac spectrum monitor
- Compatible with IEEE 802.3af PoE

- Centralized management configuration
- Integrated BLE Radio

For technical specifications, see the OAW-AP360 Series data sheet. For installation instructions, see the *OAW-AP360 Series Outdoor Access Points Installation Guide*.

Support for BLE-based Asset Tracking

Starting with AOS-W 6.5.2.0, APs can monitor BLE asset tags to track the location of time-sensitive, high-value assets embedded with BLE tags.

Support for Franklin Wireless U772 LTE Modem

AOS-W 6.5.2.0 introduces support for the Franklin Wireless U772 LTE modem on the following AP platforms:

- OAW-AP200 Series access points
- OAW-AP203R Series access point
- OAW-AP205H access points
- OAW-AP210 Series access points
- OAW-AP220 Series access points
- OAW-AP300 Series access points
- OAW-AP303H access points
- OAW-AP310 Series access points
- OAW-AP320 Series access points
- OAW-AP330 Series access points

AP Discovery Logic

Starting with AOS-W 6.5.2.0, select APs can run in both switch-based mode and switch-less mode. Based on the selected mode, the AP runs a different image:

- Switch-based APs run an AOS-W image.
- Switch-less APs run an Instant image.

The following APs support both switch-based mode and switch-less mode:

- 203H Series access points
- 203R/203RP Series access points
- 303H Series access points
- OAW-AP365 and OAW-AP367 access points

In the AOS-W 6.5.1.x and earlier release trains, APs are predefined as either switch-based campus APs or switch-less Instant APs. Each campus AP is shipped with the AOS-W manufacturing image and must connect to a switch in order to receive configurations. Campus APs can only run the AOS-W image and cannot be converted into Instant APs. Each Instant AP is shipped with the Instant manufacturing image and must join an IAP cluster in order to receive configurations from a virtual switch. Instant APs run the Instant image and can also be converted into campus APs.

In AOS-W 6.5.2.0, each AP is shipped with a manufacturing image based on the Instant image, but containing reduced functions. When the AP is booted up with the manufacturing image, it enters the switch/Instant discovery process to determine if it will be upgraded to the switch-based mode (AOS-W image) or switch-less mode (Instant image). After the switch, Instant virtual switch (VC), or Activate/OV3600/Central is discovered, the AP image is upgraded accordingly.

By default, switch discovery has a higher priority than Instant discovery. APs can discover the IP address of a switch through one of the following methods:

- ADP
- DHCP server
- DNS server

APs can support up to 12 switch IP addresses via DHCP/DNS discovery. APs attempt to connect to each switch 10 times before switching to the next switch.

An AP can only be converted into a switch-based AP if the switch to which it connects is running AOS-W 6.5.2.0.

If the AP cannot locate any switches during the switch discovery process, the AP enters Instant discovery.

Enabling Flexible Radio

This feature allows the AP to seamlessly switch between modes where the radio resources are either combined in a single 2x2 radio (2.4 GHz or 5 GHz), or separated in two 1x1 radios (2.4 GHz and 5 GHz).

Intelligent Power Monitoring

Starting with AOS-W 6.5.2.0, IPM is supported in OAW-AP303H access points. IPM is a feature that actively measures the power utilization of an AP and dynamically adapts to the power resources.

Smart Antenna Polarization

The OAW-AP335 access point supports the smart antenna feature, which optimizes the selection of antenna polarization values based on data collected from the training of polarization pattern combinations. This feature identifies the clients most likely to benefit from smart antenna polarization, based upon the average RSSI of the received frames, and the number of streams. This feature uses frame-based antenna training, which allows the AP to cycle through training combinations for training and collect statistics without any impact on the client. At the end of training sequence, the AP selects the best antenna polarization based upon these collected statistics.

The Smart Antenna feature does not support optimized antenna polarization for clients using Single-User or Multi-User transmit beamforming.

Transmit Power Calculation Support

Starting with AOS-W 6.5.2.0, AP transmit power calculation has been modified to comprehend the increasing sophistication of signal processing techniques that address radio range and reliability. Due to this greater accuracy in computing the transmit power on a per packet basis through the contributing DSP techniques and due to regulatory limitations, ensure to slightly increase the transmit power settings to obtain the same conducted power as before.

Authentication

Configuring Source Interface VLAN in the TACACS Server

Starting with AOS-W 6.5.2.0, a user has the option of specifying the source IP for a TACACS server.

Roaming RADIUS Accounting Service

Starting with AOS-W 6.5.2.0, the Roaming RADIUS Accounting Service creates an Accounting session for each wireless client. The records in the session contain the same set of RADIUS attributes as compared to the timer-based RADIUS Interim-Update Accounting record, except the statistics attributes. Whenever a wireless client roams to a different AP, the Roaming triggered RADIUS Interim-Update Accounting record is sent to the configured RADIUS Accounting server. This record is used to track the current location of the wireless client. Currently this feature is supported for wireless clients in non-cluster environments, but is not supported for wired, VPN/VIA, and L3 mobility clients.

Base OS Security

Support for Querying RADIUS and Internal Server Users

Starting with AOS-W 6.5.2.0, the **aaa query-user** command accepts RADIUS and internal authentication server names in addition to the LDAP server name for user search.

Dynamically Customizing the RADIUS Attributes

Starting with AOS-W 6.5.2.0, supports dynamic data for the included attributes in the RADIUS Attribute modifier. Users can configure the dynamic value for each included attribute in the RADIUS modifier to be one or two data items.

Captive Portal

Support for Cisco-AvPair VSA

Starting with AOS-W 6.5.2.0, the switch provides support for **Cisco AV-Pair** VSA in the **url-redirect** parameter configured in captive portal.

Centralized Licensing

License Server Supports Standalone and Local License Clients

Starting with AOS-W 6.5.2.0, the centralized licensing feature supports topologies where a licensing master is connected to a standalone master licensing client switch, a master switch acting as a redundant licensing server, and a local licensing client switch. In previous releases of AOS-W, licensing servers in centralized licensing topologies supported standalone master switches or local switches, but not both.

DHCP

Character Limitation for DHCP Option 242

Starting with AOS-W 6.5.2.0, the number of characters for the text field under the DHCP pool option is increased from 128 to 256.

IPsec

Support IKEv1 SHA-2 for PSK RAP

Starting with AOS-W 6.5.2.0, PSK RAPs support IKEv1 SHA-2 cryptographic hash function.

Forced Tunnel Mode

Starting from AOS-W 6.5.2.0, the site-to-site IPsec SA can be switched to forced-tunnel mode, even if the protected network/mask and the peer-IP are the same. Enable or disable the forced-tunnel mode or the transport mode on both peers, otherwise a tunnel will not be established.

WebUI

Authentication Survivability Timeout

Starting with AOS-W 6.5.2.0, the upper limit of the authentication survivability timeout is extended from 72 hrs to 168 hrs. To configure authentication survivability timeout, in the WebUI, navigate to **Configuration > Branch > Smart Config > WAN** and configure a value for the **Local Cache Lifetime (hrs)** parameter.

Chapter 3
Regulatory Updates

This chapter describes the regulatory updates in AOS-W 6.5.2.0.

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.

The following default Downloadable Regulatory Table (DRT) version is part of AOS-W 6.5.2.0:

- DRT-1.0_59118

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

This software release supports the channel requirements described in *ALE Support Advisory SA-N0033*, available for download from the support.esd.alcatel-lucent.com site.

This chapter describes the issues resolved in AOS-W 6.5.2.0.

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
104874 139962 149550 150743 151483 155084	**Symptom:** Stale entries were present in both the switch and the AP association tables but not in the AP driver's client table, or vice versa. The fix ensures that the stale entries are cleared periodically from the association tables. **Scenario:** This issue occurred if APs were up for several weeks. This issue was not limited to any specific switch or AP model and AOS-W release version.	Station Management	All platforms	AOS-W 6.4.3.0	AOS-W 6.5.2.0
126244 133950 136632 136957 141924	**Symptom:** The status of an AP did not match between a master and a local switch. The fix ensures that the status of an AP is consistent between a master and a local switch. **Scenario:** This issue occurred when an AP moved from one local switch to another but its status was not updated in the master switch. This issue was observed in APs running AOS-W 6.4.4.8.	AP-Platform	All platforms	AOS-W 6.4.4.8	AOS-W 6.5.2.0
126727 139011	**Symptom:** There was EIRP value mismatch between the mesh portal and the mesh point. This issue is resolved by setting an init value of (127-1) dBm for the mesh point. **Scenario:** This issue occurred in a mesh environment and was observed in OAW-AP270 Series access points. This issue was not limited to any specific AOS-W release version.	Mesh	OAW-AP270 Series access points	AOS-W6.4.4.5	AOS-W 6.5.2.0
127094 138590 139656 144730 151357	**Symptom:** The **Dashboard > Access Points > Radios** page of the WebUI displayed some of the AP names as **unknown**. The fix ensures that the WebUI Dashboard displays the AP names correctly. **Scenario:** This issue occurred during a HA failover when the AP switched from the master switch to a standby switch. This issue was not limited to any specific AP model or AOS-W version.	AP-Platform	All AP platforms	AOS-W 6.4.2.12	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
132770	**Symptom:** In a centralised licensing system, the following license expiry message was displayed without sufficient information: **Jan 7 08:30:00 :300158: <WARN> |licensemgr| Licenses contributed by the client will expire in 29 days** The fix ensures that the license expiry message includes sufficient information such as the MAC address of the switch when it goes down if it contributes licenses. **Scenario:** This issue occurred in a centralised licensing system when a client switch that contributed license went down. This issue was not limited to any specific switch model or AOS-W version.	AP-Platform	All AP platforms	AOS-W 6.4.2.12	AOS-W 6.5.2.0
141310	**Symptom:** The **All WLAN Clients** tab on the acting master switch did not display any records for the clients that were connected. This issue is resolved by always relaying the LMS list whenever switch role changes. **Scenario:** This issue occurred because of the following reasons: ■ The LMS list was not relayed to apps if the role changed between master and standby switches. ■ There was no heartbeat activity on the master. This issue was observed in a Master-Standby topology and was not specific to any switch or AOS-W version.	Master-Redundancy	All platforms	AOS-W 6.4.4.4	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
141594 142974 144029 145174 145583 147933 148379 148380 148381 148382 148383 148384 149916 151187 151466 153615 156639	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **Internal watchdog reset**. Improvements in the wireless driver resolves this issue. **Scenario:** This issue was observed in OAW-AP315 or OAW-AP325 access points running AOS-W 6.4.4.8.	AP-Wireless	OAW-AP315 and OAW-AP325 access points	AOS-W 6.4.4.8	AOS-W 6.5.2.0
141661 153779 158448 158899 158907 159343	**Symptom:** A OAW-RAP109 access point crashed because of data bus error. This issue is resolved by stopping radio reset when pending packets exist. **Scenario:** This issue occurred because of radio reset when pending packets existed. This issue was observed in OAW-4750 switches running AOS-W 6.4.3.7 in Master-Standby topology.	AP-Wireless	OAW-RAP109 access points	AOS-W 6.4.3.7	AOS-W 6.5.2.0
143016	**Symptom:** The IPv6 link local address was deleted from the switch IP VLAN. The fix ensures that the IPv6 link local address is not deleted from the switch IPv6 VLAN, when the switch is rebooted. **Scenario:** This issue occurred when the switch was rebooted with user configured link local address for IPv6 VLAN. This issue was observed in switches running AOS-W 6.4.4.6.	IPv6	All platforms	AOS-W 6.4.4.6	AOS-W 6.5.2.0
143062	**Symptom:** Port 1144 was open in an AP although the RTLS feature was disabled. This issue is resolved by opening port 1144 only when the RTLS feature is enabled. **Scenario:** This issue occurred during the AP boot sequence irrespective of the status of the RTLS feature. This issue was observed in access points running AOS-W 6.4.4.6.	Air Management-IDS	All AP platforms	AOS-W 6.4.4.6	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
143566	**Symptom:** The error **Module authentication is busy. Please try later.** was displayed when the command, **show reference user-role <role-name>** was executed. The fix ensures that the output is displayed without any error. **Scenario:** This issue occurred when there were more than 212 entries for a given role in user derivation-rules or server-group derivation rules. This issue was observed in a master local topology with switches running AOS-W 6.4.2.16.	Configuration	All platforms	AOS-W 6.4.2.16	AOS-W 6.5.2.0
144156 145374 145759 150408 156415	**Symptom:** A switch processed wrong instructions. The fix ensures that the switch processes the correct instructions. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.5.	Switch-Platform	All platforms	AOS-W 6.4.4.5	AOS-W 6.5.2.0
145234 151998	**Symptom:** The WebUI displayed an incorrect switch IP address for an AP. The fix ensures that the WebUI displays the correct switch IP address for an AP. **Scenario:** This issue occurred when a master switch was part of HA active-standby configuration and an AP associated with the master switch switched from active to standby state. This issue was observed in a master-local topology with switches running AOS-W 6.4.4.3.	WebUI	All platforms	AOS-W 6.4.4.3	AOS-W 6.5.2.0
144774	**Symptom:** An AP stopped responding and rebooted. The log file of the event suggested a radio set on the AP. Improvements in the wireless driver of the AP resolved the issue. **Scenario:** This issue was observed in OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, and OAW-AP270 Series access points running AOS-W 6.4.4.8 or later versions.	AP-Platform	OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, and OAW-AP270 Series access points	AOS-W 6.4.4.8	AOS-W 6.5.2.0
145385	**Symptom:** An AP rebooted frequently. The log file listed the reason for the event as **SAPD: Reboot requested by controller**. The fix ensures that the switch does not trigger an incorrect AP reboot. **Scenario:** This issue was observed in switches running AOS-W 6.3.1.14.	Local Database	All platforms	AOS-W 6.3.1.14	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
145934 149784 150173 155544 156308	**Symptom:** Multiple processes in a switch crashed unexpectedly. The log file listed the reason for the event as **KERNEL: Out of Memory signal 9: Killed process 30929 (httpd). Out of memory**. Improvements in the switch memory management resolves this issue. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.x and AOS-W 6.4.3.x.	Switch-Platform	All platforms	AOS-W 6.3.1.22	AOS-W 6.5.2.0
147300	**Symptom:** A switch failed to respond and rebooted. Improvements in the process that handles AP management and user association resolves this issue. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.6.	Station Management	All platforms	AOS-W 6.4.3.6	AOS-W 6.5.2.0
148004 155405 157742	**Symptom:** An AP experienced the following issues: ■ The 2.4 GHz BSSID disappeared for a fraction of a second. ■ High CPU and memory utilization. ■ High ping latency on the physical interface of the AP. The fix ensures that the AP performs as expected. **Scenario:** This issue occurred when the clock of the AP was slower than the clock of the switch. This issue was observed in OAW-AP103H , OAW-AP100 Series, and OAW-RAP100 Series access points running AOS-W 6.4.3.6 or later versions.	AP-Platform	OAW-AP103H, OAW-AP100 Series, and OAW-RAP100 Series access points	AOS-W 6.4.3.6	AOS-W 6.5.2.0
148416 149211	**Symptom:** A crash was observed in the **Station Management (STM)** process due to memory corruption. This issue is resolved by fragmenting the role bandwidth message when it does not fit in one single PAPI message. **Scenario:** This issue occurred when there was an increase in the number of user roles and as a result the role bandwidth message did not fit into one PAPI message. This issue was observed in OAW-4550 switches running AOS-W 6.4.3.4.	AP-Platform	OAW-4550 switches	AOS-W 6.4.3.4	AOS-W 6.5.2.0
148557	**Symptom:** Clients observed a sudden increase in the number of DHCPv6/Multicast messages from the access points. This issue is resolved by making changes to the **SAPD** process. **Scenario:** This issue occurred when DHCP daemon for IPv6 sent DHCPv6 solicit messages when an AP received IPv4 addresses continuously. This issue was observed in switches running AOS-W 6.4.4.9.	AP-Platform	All platforms	AOS-W 6.4.4.9	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
148977 155343	**Symptom:** A branch office switch randomly lost configuration updates from the master switch. This issue is resolved by triggering a reboot of the branch office switch whenever a new license is added or removed. **NOTE:** Adding an additional license count to an existing license type does not trigger a reboot of the branch office switch. **Scenario:** This issue occurred after a new license was sent from the master switch to the branch office switch. Thereafter, license dependent configuration updates were not sent to the branch office switch. This issue was observed in a master-branch office switch deployment with switches running AOS-W 6.5.0.0 or later versions.	Licensing	All platforms	AOS-W 6.5.0.0	AOS-W 6.5.2.0
149131	**Symptom:** A switch sent Alcatel Mapping Adjacency Protocol (AMAP) packets only on one member interface instead of all member interfaces of the port-channel. This issue is resolved by sending the AMAP packets on all member interfaces of the port-channel. **Scenario:** This issue occurred when AMAP was enabled on the port-channel interface. This issue was not limited to any specific switch model or AOS-W version.	SNMP	All platforms	AOS-W 6.4.3.10	AOS-W 6.5.2.0
149372	**Symptom:** Clients failed to connect to some APs randomly until the APs were rebooted. The fix ensures that the channel change is triggered only after the channel switch announcement happens. **Scenario:** This issue occurred when a channel change was triggered on the APs due to a RADAR detection before the channel switch announcement happened. This issue was observed on APs running AOS-W 6.4.4.6 or later versions.	AP-Wireless	All AP platforms	AOS-W 6.4.4.6	AOS-W 6.5.2.0
149594	**Symptom: AMON_USER_INFO_MESSAGE** did not contain the user-agent information of the device. This issue is resolved by adding the **MAC address** and **user-agent** fields in **AMON_USER_FINGERPRINT_INFO_MESSAGE**. **Scenario:** This issue was observed in a master-local setup when AMP switched from SNMP to AMON and SNMP sent the user-agent string. This issue was observed in switches running AOS-W 6.4.3.9 or later versions.	Base OS Security	All platforms	AOS-W6.4.3.9	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
149718 150678 150679 150683 151336 152025 152572 153743 154141 154574 155315 158126 158875 158970	**Symptom:** There were **do_ade** crashes in many applications as well as unaligned access. This issue is resolved by increasing the branch history table's depth to ten. **Scenario:** This issue occurred because of a complex sequence of internal CPU events. This in turn caused incorrect instruction fetch and execution of these instructions. This issue was observed in OAW-40xx Series and OAW-4x50 Series switches running AOS-W 6.4.2.15.	Switch-Platform	OAW-40xx Series and OAW-4x50 Series switches	AOS-W 6.4.2.15	AOS-W 6.5.2.0
150232	**Symptom:** A switch crashed and rebooted. The The fix ensures that the switch does not crash when running the Veriwave throughput test. **Scenario:** This issue occurred when running the Veriwave throughput test on the switch. This issue was observed in OAW-4005 and OAW-4030 switches running AOS-W 6.4.4.9 or later versions.	Switch-Datapath	OAW-4005 and OAW-4030 switches	AOS-W 6.4.4.9	AOS-W 6.5.2.0
150245	**Symptom:** The **show user essid** command failed to execute. The fix ensures that the command executes successfully. **Scenario:** This issue occurred when the ESSID contained one or more space characters. This issue was observed in switches running AOS-W 6.4.3.9.	Base OS Security	All platforms	AOS-W 6.4.3.9	AOS-W 6.5.2.0
150861	**Symptom:** A switch displayed the **Error, cert manager service is busy or not available for user** message. Improvements in handling the expired certificate resolves this issue. **Scenario:** This issue occurred in one of the following scenarios: ■ A user attempted to map a new certificate to an existing management user whose certificate had expired. ■ A user attempted to delete an existing management user whose certificate had expired. This issue was observed in switches running AOS-W 6.4.x or AOS-W 6.5.x.	Certificate Manager	All platforms	AOS-W 6.4.4.8	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
151105 151106	**Symptom:** Some APs did not communicate with a Meridian server. The fix ensures that the APs work as expected and communicate with a Meridian server. **Scenario:** This issue was observed in OAW-AP215 access points running AOS-W 6.4.4.8.	Bluetooth Low Energy	OAW-AP215 access points	AOS-W 6.4.4.8	AOS-W 6.5.2.0
151310 158038	**Symptom:** An AP rebooted unexpectedly due to low memory. The fix ensures that the debugging messages are not flooding the memory. **Scenario:** This issue occurred as a flood of debugging messages interrupted the kernel panic, which resulted in resetting the watchdog. This issue was observed in OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points running AOS-W 6.5.0.2 or later versions.	AP-Platform	OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points	AOS-W 6.5.0.2	AOS-W 6.5.2.0
151565	**Symptom:** The DHCP request packets were entering the firewall of the switch from RAP. This issue is resolved by ensuring that the AP's DHCP requests are not encrypted. **Scenario:** This issue occurred when an AP sent encrypted DHCP request packets with the DHCP server as the destination. This issue was observed in switches running AOS-W 6.3.1.22 or later versions.	Remote AP	All platforms	AOS-W 6.3.1.22	AOS-W 6.5.2.0
151579	**Symptom: Smart Configuration** page was not responding after multiple static routes were added on a branch configuration. This issue is resolved by enabling CLI pagination support for branch configuration. **Scenario:** This issue occurred when the size of the group configuration exceeded 40K. This issue was observed in branch switches running AOS-W 6.4.x and 6.5.x versions.	Branch office Switch	All platforms	AOS-W 6.5.0.1	AOS-W 6.5.2.0
151605 152410	**Symptom:** A client failed to pass traffic. The fix ensures that the client can pass traffic. **Scenario:** This issue occurred when a client sent an IP packet before the DHCP packet. This issue was observed in switches running AOS-W 6.4.4.6.	Base OS Security	All platforms	AOS-W 6.4.4.6	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
151855	**Symptom:** Some APs stopped responding and rebooted unexpectedly. The log file listed the reason for the event as **Unable to get IP address using DHCP after 10 tries, total DHCP retry:10** or **DHCP timed out**. Improvements in the AP memory management resolves this issue. **Scenario:** This issue was observed in OAW-AP90 Series, OAW-AP110 Series, OAW-RAP108, OAW-RAP109, or OAW-RAP3WN access points running AOS-W 6.4.4.9.	AP-Platform	OAW-AP90 Series, OAW-AP110 Series, OAW-RAP108, OAW-RAP109, or OAW-RAP3WN access points	AOS-W 6.4.4.9	AOS-W 6.5.2.0
151995	**Symptom:** The AP crashed and rebooted unexpectedly. The log for this event listed the reason as **Reboot caused by kernel panic: Fatal exception**. Improvements to the wireless driver resolved the issue. **Scenario:** This issue occurred due to high CPU and memory utilization. This issue was observed in APs running AOS-W 6.4.4.8 or later versions.	Wi-Fi Driver	All platforms	AOS-W 6.4.4.8	AOS-W 6.5.2.0
152040	**Symptom:** The AP crashed and rebooted unexpectedly. The log for this event listed the reason as **Reboot caused by kernel panic: Fatal exception**. The fix ensure that the race condition is prevented. **Scenario:** This issue occurred because of a race condition when scan table entries were getting updated. This issue was observed in OAW-AP325 access points running AOS-W 6.5.1.0 or later versions.	AP-Platform	OAW-AP325 access points	AOS-W 6.5.1.0	AOS-W 6.5.2.0
152332	**Symptom:** A blank image was displayed on the logon wait screen before the user was redirected to the captive portal page. The fix ensures that the user is redirected without any delay and the captive portal page appears correctly. **Scenario:** This issue occurred when the **logon-wait cpu-threshold** parameter was configured and the CPU utilization was high. As a result, HTTPD returned a transitional HTML page before redirecting to the captive portal page.	Web Server	All platforms	AOS-W 6.4.4.9	AOS-W 6.5.2.0
152467	**Symptom:** OAW-AP305 crashed and rebooted unexpectedly. The log for this event listed the reason as, **kernel panic: soft lockup: hung tasks**. The fix ensures that the AP does not crash. **Scenario:** This issue occurred when the **mac-address-and-dhcp-options** parameter was configured and the DHCP packet was incorrectly delivered to the DNS server. This issue was observed in OAW-AP305 access points running AOS-W 6.5.1.0 or later versions.	AP-Platform	OAW-AP305 access points	AOS-W 6.5.1.0	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
152602 154513	**Symptom:** The master switch failed to delete the stale route entries of the branch office switch on the master switch. When you attempted to manually delete an entry, the switch did not delete the entry and displayed the following error message: **ERROR: Cannot Delete Static Route**. The fix ensures that the master switch deletes the stale route entries of the branch office switch when you change the VLAN IP address of the branch office switch. **Scenario:** This issue occurred when you change the VLAN IP address of the branch office switch and uploaded an updated CSV file (static IP address template) on the master switch. This triggered a reboot of the branch office switch but failed to delete the stale route entries from the master switch. This issue was observed in a master-branch office switch deployment with switches running AOS-W 6.5.1.1 or later versions.	Branch Office Switch	All platforms	AOS-W 6.5.1.1	AOS-W 6.5.2.0
152665	**Symptom:** OAW-4550 switch crashed unexpectedly on the **FPCLI** module. The fix ensures that the switch works as expected. **Scenario:** This issue was observed in a master-standby topology with OAW-4550 switches running AOS-W 6.4.4.9 or later versions.	Switch-Platform	OAW-4550 switches	AOS-W 6.4.4.9	AOS-W 6.5.2.0
152672	**Symptom:** An AP generated multiple **asap_voip_log: netif_rx to stm failedwith ret : 1** messages. The fix ensures that these messages are not printed in the log files. **Scenario:** This issue occurred when an AP generated unwanted log messages. This issue was observed in access points running AOS-W 6.4.4.10.	UCC	All AP platforms	AOS-W 6.4.4.10	AOS-W 6.5.2.0
152688	**Symptom:** Windows clients lost connectivity when they roamed to a different L3 cluster. The fix ensures the client is not disconnected when roaming from one cluster to another. **Scenario:** This issue was observed in access points running AOS-W 6.4.2.6.	L3 Mobility	All platforms	AOS-W 6.4.2.6	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
152740 154234	**Symptom:** An increase in the memory consumption of the **authentication** process was observed when 802.11r clients were connected to the network. The fix ensures that when a user entry times out or is deleted, the neighbor entry list and the data associated with the user is deleted to avoid memory leak. **Scenario:** The neighbor list entry associated with the roaming user was not released when the user entry timed out or was deleted. This resulted in a memory leak of the **authentication** process in the switch. This issue was observed in OAW-4650 switches running AOS-W 6.4.3.10.	Base OS Security	OAW-4650 switches	AOS-W 6.4.3.10	AOS-W 6.5.2.0
152890 153324	**Symptom:** A switch stopped responding and rebooted. The log file for the event listed the reason as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. Updating the SDK to the latest version resolved the issue. **Scenario:** This issue occurred when the WebCC feature was enabled on the switch. This issue was observed in switches running AOS-W 6.5.0.2 or later versions.	Switch-Datapath	All platforms	AOS-W 6.5.0.2	AOS-W 6.5.2.0
153011 153017	**Symptom:**An AP-125 access point crashed. This issue is resolved by incorporating code changes in the Ethernet driver. **Scenario:** This issue was observed in AP-125 access points running AOS-W 6.4.4.10.	AP-Wireless	AP-125 access points	AOS-W 6.4.4.10	AOS-W 6.5.2.0
153073	**Symptom:** The Layer 2 (L2) GRE tunnel inside IPsec failed. This issue is resolved by resetting the packet VLAN after GRE encapsulation. Doing so ensures that the inner payload VLAN does not get applied to the outer GRE packet. **Scenario:** The issue occurred when L2 GRE configuration with tunnel VLAN having PBR rules was configured. This caused the payload VLAN getting applied to encapsulated GRE packets. This issue was observed in all switches running AOS-W 6.4.3.x or later versions.	GRE	All platforms	AOS-W 6.4.4.9	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
153216 153217	**Symptom:** Memory leak in the **auth** process caused a switch to go out of memory. This resulted in multiple processes getting killed. This issue is resolved by making the RADIUS server drop the RADIUS response packet that has more than one RADIUS-state attributes. **Scenario:** This issue occurred when the AAA server responded with more than one RADIUS-state attributes in the RADIUS packets. This did not comply with RFC 2865. This issue was observed in all platforms running AOS-W 6.3.x, AOS-W 6.4.x, or AOS-W 6.5.x.	Base OS Security	All platforms	AOS-W 6.4.3.6	AOS-W 6.5.2.0
153222	**Symptom:** OAW-AP324 and OAW-AP325 access points rebooted and the log files listed the reason as **kernel panic: softlockup: hung tasks**. This issue is resolved by removing the station device. **Scenario:** This issue was observed in OAW-AP324 and OAW-AP325 access points connected to switches running AOS-W 6.5.1.	ARM	OAW-AP324 and OAW-AP325 access points	AOS-W 6.5.1	AOS-W 6.5.2.0
153227	**Symptom:** Users were unable to configure an **ESSID** in the **Configuration > Wizards** page. This issue is resolved by updating the ESSID value for decrypt tunnel and bridge mode and allowing ESSID configuration for all modes. **Scenario:** This issue occurred when users tried to configure an ESSID through the WebUI with the forward mode set to decrypt tunnel or bridge mode. This issue was observed in switches running AOS-W 6.5.0.2.	ARM	All platforms	AOS-W 6.5.0.2	AOS-W 6.5.2.0
153463	**Symptom:** The AP channel utilization graph showed multiple breaks and was incomplete. The fix ensures that the AP channel utilization graph shows continuous and complete channel utilization. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.10.	AP-Wireless	All platforms	AOS-W 6.4.3.10	AOS-W 6.5.2.0
153576	**Symptom:** ARM was changing channels frequently. The fix ensures that ARM does not change channels frequently. **Scenario:** This issue was caused by a missing software logic. This issue was observed in access points connected to switches running AOS-W 6.5.0.0.	ARM	All platforms	AOS-W 6.5.0.0	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
153824	**Symptom:** Data was not transmitted when static IPsec routing with ip-to-ip IPsec tunnel was enabled. This issue is fixed by ensuring that the correct flag is used while installing route cache entry. **Scenario:** This issue occurred when the route cache entry was installed with the wrong flag. This issue was observed on switches running AOS-W 6.4.4.10.	IPsec	All platforms	AOS-W 6.4.4.10	AOS-W 6.5.2.0
153951 157497	**Symptom:** Datapath next hop was null. This issue is resolved by making sure that the incoming SPI and the SPI negotiated with the PAN Global Protect (PANGP) Gateway match. **Scenario:** This issue occurred because of incorrect modifications on incoming SPI values during decryption. This caused IP health check failure and the next hop null. This issues was observed in OAW-4005switch running AOS-W 6.5.x, in a Stand-alone topology.	Base OS Security	All platforms	AOS-W 6.5.0.3	AOS-W 6.5.2.0
154065	**Symptom:** Users were unable to access the internet periodically. This issue is resolved by changing the threshold for dropping packets from 8MB to 4MB. **Scenario:** . This issue occurred when the system dropped downstream packets to avoid an out of memory issue as the available system memory was between 4MB - 8MB. This issue was observed in OAW-AP205 access points and is not limited to any software version or switch model.	Datapath/Firewall	All platforms	AOS-W 6.4.4.8	AOS-W 6.5.2.0
154132	**Symptom:** Clients are unable to associate with APs. The fix ensures that the AP rejects HA configuration if the AP is unable to connect to LMS. **Scenario:** This issue occurred when an AP accepted HA configuration although it had lost connectivity to the LMS. This issue was observed in APs connected to switches running AOS-W 6.4.4.10.	AP-Wireless	All platforms	AOS-W 6.4.4.10	AOS-W 6.5.2.0
154147	**Symptom:** A client failed to establish an IKE VPN connection over an existing IPsec/L2TP VPN connection. This issue is resolved by adding an exception for the IKE traffic coming as L2TP traffic and by allowing the encryption of this IKE traffic in transport mode IPsec tunnel. **Scenario:** This issue occurred because IKE traffic encryption over transport mode IPsec tunnel was blocked. This also blocked the IKE traffic coming into the L2TP tunnel.	IPsec	All platforms	AOS-W 6.4.4.9	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
154245	**Symptom:** The web content classification was incorrect for some sites. Updating the SDK to the latest version resolves this issue. **Scenario:** This issue was observed in switches running AOS-W 6.4.x and AOS-W 6.5.x.	AppRF	All platforms	AOS-W 6.4.4.0	AOS-W 6.5.2.0
154291	**Symptom:** Although the user completed Captive Portal authentication and the appropriate role was set in the user table, **web auth disabled** message was displayed when the user tried to login again. The fix ensures that the authentication and user tables are synchronized. **Scenario:** When the user logged in again, MAC authentication failed. The user was deauthenticated from the L3 role and placed in pre-auth role as the authentication and user tables were not synchronized. This issue was observed in switches running AOS-W 6.3.1.23.	Base OS Security	All platforms	AOS-W 6.3.1.23	AOS-W 6.5.2.0
154422	**Symptom:** Clients failed to establish a VPN connection using L2TP over IPsec. The fix ensures that the clients can successfully establish a VPN connection when they are behind a NAT device. **Scenario:** This issue occurred when the clients were behind a NAT device. This issue was observed in switches running AOS-W 6.5.0.3 or later versions.	L2TP	All platforms	AOS-W 6.5.0.3	AOS-W 6.5.2.0
154443	**Symptom:** A user was stuck in the machine authentication role after an 802.1X authentication. The fix ensures that the user role is updated in the AP datapath. **Scenario:** This issue occurred when a user attempted multiple L2 authentications in split-tunnel forwarding mode and the user role was not updated in the AP datapath. This issue was observed in a master-local deployment with switches running AOS-W 6.4.4.10.	Base OS Security	All platforms	AOS-W 6.4.4.10	AOS-W 6.5.2.0
154483	**Symptom:** A switch stopped responding and rebooted. The log file for the event listed the reason as **isakmpd** and **datapath timeout**. This issue is resolved by restricting the deletion of a CA certificate if it is configured in group certificate. **Scenario:** This issue was triggered when you delete the global CA certificate from ISAKMP which is referenced in the group certificate. This issue was observed in switches running AOS-W 6.5.0.2 or later versions.	IPsec	All platforms	AOS-W 6.5.0.2	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
154487	**Symptom:** The **FPCLI** process crashed when the **show user authentication-method stateful-dot1x** command was executed. This issue is resolved by initializing the MAC address to NULL, if there is no entry made by the user. **Scenario:** This issue occurred when the user did not specify the MAC address when the **show user authentication-method stateful-dot1x** command was executed. This issue was observed in OAW-4750 switches running AOS-W 6.4.2.16, in a master-local topology.	Base OS Security	OAW-4750 switches	AOS-W 6.4.2.16	AOS-W 6.5.2.0
154507	**Symptom:** A switch redirected to the wrong URL. The fix ensures that the switch redirects to the correct URL. **Scenario:** This issue was observed in switches running AOS-W 6.5.1.0.	OEM	All platforms	AOS-W 6.5.1.0	AOS-W 6.5.2.0
154533	**Symptom:** An AirGroup user was not able to see an AirGroup server. The fix ensures that an AirGroup user is able to see an AirGroup server. **Scenario:** This issue occurred when an AirGroup user logged in with the domain name but the username was stored without stripping the domain name. This issue was observed in switches running AOS-W 6.4.x or AOS-W 6.5.x with ClearPass Policy Manager.	Switch-Platform	OAW-4750switches	AOS-W 6.4.3.0	AOS-W 6.5.2.0
154827 155214	**Symptom:** When the **show datapath dns-id-map** command was executed, the format of the IPv6 addresses listed were incorrect. This issue is resolved by modifying the mobility packets of the DNS list. **Scenario:** This issue occurred when the DNS packets contained AAA records for IPv6 address. This issue was observed in APs running AOS-W 6.5.1.0.	IPv6	All platforms	AOS-W 6.5.1.0	AOS-W 6.5.2.0
154882	**Symptom:** OAW-AP335 access point crashed and rebooted unexpectedly. The log for this event listed the reason as, **Kernel panic – not syncing Fatal Exception in Interrupt**. Improvements to the ethernet driver resolved the issue. **Scenario:** This issue was observed in OAW-AP335 access points running AOS-W 6.5.0.3 and later versions.	AP-Datapath	OAW-AP335 access points	AOS-W 6.5.0.3	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
154915 156084	**Symptom:** AP crashed and rebooted. The fix ensures that the AP does not crash when a wireless client tries to establish a connection to its BSS ID. **Scenario:** AP crashed when a wireless client tried to establish a connection to its BSS ID. This issue was observed in OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points running AOS-W 6.5.2.0.	AP-Wireless	OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points	AOS-W 6.5.2.0	AOS-W 6.5.2.0
155038	**Symptom:** The TACACS accounting configuration was deleted. The fix ensures that the TACACS accounting configuration is retained after upgrading AOS-W. **Scenario:** This issue occurred after upgrading a switch from AOS-W 6.4.2.x to AOS-W 6.4.3.x or later versions.	Base OS Security	All platforms	AOS-W 6.4.4.11	AOS-W 6.5.2.0
155081	**Symptom:** The **SNMP** process displayed an error - **OID not increasing**, when clients had a MAC address ending with **FF**. The fix ensures that the packets of clients having MAC address ending with **FF** are forwarded to the next node. **Scenario:** This issue was observed when the **SNMP** process used MAC address plus 1 and VLAN to search for the node. When the client had a MAC address ending with **FF**, the **SNMP** process used the MAC address ending with FF and VLAN to search for the next node, which resulted in an infinite loop. This issue was observed in access points running AOS-W 6.4.2.6.	SNMP	All platforms	AOS-W 6.4.2.6	AOS-W 6.5.2.0
155090 156580	**Symptom:** The **mDNS** process in switches crashed because of specific packets coming from the Cisco switch. This issue is resolved by adding the required protection to prevent any null access. **Scenario:** This issue occurred when AirGroup was enabled on the switchesand switches. However, specific switches (Cisco) replaced the MAC address of the original packets with their own MAC address and sent them to theswitch. This issue was observed in OAW-4650 switches running AOS-W 6.4.4.11.	AirGroup	All platforms	AOS-W 6.4.4.11	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
155215	**Symptom:** A user could not access the RAP console page. The fix ensures that the user can access the RAP console page. **Scenario:** This issue occurred when a user was in bridge-forwarding mode and attempted to access the RAP console page. This issue was observed in RAPs running AOS-W 6.4.3.x, AOS-W 6.4.4.x, or AOS-W 6.5.1.x.	AP Datapath	All platforms	AOS-W 6.4.4.11	AOS-W 6.5.2.0
155419	**Symptom:** A switch rebooted and log files listed the reason as **Nanny rebooted machine - fpapps process failed**. The issue is resolved by making changes in the **isakmpd** process. **Scenario:** This issue was caused by a memory leak that occurred due to a certificate mismatch when APs tried to establish a tunnel. This issue was observed in switches running AOS-W 6.4.3.6.	Switch-Platform	All platforms	AOS-W 6.4.3.6	AOS-W 6.5.2.0
155425	**Symptom:** Auto Sign-On between a switch and ClearPass Policy Manager failed. The fix ensures that Auto Sign-On succeeds. **Scenario:** This issue occurred when the length of a username exceeded 25 characters. This issue was observed in switches running AOS-W 6.4.4.11.	BaseOS Security	All platforms	AOS-W 6.4.4.11	AOS-W 6.5.2.0
155459 156718 158140	**Symptom:** An AP crashed unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue was observed after configuring a **deny-inter-user-bridging** ACL. This issue was observed in OAW-AP215 or OAW-AP305 access points running AOS-W 6.5.2.0.	Datapath/Firewall	OAW-AP215 and OAW-AP305 access points	AOS-W 6.5.2.0	AOS-W 6.5.2.0
155672	**Symptom:** When the **snmpwalk** command was executed, the output did not reflect the configured Link Aggregation Identifier. This issue is resolved by modifying the MIB value of the LinkAggregation interface to match the Port Channel Id. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.9.	SNMP	All platforms	AOS-W 6.4.4.9	AOS-W 6.5.2.0
155685	**Symptom:** A master switch crashed and rebooted unexpectedly. The log file for the event listed the reason as **Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2) and crashed on fpapps module**. The fix ensures that the applications are valid DPI applications. **Scenario:** This issue occurred when the **show datapath session dpi counters** command was executed. This issue was observed in switches running AOS-W 6.4.3.7 or later versions.	Switch-Platform	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
155730	**Symptom:** Client search based on the **User Name** field in the **Monitoring > NETWORK > All WLAN Clients** page of the WebUI failed to display correct results. The fix ensures that the client search from the WebUI works as expected. **Scenario:** This issue occurred when the user name of the client contained a special character such as **/**. This issue was observed in switches running AOS-W 6.4.4.10 or later versions.	WebUI	All platforms	AOS-W 6.4.4.10	AOS-W 6.5.2.0
155750	**Symptom:** The user roles went missing in a local switch. This issue is resolved by adding missing checks in handling Master-Master redundancy and license changes. **Scenario:** This issue occurred in a Master-Local or Master-Standby setup where Master had PEF license and Standby did not have PEF license. This issue was observed in all switches running AOS-W 6.4.x or later versions, in Master-Local or Master-Standby topology.	Base OS Security	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.2.0
155977	**Symptom:** A switch prompted to reboot when a non-master VRRP instance was added. The fix ensures that the switch does not prompt to reboot when a non-master VRRP instance is added. **Scenario:** This issue occurred when the **no shutdown** command was executed after adding a non-master VRRP instance. This issue was observed in a master-standby topology with switches running AOS-W 6.3.1.18.	VRRP	All platforms	AOS-W 6.3.1.18	AOS-W 6.5.2.0
156586	**Symptom:** When the VLAN of the server changed, the switch could not handle the DLNA update. This issue is resolved by sending wildcard query on the new VLAN. **Scenario:** This issue occurred when the final VLAN was not the default VLAN of the VAP. This resulted in the switch unable to learn DLNA from Chromecast. This issue was observed in OAW-4x50 Series switches running AOS-W 6.4.4.10.	AirGroup	All platforms	AOS-W 6.4.4.10	AOS-W 6.5.2.0
156951	**Symptom:** The **show running-config** command displayed extra spaces for IPv6-related ACLs, though the administrator configured the ACLs without any extra spaces. The fix ensures that the extra spaces are removed from the running configuration. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.9 or later versions.	Base OS Security	All platforms	AOS-W 6.4.4.9	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
157044	**Symptom:** The switches disclosed the SSH server version on performing a vulnerability scan. The fix ensures that the SSH server version is not disclosed. **Scenario:** This issue was not limited to any specific switch model or AOS-W version.	Base OS Security	All platforms	AOS-W 6.4.2.10	AOS-W 6.5.2.0
157056	**Symptom:** A local switch did not generate a syslog message for a successful 802.1X authentication of a client. The fix ensures that the syslog message is generated for successful 802.1X client authentications. **Scenario:** This issue was observed in a master local setup running AOS-W 6.4.4.10 or later versions.	Base OS Security	All platforms	AOS-W 6.4.4.10	AOS-W 6.5.2.0
157198	**Symptom:** Switch was unable to send IP address as a calling station ID. This issue is resolved by: ■ Changing the RADIUS attribute Calling-Station-Id based on the **use-ip-for-calling-station** parameter in RADIUS authentication server. ■ Adding Framed-IP-Address in the RADIUS packet. **Scenario:** When a VIA client was configured to use IKEv2 EAP-pass-through, the following issues were observed in the RADIUS packets that were exchanged with an external authentication server: ■ The Calling-Station-ID RADIUS-attribute was sent with zero-mac, allthough the **use-ip-for-calling-station** parameter was enabled in the RADIUS authentication server. ■ Framed-IP-Address RADIUS-attribute was not sent to the authentication server as its order in the **sending-VP-list** was after Message-Auth. This issue was observed during VIA authentication when connection-profile was configured with IKEv2 and EAP-pass through. This issue was observed in switches running AOS-W 6.5.0.3.	RADIUS	All platforms	AOS-W 6.5.0.3	AOS-W 6.5.2.0
157450	**Symptom:** APs did not come up in 802.3at mode although the switch provided 25.5W power. This issue is resolved by null terminating the power strings. **Scenario:** This issue randomly occurred when APs were configured to send and receive power TLV in LLDP. This issue was observed in OAW-AP330 Series access points running AOS-W 6.5.0.x and AOS-W 6.5.1.x versions.	AP-Platform	OAW-AP330 Series access points	AOS-W 6.5.0.0	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
157610	**Symptom:** While connecting to an external host using the **ssh** command on the switch, a random syntax error message was displayed. Improvements in handling special characters in the password field of the **ssh** command resolved this issue. **Scenario:** This issue occurred when the password for the host contained a special character such as **&**,*****,**(**,**)**, and **"**. This issue was observed in switches running AOS-W 6.5.0.0 or later versions.	Switch-Platform	All platforms	AOS-W 6.5.1.2	AOS-W 6.5.2.0
158031	**Symptom:** The **MobileIP** process crashed on a switch. The fix ensures that the **MobileIP** process does not crash. **Scenario:** This issue was observed when **router mobile** was enabled on the switch in the following scenarios: ■ When anchor tables were configured on the switch. ■ When the clients had static IP address. This issue was observed in switches running AOS-W 6.4.3.4 or later versions.	Mobility	All platforms	AOS-W 6.4.3.11	AOS-W 6.5.2.0
158229	**Symptom:** A switch showed an error on boot after an upgrade. The log file listed the reason for this event as **WARNING: Configuration upgrade failed**. The fix ensure that the switch upgrade is successful. **Scenario:** This issue was seen when a switch was upgraded from AOS-W 6.3 to AOS-W 6.4.4.12. This issue was observed in switches running AOS-W 6.4.4.12.	Base OS Security	All platforms	AOS-W 6.4.4.12	AOS-W 6.5.2.0
158368	**Symptom:** Users were not able to an access point and the log file listed the reason as **AP is resource constrained**. This issue is resolved by removing stale entries. **Scenario:** This issue was caused by stale entries. This issue was observed in access points connected to a OAW-4750 switch running AOS-W 6.5.1.3.	Base OS Security	All platforms	AOS-W 6.5.1.3	AOS-W 6.5.2.0

Table 3: *Resolved Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
158551	**Symptom:** Memory leak in the auth process caused a switch to go out of memory. This issue is resolved by freeing the memory reserved to handle a response from the RADIUS server. **Scenario:** This issue was caused when memory allocated for a response was not freed. This issue was observed in switches running AOS-W 6.5.0.3.	Base OS Security	All platforms	AOS-W 6.5.0.3	AOS-W 6.5.2.0
158580	**Symptom:** The **authentication** process on the switch crashed. The fix ensures that the **authentication** process functions as expected. **Scenario:** This issue occurred when the MAC address of a client was processed using an incorrect format specifier. This issue was observed in switches running AOS-W 6.5.1.4 or later versions.	Base OS Security	All platforms	AOS-W 6.5.1.4	AOS-W 6.5.2.0
159108 159268	**Symptom:** An AP crashed unexpectedly. The CPU core was stuck and the AP remained in the AP boot state until reboot. Improvements in handling the internal watchdog resolves this issue. **Scenario:** This issue occurred when the internal watchdog in an AP was stuck during AP boot. This issue was observed in APs running AOS-W 6.5.2.	AP-Platform	All AP platforms	AOS-W 6.5.2.0	AOS-W 6.5.2.0

This chapter describes the known and outstanding issues identified in AOS-W 6.5.2.0.

Table 4: *Known Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version
121019	**Symptom:** A few wireless clients are marked as internal in the user-table and assume ap-role. **Scenario:** This issue occurs when some wireless clients are assigned with the commonly used nonpublic IP addresses such as 192.168.1.*. These IP addresses clash with the AP's IP address. This issue is observed in switches running AOS-W 6.4.2.5 in a master-standby topology. **Workaround:** Do not assign commonly used non-public IP-addresses to APs.	Base OS Security	All platforms	AOS-W 6.4.2.5
128448	**Symptom:** A switch crashes and reboots unexpectedly. **Scenario:** After upgrading the switch from AOS-W 6.3.1.2 to AOS-W 6.4.4.1, the switch crashes while running some SNMPv3 queries if configured with VRRP. This issue is observed in OAW-4750 switches running AOS-W 6.4.4.1. **Workaround:** None.	Switch-Datapath	OAW-4750 switches	AOS-W 6.4.4.1
133036	**Symptom:** A switch encounters kernel panic. **Scenario:** This issue occurs when the USB reclassification happens many times, when a cellular modem—that is, modem models E3276 and E3372 (one that is not supported in AOS-W 6.5.0.0)— is connected as uplink to the switch in addition to the wired uplink. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** Either plug out and plug in the modem or reboot the switch.	Switch-Platform	All platforms	AOS-W 6.5.0.0

Table 4: *Known Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version
136329 138009	**Symptom:** An OAW-4650 switch (local) reboots because of datapath timeout. **Scenario:** This issue occurs after the local switch—supporting more than 1000 RAPs and 3000 wireless clients—is upgraded to AOS-W 6.4.2.15. This issue is observed in OAW-4650 switches running AOS-W 6.4.2.15 in a master-local topology. **Workaround:** None.	Switch-Datapath	OAW-4650 switches	AOS-W 6.4.2.15
138224	**Symptom:** A switch does not generate the syslog message 124821 when a Remote AP has loop on Ethernet ports. **Scenario:** This issue is observed in switches running AOS-W 6.3.1.16. **Workaround:** None.	Remote Access Point	All platforms	AOS-W 6.3.1.16
141285	**Symptom:** The ports on a switch move to **DOWN** state unexpectedly. **Scenario:** This issue is observed in OAW-4x50 Series switches running AOS-W 6.5.0.0. **Workaround:** None.	Switch-Platform	OAW-4x50 Series switches	AOS-W 6.5.0.0
148053	**Symptom:** A local switch reboots unexpectedly. The log file for the event lists the reason as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.4.4.9 in a master-local topology. **Workaround:** None.	Switch-Datapath	OAW-4650 switches	AOS-W 6.4.4.9
148172	**Symptom:** Users are unable to create VLANs as **Trusted** in a BOC interface. **Scenario:** This issue is observed in a master-branch switch deployment. This issue is persistent even after upgrading to AOS-W 6.5.0.0. **Workaround:** None.	WebUI	OAW-4x50 Series switches	AOS-W 6.5.0.0

Table 4: *Known Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version
149431	**Symptom:** Clients trying to access the Captive Portal page are redirected to the secure login page. **Scenario:** The WebUI shows that the default certificate is mapped for Captive Portal though the web-server profile in the CLI shows that custom certificate being mapped. This issue is observed in OAW-4650 stand-alone switches running AOS-W 6.5.0.0. **Workaround:** Reonfigure the web-server profile for skype4b configuration by executing the **web-skype4b-listen-port https 3999** command in the switch CLI.	Captive Portal	OAW-4650 switches	AOS-W 6.5.0.0.
152595	**Symptom:** The **datapath** process in a switch crashes and the switch 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 OAW-4550 switches running AOS-W 6.5.0.0. **Workaround:** None.	Switch-Datapath	OAW-4550 switches	AOS-W 6.5.0.0
152602 154513	**Symptom:** A master switch fails to delete the stale route entries of a branch office switch. When you attempt to manually delete an entry, the switch does not delete the entry and displays the **ERROR: Cannot Delete Static Route** error message. **Scenario:** This issue occurs when you change the VLAN IP address of the branch office switch and upload the updated CSV file (static IP address template) on the master switch. This triggers a reboot of the branch office switch but fails to delete the stale route entries from the master switch. This issue is observed in a master-branch office switch deployment with switches running AOS-W 6.5.1.1 or later versions. **Workaround:** None.	Branch Office Switch	All platforms	AOS-W 6.5.1.1
154286	**Symptom:** Client loses connectivity randomly and is unable to pass traffic. **Scenario:** This issue is observed in master-standby topology with switches running AOS-W 6.4.4.9. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.9

Table 4: *Known Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version
154470	**Symptom:** A user cannot upload a CSV file to a branch office switch using the WebUI or the CLI. The WebUI displays the **Failed to query VLANS** error and the CLI displays the **Error occurred while executing CLI command: bulkedit config-group SOHO-AMR-ShillerPark csv SOHO-AMR-ShillerPark.csv - Failed to query VLANS** error. **Scenario:** This issue occurs when a user attempts to upload a CSV file to a branch office switch. This issue is observed in a branch office switch topology with OAW-4550 switches running AOS-W 6.4.4.10. **Workaround:** None.	Branch Switch	OAW-4550 switches	AOS-W 6.4.4.10
154625	**Symptom:** There is a change in the VRRP state though there are no missed heartbeats. **Scenario:** This issue is observed when a standby switch inadvertently transitions to **Master** state due to delayed processing of VRRP advertisements from the master switch. **Workaround:** Disable debug logs and syslog server. Increase the advertisement interval.	VRRP	All platforms	AOS-W 6.5.0.3
155190	**Symptom:** A switch does not identify certain models of HPE DAC cables of 1 m, 3 m, or 7 m; for example, J9281B, J9285B, or J9536A. **Scenario:** This issue is observed in OAW-4550, OAW-4650, OAW-4750, or OAW-4750XM switches running AOS-W 6.x versions. **Workaround:** None.	Switch-Platform	OAW-4550, OAW-4650, OAW-4750, and OAW-4750XM switches	AOS-W 6.4.3.9

Table 4: *Known Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version
155332	**Symptom:** The number of DOWN APs in the **Monitoring > Network Summary > WLAN Network Status** page (in the **Access Points > Down APs** hyperlink) and that in the **All Access Points** page do not match. **Scenario:** This issue occurred when the user executed the command in the Master switch. This issue is observed in OAW-4550 switches deployed in Master-Local setup, running AOS-W 6.4.4.11 version. **Workaround:** ■ Use **Dashboard** in the WebUI to access the AP information. ■ Execute the **show ap database-summary** command or the **show ap database status down** command to display the correct number of DOWN APs.	UI-Monitoring	OAW-4550 switches	AOS-W 6.4.4.11
156030	**Symptom:** The **datapath** process in a switch crashes and the switch reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:2c)**.. **Scenario:** This issue is observed in a master-standby topology with 7205 switches running AOS-W 6.5.0.3. **Workaround:** None.	Switch-Datapath	OAW-4450 switches	AOS-W 6.5.0.3
156061 158728 159140	**Symptom:** Clients are unable to get a DHCP IP and the datapath bridge counters shows high allocation failures. **Scenario:** This issue is observed when the user upgrades to AOS-W 6.5.0.4. This issue is observed in OAW-4750 switches running AOS-W 6.5.0.2. **Workaround:** Enable preserve VLAN.	Switch-Datapath	OAW-4750 switches	AOS-W 6.5.0.2

Table 4: *Known Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version
156496	**Symptom:** Some APs are randomly stuck in ID state when trying to establish standby tunnel with the master switch. **Scenario:** This issue occurs when the PAPI remote-IP hash table is full and hence does not allow to create new PAPI entries. This issue is observed in OAW-4550 switch, which is deployed in Master-Local setup, running AOS-W 6.4.4.11. **Workaround:** None. Reboot is required to clean up the hash table.	Switch-Datapath	OAW-4550 switches	AOS-W 6.4.4.11
156660	**Symptom:** The AP image preload operation fails when executed from a OAW-4750 switch. **Scenario:** This issue is observed in OAW-4750 switches running AOS-W 6.5.2.0. **Workaround:** Disable DPI using the **no firewall dpi** command and reboot the switch.	Switch-Datapath	OAW-4750 switches	AOS-W 6.5.2.0
156878	**Symptom:** WMS offloading does not work in switches. **Scenario:** This issue occurs when **snmp-server source controller-ip** is configured in switches. Even after pushing the Mobility Manager commands from the OV3600 server, the Mobility Manager is not enabled. This issue is observed in all platforms running AOS-W 6.x-FIPS version, in a Master-Local or Stand-alone topology. **Workaround:** Remove the **snmp-server source controller-ip** configuration in switches.	SNMP	All platforms	AOS-W 6.4.3.7-FIPS
157661	**Symptom:** SDR-based VLAN assignment does not work in a switch when 802.11R is enabled. **Scenario:** This issue occurs when a client roams between 802.11R enabled BSSIDs. This issue is observed in switches running AOS-W 6.4.3.7. **Workaround:** None.	Role/VLAN Derivation	All platforms	AOS-W 6.4.3.7

Table 4: *Known Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version
157662	**Symptom:** A switch reboots unexpectedly. The log file for the event lists the reason as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:2c)**. **Scenario:** This issue was observed in a standalone master switch running AOS-W 6.4.4.8. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.8
157752	**Symptom:** Viber application traffic is not denied by AppRF as expected. **Scenario:** This issue occurs when a Viber call is initiated from one of the clients from an external network. This issue is observed in a OAW-4550 switch running AOS-W 6.4.4.10 **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.10
158108	**Symptom:** PPTP VPN does not work after upgrading from AOS-W 6.4.4.10 to AOS-W 6.5.0.3. **Scenario:** This issue was not specific to any switch model or AOS-W version. **Workaround:** None.	Remote Access VPN-PPTP	All platforms	AOS-W 6.4.4.10
158110	**Symptom:** The synchronization between a master and local switch fails randomly. **Scenario:** This issue is observed in a master-local-standby topology with switches running AOS-W 6.5.0.3. **Workaround:** None.	IPSec	All platforms	AOS-W 6.5.0.3
158252	**Symptom:** Network advertisement (NA) packets sent from the router are modified by the switch. **Scenario:** When Neighbor Discovery (ND) proxy is used in case of **bcmc-optimization**, the route-cache entry is used to send a proxy NA. The ipv6 route-cache entry in datapath does not store the R-bit status, as a result the proxy ND does not have this bit set. This issue is observed in switches running AOS-W 6.5.0.3 in a in a master-standby topology. **Workaround:** Disable **bcmc-optimization**.	IPv6	All platforms	AOS-W 6.5.0.3

Table 4: *Known Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version
158409	**Symptom:** Some APs fail to download the image from a OAW-4750 switch operating in FIPS mode. **Scenario:** This issue is observed in OAW-AP360 Series and OAW-AP303H access points while downloading the image from a OAW-4750 switch running AOS-W 6.5.2.0-FIPS version. **Workaround:** Disable DPI using the **no firewall dpi** command and reboot the switch.	Switch-Platform	OAW-4750 switches	AOS-W 6.5.2.0-FIPS
158448	**Symptom:** An AP crashes unexpectedly. **Scenario:** This issue is observed in OAW-AP103 access points running AOS-W 6.5.0.0. **Workaround:** Disable **bcmc-optimization**.	AP-Platform	OAW-AP103 access points	AOS-W 6.5.0.0
158842	**Symptom:** The enet1 port of an AP shows OperState UP although the wired port was shut down in the enet1 profile. **Scenario:** This issue is observed in OAW-AP225 access points running AOS-W 6.4.3.9. **Workaround:** None.	AP-Platform	OAW-AP225 access points	AOS-W 6.4.3.9
158872	**Symptom:** The **show iap table** command output shows duplicate entries after a VRRP failover. **Scenario:** This issue is observed in a OAW-4750 switch, which is deployed in a Master-Local topology, running AOS-W 6.4.4.11. **Workaround:** None.	VPN	All platforms	AOS-W 6.4.4.11
158899	**Symptom:** An AP crashes unexpectedly. **Scenario:** This issue is observed in OAW-AP103 access points running AOS-W 6.5.0.0 **Workaround:** None.	AP-Wireless	OAW-AP103 access points	AOS-W 6.5.0.0
158901	**Symptom:** An AP crashes and reboots unexpectedly. **Scenario:** This issue is observed in OAW-AP104 access points running AOS-W 6.5.0.0 **Workaround:** None.	AP-Wireless	OAW-AP104 access points	AOS-W 6.5.0.0

Table 4: *Known Issues in AOS-W 6.5.2.0*

Bug ID	Description	Component	Platform	Reported Version
158907	**Symptom:** An AP crashes and reboots unexpectedly. **Scenario:** This issue is observed in OAW-AP115 access points running AOS-W 6.5.0.0 **Workaround:** None.	AP-Wireless	OAW-AP115 access points	AOS-W 6.5.0.0
158965	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **Kernel panic – not syncing: Fatal exception in interrupt**. **Scenario:** This issue is observed in OAW-AP305 access points running AOS-W 6.5.1.4 **Workaround:** None.	AP-Wireless	OAW-AP305 access points	AOS-W 6.5.1.4
158996	**Symptom:** An AP crashes and reboots unexpectedly.. **Scenario:** This issue is observed in OAW-AP225 access points running AOS-W 6.4.4.11 with BLE on USB. **Workaround:** None.	AP-Platform	OAW-AP225 access points	AOS-W 6.4.4.11
159125	**Symptom:** A mesh point crashes unexpectedly and recovers after a few minutes. **Scenario:** This issue is observed OAW-AP274 access points which are configured as mesh points and run AOS-W 6.4.3.11. **Workaround:** None.	AP-Wireless	OAW-4650 switches	AOS-W 6.4.3.11
159137	**Symptom:** An AP crashes and reboots unexpectedly. **Scenario:** This issue is observed in OAW-AP104 access points running AOS-W 6.5.0.0 **Workaround:** None.	AP-Wireless	OAW-AP104 access points	AOS-W 6.5.0.0
159212	**Symptom:** The **Dashboard > Access Points** page in the WebUI shows the name of an AP as **UNKNOWN**. **Scenario:** This issue occurs after an AP failover. This issue is observed in switches running AOS-W 6.5.1.4. **Workaround:** None.	WebUI	OAW-AP104 access points	AOS-W 6.5.1.4
159235	**Symptom:** A switch goes offline in the OV3600 server. **Scenario:** This issue occurs when the SNMP trap host is deleted in the switch and the switch shows offline in the OV3600 server. This issue is observed in switches running AOS-W 6.4.4.9 or later version. **Workaround:** Configure the SNMPv3 user again using the **snmp-server user "test" auth-prot sha ****** priv-prot AES ******** command.	SNMP	All platforms	AOS-W 6.4.4.9

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

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

Topics in this chapter include:

Upgrade Caveats

- OAW-AP120 Series access points, OAW-4306 Series, OAW-4x04 Series, OAW-S3, and OAW-6000 switches are not supported from AOS-W 6.5.x. Do not upgrade to AOS-W 6.5.x if your deployment contains a mix of these switches in a master-local setup.
- If your switch is running AOS-W 6.4.0.0 or later versions, do not use a Windows-based TFTP server to copy the AOS-W image to the nonboot partition of the switch for upgrading or downgrading. Use FTP or SCP to copy the image.
- Starting from AOS-W 6.4.x, you cannot create redundant firewall rules in a single ACL. AOS-W will consider a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
  - source IP/alias
  - destination IP/alias
  - proto-port/service

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

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

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

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

- When upgrading the software in a multiswitch network (one that uses two or more Alcatel-Lucent switches), special care must be taken to upgrade all the switches in the network and to upgrade them in the proper sequence. (See Upgrading in a Multiswitch Network on page 50.)

GRE Tunnel-Type Requirements

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

- AOS-W 6.5.2.0 continues to support L2 GRE tunnel type zero, but it is recommended to use a non-zero tunnel type.
- If both L2 and L3 tunnels are configured between endpoint devices, you must use a non-zero tunnel type for L2 GRE tunnels.

Important Points to Remember and Best Practices

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

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

- What version of AOS-W is currently on the switch?
- Are all switches in a master-local cluster running the same version of software?
- Which services are used on the switches (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 switch. 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, refer to the "Software Licenses" chapter in the *AOS-W 6.5.x User Guide*.

Memory Requirements

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

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

In certain situations, a reboot or a shutdown could cause the switch 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 switch logs, crash data, or flash backups should be copied to a location off the switch, then deleted from the switch to free up flash space. You can delete the following files from the switch 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 49 to copy the **crash.tar** file to an external server, and then execute the **tar clean crash** command to delete the file from the switch.
- **Flash Backups:** Use the procedures described in Backing up Critical Data on page 49 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 switch.
- **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 49 to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the switch.

Backing up Critical Data

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

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

Backing up and Restoring Compact Flash in the WebUI

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

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

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

Backing up and Restoring Compact Flash in the CLI

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

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

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

   ```
   (host) # backup flash
   Please wait while we tar relevant files from flash...
   Please wait while we compress the tar file...
   Checking for free space on flash...
   ```

```
Copying file to flash...
File flashbackup.tar.gz created successfully on flash.
```

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

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

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

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

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

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

Upgrading in a Multiswitch Network

In a multiswitch network (a network with two or more Alcatel-Lucent switches), special care must be taken to upgrade all switches based on the switch type (master or local). Be sure to back up all switches being upgraded, as described in Backing up Critical Data on page 49.

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

To upgrade an existing multiswitch system to this version of AOS-W:

1. Load the software image onto all switches (including redundant master switches).
2. If all the switches cannot be upgraded with the same software image and rebooted simultaneously, use the following guidelines:
   a. Upgrade the software image on all the switches. Reboot the master switch. After the master switch completes rebooting, you can reboot the local switches simultaneously.
   b. Verify that the master and all local switches are upgraded properly.

Installing the FIPS Version of AOS-W 6.5.2.0

Download the FIPS version of the software from https://support.esd.alcatel-lucent.com.

Instructions on Installing FIPS Software

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

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

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

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

Upgrading to AOS-W 6.5.2.0

The following sections provide the procedures for upgrading the switch to AOS-W 6.5.2.0 by using the WebUI and the CLI.

Install Using the WebUI

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash space available for an upgrade using the WebUI. For details, see Memory Requirements on page 48.

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

Upgrading From an Older Version of AOS-W

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

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

Follow step 2 to step 11 of the procedure described in Upgrading From a Recent Version of AOS-W on page 51 to install the interim version of AOS-W, and then repeat steps 1 through 11 of the procedure to download and install AOS-W 6.5.0.0.

Upgrading From a Recent Version of AOS-W

The following steps describe the procedure to upgrade from one of these recent AOS-W versions:

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

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

Install the AOS-W software image from a PC or workstation using the WebUI on the switch. You can also install the software image from a TFTP or FTP server using the same WebUI page.

1. Download AOS-W 6.5.2.0 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.

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

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

Upgrade will not take effect until you reboot the switch.

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

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

    If you chose to automatically reboot the switch in step 8, the reboot process starts automatically within a few seconds (unless you cancel it).

12. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > NETWORK > All WLAN Controllers** page to verify the upgrade.

When your upgrade is complete, perform the following steps to verify that the 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 **Monitoring > NETWORK > Network Summary** page to determine if your APs are up and ready to accept clients. In addition, verify that the number of access points and clients are what you would expect.
3. Verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 49 for information on creating a backup. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses.

Install Using the CLI

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash space available for an upgrade using the CLI. For details, see Memory Requirements on page 48.

Upgrading From an Older Version of AOS-W

Before you begin, verify the version of AOS-W currently running on your switch. For more information, see Upgrading From an Older Version of AOS-W on page 51.

Follow steps 2 through 7 of the procedure described in Upgrading From a Recent Version of AOS-W on page 53 to install the interim version of AOS-W, and then repeat steps 1 through 7 of the procedure to download and install AOS-W 6.5.0.0.

Upgrading From a Recent Version of AOS-W

The following steps describe the procedure to upgrade from one of these recent AOS-W versions:

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

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

1. Download AOS-W 6.5.2.0 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**.
5. Execute the **copy** command to load the new image onto the nonboot partition.

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

or

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

or

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

or

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

The USB option is available on the OAW-40xx Series and OAW-4x50 Series switches.

6. Execute the **show image version** command to verify that the new image is loaded.
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 49 for information on creating a backup.

Downgrading

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

If you upgraded from AOS-W 3.3.x to AOS-W 5.0, the upgrade script encrypts the internal database. New entries created in AOS-W 6.5.2.0 are lost after the downgrade (this warning does not apply to upgrades from AOS-W 3.4.x to AOS-W 6.1).

If you do not downgrade to a previously saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from AOS-W 6.5.2.0 to 5.0.3.2, changes made to WIPS in AOS-W 6.x prevent the new predefined IDS profile assigned to an AP group from being recognized by the older version of AOS-W. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.

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

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

Before You Begin

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

1. Back up your switch. For details, see Backing up Critical Data on page 49.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W 6.5.2.0 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 6.5.2.0 flash backup from the file stored on the switch. Do not restore the AOS-W 6.5.2.0 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 6.5.2.0, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W 6.5.2.0, 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 preupgrade configuration file is on an external FTP/TFTP server, copy the file to the switch by navigating to the **Maintenance > File > Copy Files** page.

a. For **Source Selection**, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the preupgrade configuration file.
b. For **Destination Selection**, enter a file name (other than default.cfg) for Flash File System.

2. Set the switch to boot with your preupgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved preupgrade configuration file from the **Configuration File** drop-down list.
   b. Click **Apply**.
3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition) by performing the following steps:
   a. Enter the FTP/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
4. Navigate to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the system partition that contains the preupgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The switch reboots after the countdown period.
6. When the boot process is complete, verify that the switch is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

Downgrading Using the CLI

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

1. If the saved preupgrade 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 preupgrade configuration file.

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

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

   In the following example, partition 1, the backup system partition, contains the backup release AOS-W 6.1.3.2. Partition 0, the default boot partition, contains the AOS-W 6.5.2.0 image.

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 switch 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 switch logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
4. Provide the syslog file of the switch 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 logs from the switch.
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 switch) or any recent changes to your switch 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 switch 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 provides context-based controls to enforce application-layer security and prioritization.

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 AP. Remote AP extends the corporate network to users working from home, or at temporary work sites.

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.

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 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.