

# AOS-W 8.5.0.3



## **Copyright Information**

Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit:

<https://www.al-enterprise.com/en/legal/trademarks-copyright>

All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. (2019)

## **Open Source Code**

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses.

---

<b>Contents</b> .....	<b>3</b>
Revision History .....	5
<b>Release Overview</b> .....	<b>6</b>
Important Points Before Upgrading to AOS-W 8.5.0.0 .....	6
Related Documents .....	7
Supported Browsers .....	7
Contacting Support .....	8
<b>New Features and Enhancements</b> .....	<b>9</b>
<b>Supported Platforms</b> .....	<b>10</b>
Mobility Master Platforms .....	10
OmniAccess Mobility Controller Platforms .....	10
AP Platforms .....	10
<b>Regulatory Updates</b> .....	<b>13</b>
<b>Resolved Issues</b> .....	<b>14</b>
<b>Known Issues and Limitations</b> .....	<b>30</b>
<b>Upgrade Procedure</b> .....	<b>40</b>
Migrating from AOS-W 6.x to AOS-W 8.x .....	40

---

Important Points to Remember and Best Practices .....	41
Memory Requirements .....	41
Backing up Critical Data .....	42
Upgrading .....	44
Downgrading .....	46
Before You Call Technical Support .....	48
<b>Glossary of Terms .....</b>	<b>50</b>

## Revision History

The following table provides the revision history of this document.

**Table 1:** *Revision History*

Revision	Change Description
Revision 01	Initial release.

Use the following links to navigate to the corresponding topics:

- [New Features and Enhancements on page 9](#) describes the new features and enhancements introduced in this release.
- [Supported Platforms on page 10](#) describes the hardware platforms supported in this release.
- [Regulatory Updates on page 13](#) lists the regulatory updates in this release.
- [Resolved Issues on page 14](#) lists the issues resolved in this release.
- [Known Issues and Limitations on page 30](#) lists the issues identified in this release.
- [Upgrade Procedure on page 40](#) describes the procedures for upgrading your WLAN network to the latest AOS-W version.



---

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

---

## Important Points Before Upgrading to AOS-W 8.5.0.0

DPI classification is not initialized after a switch is upgraded from AOS-W 8.4.0.0, 8.4.0.1, or 8.4.0.2 to AOS-W 8.5.0.0. The affected platforms are OAW-4x50 Series switches.

An additional reboot of the affected platform is required to initialize DPI classification.

To check the status of DPI classification after upgrading an affected platform from AOS-W 8.4.0.0, 8.4.0.1, or 8.4.0.2 to AOS-W, 8.5.0.0, issue the **show firewall | include dpi** command. In the following example, DPI classification is disabled:

```
(host) #show firewall | include dpi
DPI Classification      Disabled [Cfg: enabled, PEF license: installed]
```

If DPI classification is enabled, further action is not needed. However, if DP classification is disabled, issue the **show datapath utilization** and check if the DPI classification CPUs are initialized. In the following example, the DPI classification CPUs are disabled:

```
(host) #show datapath utilization

Datapath CPU Allocation Summary
Slow Path (SP) : 1,  Slow Path Gateway (SPGW) : 1
Fast Path (FP) : 17,  Fast Path Gateway (FPGW) : 1
DPI : 0, Crypto (CRYP) : 0
Slow Path Spare (SPSPARE) : 0
```

If the DPI classification CPUs are not initialized, reboot the affected platform by:

- Issuing the **reload** command.
- Power cycling the switch.

## Related Documents

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

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

## Supported Browsers

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

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Firefox 48 and later on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 9.0 or later on macOS
- Google Chrome 67 and later on Windows 7, Windows 8, Windows 10, and macOS

## Contacting Support

**Table 2:** *Contact Information*

Contact Center Online	
Main Site	<a href="https://www.al-enterprise.com">https://www.al-enterprise.com</a>
Support Site	<a href="https://businessportal2.alcatel-lucent.com">https://businessportal2.alcatel-lucent.com</a>
Email	<a href="mailto:ebg_global_supportcenter@al-enterprise.com">ebg_global_supportcenter@al-enterprise.com</a>
Service & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

This chapter describes the features and/or enhancements introduced in AOS-W 8.5.0.3.

### **Enhancements to Datapath**

Starting from this release, new counters are added for quicker debugging when unsupported DHCP options are detected in datapath.

### **Limitation of OAW-AP510 Series Campus Access Points**

The OAW-AP510 Series Campus Access Points do not support UL MU-MIMO and DL MU-MIMO.

This chapter describes the platforms supported in AOS-W 8.5.0.3.

### Mobility Master Platforms

The following table displays the Mobility Master platforms that are supported in this AOS-W release:

**Table 3:** *Supported Mobility Master Platforms in AOS-W 8.5.0.3*

Mobility Master Family	Mobility Master Model
Hardware Mobility Master	MM-HW-1K, MM-HW-5K, MM-HW-10K
Virtual Mobility Master	MM-VA-50, MM-VA-500, MM-VA-1K, MM-VA-5K, MM-VA-10K

### OmniAccess Mobility Controller Platforms

The following table displays the OmniAccess Mobility Controller platforms that are supported in this AOS-W release:

**Table 4:** *Supported OmniAccess Mobility Controller Platforms in AOS-W 8.5.0.3*

OmniAccess Mobility Controller Family	OmniAccess Mobility Controller Model
OAW-40xx Series Hardware OmniAccess Mobility Controllers	OAW-4005, OAW-4008, OAW-4010, OAW-4024, OAW-4030
OAW-4x50 Series Hardware OmniAccess Mobility Controllers	OAW-4450, OAW-4550, OAW-4650, OAW-4750, OAW-4750XM, OAW-4850
MC-VA-xxx Virtual OmniAccess Mobility Controllers	MC-VA-50, MC-VA-250, MC-VA-1K

### AP Platforms

The following table displays the AP platforms that are supported in this AOS-W release:

**Table 5: Supported AP Platforms in AOS-W 8.5.0.3**

AP Family	AP Model
OAW-AP100 Series	OAW-AP104, OAW-AP105
OAW-AP103 Series	OAW-AP103
OAW-AP110 Series	OAW-AP114, OAW-AP115
OAW-AP130 Series	OAW-AP134, OAW-AP135
OAW-AP 170 Series	OAW-AP175AC, OAW-AP175AC-F1, OAW-AP175DC, OAW-AP175DC-F1, OAW-AP175P, OAW-AP175P-F1
OAW-AP200 Series	OAW-AP204, OAW-AP205
OAW-AP203H Series	OAW-AP203H
OAW-AP205H Series	OAW-AP205H
OAW-AP207 Series	OAW-AP207
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP
OAW-AP210 Series	OAW-AP214, OAW-AP215
OAW-AP 220 Series	OAW-AP224, OAW-AP225
228 Series	OAW-AP228
OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277
OAW-AP300 Series	OAW-AP304, OAW-AP305
OAW-AP303 Series	OAW-AP303
OAW-AP303H Series	OAW-AP303H
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP318 Series	OAW-AP210AP-318
OAW-AP320 Series	OAW-APAP-324, OAW-AP325

**Table 5:** Supported AP Platforms in AOS-W 8.5.0.3

AP Family	AP Model
OAW-AP330 Series	OAW-AP334, OAW-AP335
OAW-AP340 Series	OAW-AP344, OAW-AP345
OAW-AP360 Series	OAW-AP365, OAW-AP367
OAW-AP370 Series	OAW-AP374, OAW-AP375, OAW-AP377
OAW-AP387	OAW-AP387
OAW-AP510 Series	OAW-AP514, OAW-AP515
OAW-AP530 Series	OAW-AP534, OAW-AP535
OAW-AP550 Series	OAW-AP555
OAW-RAP3 Series	OAW-RAP3WN, OAW-RAP3WNP
OAW-RAP100 Series	OAW-RAP108, OAW-RAP109
OAW-RAP155 Series	OAW-RAP155, OAW-RAP155P

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

For a complete list of countries and the regulatory domains in which the APs are certified for operation, refer to the Downloadable Regulatory Table or the DRT Release Notes at [businessportal2.alcatel-lucent.com](http://businessportal2.alcatel-lucent.com).

The following default DRT file version is part of AOS-W 8.5.0.3:

- DRT-1.0\_72277

This chapter describes the issues resolved in AOS-W 8.5.0.3.



We have migrated to a new defect tracking tool. Some bugs are listed with the new bug ID, which is prefixed by AOS.

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-128555	155631	<p><b>Symptom:</b> A memory leak was found as a result of using a script to query the Monitoring Dashboard. The fix ensures that there is no memory leak in the managed devices.</p> <p><b>Scenario:</b> This issue occurred when certain <b>Monitoring Dashboard</b> queries were run either using a script or the WebUI, where memory relating to the query filter strings were not freed. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.</p>	Monitoring	All platforms	AOS-W 8.2.0.0
AOS-146118	178291	<p><b>Symptom:</b> The <b>dir</b> command did not contain few basic options such as sorting by date, name, size, and filtering by keyword. The fix ensures that the missing options are available in the command.</p> <p><b>Scenario:</b> This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.</p>	switch-Platform	All platforms	AOS-W 8.2.1.0
AOS-149543	183200	<p><b>Symptom:</b> During an upgrade process, the image files were left on the flash drive and the user was unable to upgrade the AOS-W image. The fix ensures that the user is able to upgrade the AOS-W image using flash.</p> <p><b>Scenario:</b> This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.</p>	switch-Platform	All platforms	AOS-W 8.2.0.0

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-154809	190272	<b>Symptom:</b> PPPoE stopped working on a OAW-RAP. The fix ensures that PPPoE works as expected on the OAW-RAP. <b>Scenario:</b> This issue occurred while provisioning a OAW-RAP using ZTP. This issue was observed in APs running AOS-W 8.2.1.1.	OAW-RAP	All platforms	AOS-W 8.2.1.1
AOS-155114	190678	<b>Symptom:</b> A user role under an ACL did not work like other session ACL in the managed device. The fix ensures that the managed device works as expected. <b>Scenario:</b> This issue was observed in managed devices running AOS-W 8.2.1.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.2.1.0
AOS-155697	191568	<b>Symptom:</b> Some user information such as client name, IP address, active controller IP, and forward mode were not visible occasionally under <b>Dashboard &gt; Clients</b> page in the WebUI. The fix ensures that the correct values are displayed. <b>Scenario:</b> This issue was observed in Mobility Masters and managed devices running AOS-W 8.3.0.1 or later versions.	WebUI	All platforms	AOS-W 8.3.0.1
AOS-155780	191686	<b>Symptom:</b> A VIA client did not connect to a VIA server. The fix ensures that the VIA client is able to connect to the VIA server. <b>Scenario:</b> This issue occurred when the VIA client was connected wirelessly to the same managed device on which the VIA VPN terminated. This issue was observed in managed devices running AOS-W 8.2.2.0 or later versions.	IPsec	All platforms	AOS-W 8.4.0.0
AOS-156727 AOS-156728 AOS-156834 AOS-158306 AOS-189954	193015 193016 193152 195249	<b>Symptom:</b> The <b>Cluster manager</b> process crashed in a managed device unexpectedly. The log files listed the reason for the event as <b>Module Cluster Manager Process is busy. Please try later</b> . The fix ensures that the managed device works as expected. <b>Scenario:</b> This issue occurred because the <b>lc-cluster exclude-vlan</b> string had more than 256 characters, which resulted in memory corruption. This issue is observed in managed devices running AOS-W 8.2.2.0 or later versions in a cluster setup.	Cluster-Manager	All platforms	AOS-W 8.2.2.0

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-156899	193229	<p><b>Symptom:</b> Multiple processes crashed on a Mobility Master. The log files listed the reason for the event as <b>PROCESS_NOT_RESPONDING_CRITICAL</b>. The fix ensures that the Mobility Master works as expected.</p> <p><b>Scenario:</b> This issue was observed in Mobility Masters running AOS-W 8.2.1.0 or later versions.</p>	switch-Platform	All platforms	AOS-W 8.2.1.0
AOS-157144	193538	<p><b>Symptom:</b> The <b>Station Management</b> process crashed continuously in a switch. The fix ensures that the switch works as expected.</p> <p><b>Scenario:</b> This issue occurred when a stand-alone switch running any AOS-W 8.x version was converted to managed node using the <b>write erase</b> command and then, upgraded to AOS-W 8.4.0.0 version and rebooted in the managed node. After that, the switch was again converted to stand-alone mode using <b>write erase</b> command. This issue was observed in switches running AOS-W 8.4.0.0 or later versions.</p>	Database	All platforms	AOS-W 8.4.0.0
AOS-158656	195704	<p><b>Symptom:</b> The password in the Active configuration was displayed in clear text in the log files when the <b>show log all   include phonehome</b> command was executed. The fix ensures that the active password is not displayed when the command is executed.</p> <p><b>Scenario:</b> This issue was observed in Mobility Masters running AOS-W 8.3.0.6.</p>	Logging	All platforms	AOS-W 8.3.0.6
AOS-182652 AOS-188650	—	<p><b>Symptom:</b> A managed device crashed and rebooted unexpectedly. The log files listed the reason for this event as <b>sos_stats_type_tnl_stats_global_display</b>. The fix ensures that the managed device works as expected.</p> <p><b>Scenario:</b> This issue occurred while trying to bring up APs and clients on the managed device. This issue was observed in OAW-4850 switches running AOS-W 8.4.0.0 or later versions.</p>	switch-Datapath	OAW-4850 switches	AOS-W 8.4.0.0

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-183626	—	<b>Symptom:</b> The CLI allowed configurations on the managed device when the <b>configuration-purge-pending-config</b> command was executed, even though previously entered commands were not committed. The fix ensures that the command works as expected. <b>Scenario:</b> This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	Configuration	All platforms	AOS-W 8.3.0.0
AOS-183656	—	<b>Symptom:</b> The WebUI displayed incorrect AP count in the <b>Dashboard &gt; Performance &gt; Access Points</b> page. The fix ensures that the correct number of APs are displayed in the WebUI. <b>Scenario:</b> This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.3.0.0
AOS-183914	—	<b>Symptom:</b> Some Skype users were unable to join conference calls. The fix ensures that the Skype users are able to connect and join conferences seamlessly. <b>Scenario:</b> This issue occurred when ALG was enabled and the PBR was configured to forward all traffic from clients to VPNC. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	switch-Datapath	All platforms	AOS-W 8.2.1.0
AOS-184051	—	<b>Symptom:</b> A Mobility Master sent NTP sync packets every 15 seconds to the NTP server. The fix ensures that the Mobility Master works as expected. <b>Scenario:</b> This issue occurred due to upstream reachability that triggered sync packets from the Mobility Master. This issue was observed in Mobility Masters running AOS-W 8.2.2.0 or later versions.	VLAN	All platforms	AOS-W 8.4.0.0
AOS-184288 AOS-188218	—	<b>Symptom:</b> The OpenFlow profile was enabled automatically in a managed device immediately after upgrade of the managed device. The fix ensures that the managed device works as expected. <b>Scenario:</b> This issue occurred when OpenFlow was disabled on the managed device prior to its upgrade. This issue was observed in managed devices running AOS-W 8.3.0.6 or later versions.	SDN	All platforms	AOS-W 8.3.0.6

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-184365 AOS-188342	—	<b>Symptom:</b> A managed device brought up in a full-setup mode got stuck during the boot up process and displayed the <b>Waiting for switch IP</b> error message. The fix ensures that the managed device works as expected. <b>Scenario:</b> This issue was observed in managed devices running AOS-W 8.4.0.2 or later versions.	DHCP	All platforms	AOS-W 8.4.0.2
AOS-184519	—	<b>Symptom:</b> A user was unable to delete the VLAN even though the VLAN was not mapped on any node or group on the managed device. The fix ensures that the managed device works as expected. <b>Scenario:</b> This issue was observed in managed devices running AOS-W 8.3.0.4.	Configuration	All platforms	AOS-W 8.3.0.4
AOS-184545 AOS-186523 AOS-187213	—	<b>Symptom:</b> An AP crashed and rebooted unexpectedly. The log file listed the reason for this event as <b>kernel panic: softlockup: hung tasks</b> . Reducing the batch size to 64 resolved this issue. <b>Scenario:</b> This issue occurred when the AP processed large batch files that led to lock stall detection and caused panic. This issue was observed in OAW-AP303H access points running AOS-W 8.2.0.0 or later versions.	AP Datapath	OAW-AP303H access points	AOS-W 8.2.0.0
AOS-184707 AOS-185647	—	<b>Symptom:</b> A few OAW-RAPs failed to come up on the managed device after reboot of the APs, and received the same inner IP which had already been assigned to other OAW-RAPs. The fix ensures that the OAW-RAPs boot up successfully with new inner IP addresses. <b>Scenario:</b> This issue occurred because most of the OAW-RAP whitelist database entries were removed from the Mobility Master. This issue was observed in APs running AOS-W 8.2.1.0 or later versions.	CPsec	All platforms	AOS-W 8.2.1.0
AOS-185327	—	<b>Symptom:</b> The <b>show ap debug radio stats</b> command displayed incorrect values of Rx Time percentage. The fix ensures that the command displays the correct values. <b>Scenario:</b> This issue was observed in Mobility Master running AOS-W 8.5.0.0 or later versions.	AP-Wireless	All platforms	AOS-W 8.5.0.0

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-185500 AOS-186325 AOS-188413 AOS-189366 AOS-192566	—	<p><b>Symptom:</b> The <b>sapd</b> process crashed in a managed device unexpectedly. The fix ensures that the managed device works as expected.</p> <p><b>Scenario:</b> This issue was observed in managed devices running AOS-W 8.3.0.6.</p>	AP-Wireless	All platforms	AOS-W 8.3.0.6
AOS-185602 AOS-187149 AOS-188372 AOS-189992 AOS-191622 AOS-192188	—	<p><b>Symptom:</b> A few APs consumed more licenses than the actual number of APs that were up on the network because S-AAC (standby) mesh AP consumed Active AP licenses. The fix ensures that the standby mesh APs do not consume Active APs' licenses.</p> <p><b>Scenario:</b> This issue occurred when virtual AP was enabled in the mesh point connected to the mesh portal in a cluster setup. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.</p>	AP-Platform	All platforms	AOS-W 8.5.0.0
AOS-185833	—	<p><b>Symptom:</b> A few APs crashed unexpectedly. The log file listed the reason for this event as <b>ar_wal_vdev.c:2528 Assertion;Thread ID : 0x0000005e;PC : 0x4b0c9de8</b>. Enhancements to the wireless driver resolved the issue.</p> <p><b>Scenario:</b> This issue was observed in OAW-AP535 access points running AOS-W 8.5.0.0 or later versions.</p>	AP-Wireless	OAW-AP535 access points	AOS-W 8.5.0.0
AOS-186009 AOS-189072	—	<p><b>Symptom:</b> The AP database for an access point displayed <b>F</b> flag after successful 802.1x authentication. The fix ensures that the AP works as expected.</p> <p><b>Scenario:</b> This issue was observed in OAW-AP303H access points running AOS-W 8.3.0.3 or later versions.</p>	AP-Platform	OAW-AP303H access points	AOS-W 8.3.0.3
AOS-186059	—	<p><b>Symptom:</b> A few clients connected to an AP in a cluster were able to discover AirGroup server from another cluster, even though the Auto-association feature was enabled on the AirGroup server. The fix ensures that the clients are restricted from discovering the AirGroup servers from other clusters.</p> <p><b>Scenario:</b> This issue occurred due to a leak in the <b>mDNS</b> process between Mobility Masters. This issue was observed in APs running AOS-W 8.2.0.0 or later versions in a cluster setup.</p>	AirGroup	All platforms	AOS-W 8.3.0.4

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-186076 AOS-187884 AOS-189850 AOS-191866 AOS-192125 AOS-192310 AOS-193177 AOS-193387 AOS-193581	—	<p><b>Symptom:</b> The <b>stm</b> process crashed in a managed device unexpectedly during cluster failover. The fix ensures that the managed device works as expected.</p> <p><b>Scenario:</b> This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions in a cluster setup.</p>	Station Management	All platforms	AOS-W 8.3.0.0
AOS-186160	—	<p><b>Symptom:</b> A few users were unable to move the managed device with LACP port configuration to the new node path. The log files listed the reason for the event as <b>Illegal Operation: Interface belongs to lacp group</b>. The fix ensures that the managed device can be moved to the new node.</p> <p><b>Scenario:</b> This issue was observed in Mobility Master Virtual Appliances running AOS-W 8.2.2.4 or later versions.</p>	Interface	All platforms	AOS-W 8.2.2.4
AOS-186184	—	<p><b>Symptom:</b> The <b>Configuration &gt; Access Points</b> page in the WebUI did not display the SNMP System Location. The fix ensures that SNMP System Location is displayed in the WebUI.</p> <p><b>Scenario:</b> This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.</p>	WebUI	All platforms	AOS-W 8.3.0.0
AOS-186204	—	<p><b>Symptom:</b> A few users got disconnected when the managed device crashed on <b>authentication</b> process. The fix ensures that the managed device works as expected.</p> <p><b>Scenario:</b> This issue was observed in OAW-40xx Series switches and OAW-4x50 Series switches running AOS-W 8.3.0.0 or later versions.</p>	Base OS Security	OAW-40xx Series switches and OAW-4x50 Series switches	AOS-W 8.3.0.0
AOS-186252	—	<p><b>Symptom:</b> A switch crashed and rebooted unexpectedly. The log file listed the reason for this event as <b>Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)</b>. The fix ensures that the switch works as expected.</p> <p><b>Scenario:</b> This issue was observed in OAW-4750 switches running AOS-W 8.2.0.0 or later versions.</p>	switch-Datapath	OAW-4750 switches	AOS-W 8.2.0.0

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-186386 AOS-186556	—	<p><b>Symptom:</b> A few clients failed to obtain the IPv6 address from the external DHCPv6 servers. The fix ensures that the managed devices work as expected.</p> <p><b>Scenario:</b> This issue occurred when the <b>bc-mc optimization</b> parameter was enabled by using the <b>interface vlan &lt;vlan&gt;</b> command. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.</p>	DHCP	All platforms	AOS-W 8.3.0.0
AOS-186526	—	<p><b>Symptom:</b> The <b>profmgr</b> process in a Mobility Master crashed unexpectedly. The fix ensures that the Mobility Master works as expected.</p> <p><b>Scenario:</b> This issue was observed in Mobility Masters running AOS-W 8.4.0.0.</p>	IPsec	All platforms	AOS-W 8.4.0.0
AOS-186653	—	<p><b>Symptom:</b> The <b>authentication</b> process in a managed device crashed unexpectedly. The fix ensures that the managed device works as expected.</p> <p><b>Scenario:</b> This issue occurred when the conflicting authentication types (OAW-AP and OAW-RAP) passed through the same NAT routing path. This issue was observed in managed devices running AOS-W 8.3.0.0.</p>	Base OS Security	All platforms	AOS-W 8.3.0.0
AOS-186840	—	<p><b>Symptom:</b> The <b>DPI</b> process incorrectly categorized all traffic as <b>alg-rtp</b>. The fix ensures that <b>DPI</b> process categorizes the traffic appropriately.</p> <p><b>Scenario:</b> This issue occurs when DPI was enabled and maximum support datapath sessions were created. This issue was observed in managed devices running AOS-W 8.3.0.6.</p>	UCC	All platforms	AOS-W 8.3.0.6

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-186884	—	<p><b>Symptom:</b> The POE status of an AP was displayed as <b>POE AF</b> even though 25.5 W of power was allocated to the AP through LLDP. This issue is resolved by changing the output of the <b>show ap debug system-status ap-name</b> command and associating the power supply status with the overall AP power status. The overall AP power status is derived from the results of the physical layer classification and the data link classification. For APs that have a single Ethernet port, a line with title <b>HW POE Status</b> is added.</p> <p><b>Scenario:</b> This issue was observed in APs running AOS-W 8.5.0.0.</p>	AP-Wireless	All platforms	AOS-W 8.5.0.0
AOS-186969	—	<p><b>Symptom:</b> The <b>Acct-Authentic radius</b> attribute was not sent from the managed device. The fix ensures that the managed device works as expected.</p> <p><b>Scenario:</b> This issue occurred when the managed devices were upgraded to AOS-W 8.4.0.2. This issue was observed in managed devices running AOS-W 8.4.0.2 or later versions.</p>	Radius	All platforms	AOS-W 8.4.0.2
AOS-186979	—	<p><b>Symptom:</b> A few APs were unable to reboot automatically after an uplink or WAN link status change. The fix ensures that the APs work as expected.</p> <p><b>Scenario:</b> This issue was observed in APs running AOS-W 8.3.0.6 or later versions.</p>	AP-Platform	All platforms	AOS-W 8.3.0.6
AOS-187041	—	<p><b>Symptom:</b> A FIPS-enabled ClearPass Policy Manager server failed to establish an SSH session with the Mobility Master. This issue is resolved by adding support for Diffie-Hellman-Group14-SHA256 in Mobility Masters.</p> <p><b>Scenario:</b> This issue occurred when a Mobility Master offered only Diffie-Hellman-Group14-SHA1 keys instead of Diffie-Hellman- Group14-SHA256 keys. This issue was observed in Mobility Masters running AOS-W 8.2.0.0 or later versions in both FIPS and non- FIPS mode.</p>	Base OS Security	All platforms	AOS-W 8.3.0.0

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-187115 AOS-190146	—	<p><b>Symptom:</b> The application name in the policy configuration was incorrect in the <b>Configuration &gt; Roles &amp; Policies &gt; Policies &gt; &lt;Policy name&gt;</b> page in the WebUI. The fix ensures that the correct application name is displayed in the WebUI.</p> <p><b>Scenario:</b> This issue occurred when the WebUI was accessed for the first time. This issue was observed in Mobility Masters running AOS-W 8.2.0.0 or later versions.</p>	WebUI	All platforms	AOS-W 8.3.0.4
AOS-187171	—	<p><b>Symptom:</b> A few split tunnel clients got disconnected frequently. The log files listed the reason for the event as <b>Denied; Ageout</b>. The fix ensures that the clients do not get disconnected.</p> <p><b>Scenario:</b> This issue was observed in stand-alone switches running AOS-W 8.2.0.0 or later versions.</p>	Base OS Security	All platforms	AOS-W 8.4.0.1
AOS-187328	—	<p><b>Symptom:</b> A configuration failure error occurred on managed devices. This issue is resolved by adding a validation check for SNMP names in the <b>profile manager</b> process.</p> <p><b>Scenario:</b> This issue occurred when a deprecated SNMP trap was pushed from the Mobility Master to the managed devices. When the SNMP trap was not part of the <b>show snmp trap-list</b> command, the SNMP process validation failed but the <b>profile manager</b> process did not perform the validation. This issue was observed in managed devices and stand-alone switches running AOS-W 8.2.2.3.</p>	SNMP	All platforms	AOS-W 8.2.2.3
AOS-187337	—	<p><b>Symptom:</b> The WebUI allowed user to access pages which were inaccessible to administrators. This issue is resolved by providing access only to the authorized pages and removing access privileges to unauthorized pages.</p> <p><b>Scenario:</b> This issue was observed in managed devices running AOS-W 8.5.0.0.</p>	WebUI	All platforms	AOS-W 8.5.0.0

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-187341	—	<p><b>Symptom:</b> The <b>panic list file</b> command listed operating system files. This issue is resolved by removing the obsolete <b>panic</b> command from the CLI.</p> <p><b>Scenario:</b> This issue was observed in managed devices running AOS-W 8.5.0.0.</p>	switch-Platform	All platforms	AOS-W 8.5.0.0
AOS-187671	—	<p><b>Symptom:</b> The <b>mDNS</b> process crashed and the managed device rebooted unexpectedly. This issue is resolved by avoiding memory corruption in the <b>mDNS</b> process.</p> <p><b>Scenario:</b> This issue occurred because of a memory corruption in the <b>mDNS</b> process. This issue was observed in managed devices running AOS-W 8.3.0.7.</p>	AirGroup	All platforms	AOS-W 8.3.0.7
AOS-187906	—	<p><b>Symptom:</b> The AP image mismatch logs were classified as debugging logs instead of error logs. The fix ensures that the AP works as expected.</p> <p><b>Scenario:</b> This issue was observed in APs running AOS-W 8.3.0.6 or later versions.</p>	AP-Platform	All platforms	AOS-W 8.3.0.6
AOS-188170	—	<p><b>Symptom:</b> The Common Name of captive portal certificate was changed from the company's domain name to <b>securelogin.arubanetworks.com</b> after upgrading the managed device. The fix ensures that when the switch certificate expires, the captive portal certificate does not get replaced by the default certificates.</p> <p><b>Scenario:</b> This issue occurred when a custom certificate used for switch certificate expired and the captive portal certificate got replaced with the default certificate. This issue was observed in managed devices running AOS-W 8.3.0.7 or later versions.</p>	Certificate Manager	All platforms	AOS-W 8.3.0.7
AOS-188207	—	<p><b>Symptom:</b> A few users were unable to discover a Google Chromecast device that acted as an AirGroup server on the Mobility Master. The fix ensures that the Mobility Master works as expected and the users are able to discover the Google Chromecast device.</p> <p><b>Scenario:</b> This issue was observed in Mobility Masters running AOS-W 8.2.2.0 or later versions.</p>	AirGroup	All platforms	AOS-W 8.3.0.7

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-188486	—	<p><b>Symptom:</b> A client was redirected to the hostname configured in the captive portal profile but a blank page was displayed in the browser. This issue is resolved by adding a netdestination entry for the captive portal host.</p> <p><b>Scenario:</b> This issue occurred when the captive portal login page was configured as FQDN host. This issue was observed in managed devices running AOS-W 8.4.0.2.</p>	WebUI	All platforms	AOS-W 8.4.0.2
AOS-188590	—	<p><b>Symptom:</b> The <b>mDNS</b> process crashed and the Mobility Master rebooted unexpectedly. This issue is resolved by identifying all the nodes where the AirGroup service is used and deactivating or activating the AirGroup profile at the child nodes.</p> <p><b>Scenario:</b> This issue occurred when an AirGroup profile was not found at a node but the activate API was invoked. This issue was observed in a Mobility Master running AOS-W 8.3.0.7.</p>	AirGroup	All platforms	AOS-W 8.3.0.7
AOS-188594	—	<p><b>Symptom:</b> The <b>datapath</b> process in a switch crashed unexpectedly. The fix ensures that the <b>datapath</b> process does not crash and the switch works as expected.</p> <p><b>Scenario:</b> This issue occurred when the data traffic that was sent from the switch to the VPN Concentrator (VPNC) was not fully compressed. This issue was observed in OAW-4450 switches running AOS-W 8.2.0.0 or later versions.</p>	switch-Datapath	OAW-4450 switches	AOS-W 8.5.0.0
AOS-188597	—	<p><b>Symptom:</b> A managed device failed to send User-ID update to Palo Alto Network even though the managed device successfully established HTTPS connection to Palo Alto Network firewall. This issue is resolved by providing the missing key-name for the key-attribute in the User-ID PAN-API message.</p> <p><b>Scenario:</b> This issue occurred because of a missing key-name for the key-attribute in the User-ID PAN-API message. This issue was observed in managed devices running AOS-W 8.4.0.0 or later versions.</p>	Base OS Security	All platforms	AOS-W 8.4.0.0

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-188830	—	<p><b>Symptom:</b> Some configurations were lost when L2 switchover occurred in a Mobility Master. The fix ensures that the Mobility Master works as expected.</p> <p><b>Scenario:</b> This issue was observed in a Mobility Master running AOS-W 8.5.0.2.</p>	Configuration	All platforms	AOS-W 8.5.0.2
AOS-188971	—	<p><b>Symptom:</b> A few split tunnel clients got disconnected frequently. The log files listed the reason for the event as <b>Denied; Ageout</b>. The fix ensures that the split tunnel clients do not get disconnected.</p> <p><b>Scenario:</b> This issue occurred when the split tunnel had more than one IP address (IPv4 and IPv6), and the client got deauthenticated even if one of the IP addresses sent or received traffic. This issue was observed in a stand-alone switch running AOS-W 8.4.0.1 or later versions.</p>	Station Management	All platforms	AOS-W 8.4.0.1
AOS-189008	—	<p><b>Symptom:</b> An AP showed a high RSSI value. This issue is resolved by enhancing the wireless driver to show the correct RSSI value.</p> <p><b>Scenario:</b> The issue occurred when low power was used on the AP radio. This issue was observed in OAW-AP515 access points running AOS-W 8.4.0.3.</p>	AP-Wireless	OAW-AP515 access points	AOS-W 8.5.0.2
AOS-189160	—	<p><b>Symptom:</b> A few APs rebooted unexpectedly. The log files listed the reason for the event as <b>Critical process /aruba/bin/rapper [pid 7933] DIED, process marked as RESTART</b>. The fix ensures that the APs work as expected.</p> <p><b>Scenario:</b> This issue was observed in APs running AOS-W 8.3.0.4 or later versions in a Mobility Master-Managed Device topology.</p>	IPsec	All platforms	AOS-W 8.3.0.4
AOS-189189	—	<p><b>Symptom:</b> A few users were unable to establish a VPN connection with the managed device or VPNC using AnyConnect application. The fix ensures that the AnyConnect application is able to establish the VPN connection.</p> <p><b>Scenario:</b> This issue occurred when IP Compression was enabled on the managed device or VPNC. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.</p>	switch-Datapath	All platforms	AOS-W 8.5.0.0

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-189300 AOS-192761	—	<p><b>Symptom:</b> A few managed devices crashed and rebooted unexpectedly. The log file listed the reason for this event as <b>Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)</b>. The fix ensures that the managed devices work as expected.</p> <p><b>Scenario:</b> This issue occurred when the site-to-site IPsec tunnel was disconnected on the managed device. This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.</p>	switch-Datapath	All platforms	AOS-W 8.5.0.0
AOS-189429	—	<p><b>Symptom:</b> XSS allowed client-supplied data from malicious users to execute commands in users' web browser. The fix ensures that the XSS does not allow data supplied from malicious users to execute commands in the users' web browsers.</p> <p><b>Scenario:</b> This issue was observed in managed devices running AOS-W 8.5.0.0 or later versions.</p>	Configuration	All platforms	AOS-W 8.5.0.0
AOS-189504	—	<p><b>Symptom:</b> The <b>Configuration &gt; Interfaces &gt; Ports</b> page in the WebUI displayed the <b>Expecting string of length 1 to 32</b> error message in the <b>Allowed VLANs</b> field. The output of the <b>interface port-channel</b> command also displayed the same error message. The issue is resolved by increasing the string length of the trusted VLAN to 255 characters.</p> <p><b>Scenario:</b> This issue occurred when the trunk allowed VLAN was added from either WebUI or CLI, due to which trusted VLANs beyond 32 characters could not be added. This issue was observed in Mobility Masters running AOS-W 8.2.1.0 or later versions.</p>	VLAN	All platforms	AOS-W 8.4.0.0
AOS-189551	—	<p><b>Symptom:</b> Port Based Tunnel (PBT) client traffic from different ports of the same switch was not broadcasted across multiple CPUs and a single CPU was used for client traffic. The fix ensures that the switch is able to broadcast PBT to multiple CPUs.</p> <p><b>Scenario:</b> This issue was observed in OAW-4850 switches running AOS-W 8.0.0.0 or later versions.</p>	switch-Datapath	OAW-4850 switches	AOS-W 8.5.0.0

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-189625	—	<p><b>Symptom:</b> A few switches crashed and rebooted unexpectedly. The log files listed the reason for the event as <b>Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)</b>. The fix ensures that the switches work as expected.</p> <p><b>Scenario:</b> This issue occurred when DPI was enabled on the switches. This issue was observed in OAW-4750 and OAW-4750XM switches running AOS-W 8.5.0.0 or later versions.</p>	switch-Datapath	OAW-4750 and OAW-4750XM switches	AOS-W 8.5.0.2
AOS-189782	—	<p><b>Symptom:</b> A user was unable to perform SSO with ClearPass Policy Manager and had to enter the username and password manually. The fix ensures that the SSO works correctly with ClearPass Policy Manager.</p> <p><b>Scenario:</b> This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.</p>	Base OS Security	All platforms	AOS-W 8.3.0.0
AOS-189802 AOS-190543	—	<p><b>Symptom:</b> The Google Chromecast service stopped responding unexpectedly in an AP. The issue is resolved by converting the OAW-APs to OAW-RAPs.</p> <p><b>Scenario:</b> This issue occurred when the Google ChromeCast device and the guest wireless client were connected to the same AP in bridge mode SSID. This issue was observed in OAW-AP303H access points running AOS-W 8.2.2.0 or later versions in a stand alone switch.</p>	AP Datapath	OAW-AP303H access points	AOS-W 8.4.0.1
AOS-189986	—	<p><b>Symptom:</b> A few users were unable to configure the WPA passphrase and received the <b>Fields does not match</b> error message under <b>Security</b> tab in the <b>Configuration &gt; WLANs &gt; New WLAN</b> page of the WebUI. The fix ensures that the users are able to configure the WPA passphrase.</p> <p><b>Scenario:</b> This issue occurred when the users added an extra space at the end of the WPA passphrase. This issue was observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.</p>	WebUI	All platforms	AOS-W 8.4.0.2
AOS-190474 AOS-190710	—	<p><b>Symptom:</b> The <b>mDNS</b> process in a managed device crashed unexpectedly. The fix ensures that the managed device works as expected.</p> <p><b>Scenario:</b> This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.</p>	AirGroup	All platforms	AOS-W 8.5.0.1

**Table 6:** Resolved Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-190478	—	<p><b>Symptom:</b> The <b>WARN  fpapps  Duplicate MAP_ADD from IKE for default-ha-ipsecmap</b> syslog messages were generated on a managed device. The fix ensures that the syslog messages are not displayed.</p> <p><b>Scenario:</b> The syslog messages were displayed only when the logging level of type information was enabled. This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions in a cluster setup.</p>	switch-Datapath	All platforms	AOS-W 8.3.0.7
AOS-190643	—	<p><b>Symptom:</b> An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as <b>kernel panic: Fatal exception in interrupt</b>. Enhancements to the wireless driver resolved the issue.</p> <p><b>Scenario:</b> This issue was observed in OAW-AP205, OAW-AP215, and OAW-AP225 access points running AOS-W 8.3.0.0 or later versions.</p>	AP-Wireless	OAW-AP205, OAW-AP215, and OAW-AP225 access points	AOS-W 8.5.0.1
AOS-191025	—	<p><b>Symptom:</b> A few devices dropped the DHCPv6 solicit packet sent by APs. The fix ensures that the AP adds AP MAC address in link-layer address in the client identifier field.</p> <p><b>Scenario:</b> APs sent DHCPv6 solicit message with "00:00:00:00:00:00" link-layer address instead of MAC address. This issue is observed in OAW-AP320 Series access points running AOS-W 8.5.0.1.</p>	AP-platform	OAW-AP320 Series access points	AOS-W 8.5.0.1
AOS-191195	—	<p><b>Symptom:</b> An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as <b>kernel panic: Fatal exception in interrupt</b>. The fix ensures that the AP works as expected.</p> <p><b>Scenario:</b> This issue was observed in OAW-AP225 access points running AOS-W 8.5.0.1 or later versions in a Mobility Master-Managed Device topology.</p>	AP-Wireless	OAW-AP225 access points	AOS-W 8.5.0.1
AOS-193990 AOS-194511	—	<p><b>Symptom:</b> The <b>mDNS</b> process in a managed device crashed unexpectedly. The fix ensures that the managed device works as expected.</p> <p><b>Scenario:</b> This issue was observed in managed devices running AOS-W 8.3.0.0 or later versions.</p>	AirGroup	All platforms	AOS-W 8.5.0.3

This chapter describes the known issues and limitations identified in AOS-W 8.5.0.3.




---

We have migrated to a new defect tracking tool. Some bugs are listed with the new bug ID, which is prefixed by AOS.

---

### Known Issues

The following known issues are observed in AOS-W 8.5.0.3.

**Table 7:** *Known Issues in AOS-W 8.5.0.3*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-125897 AOS-189036	151952	<b>Symptom:</b> When a managed device reboots, APs and clients boot without IP addresses and other fields. <b>Scenario:</b> This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions. <b>Workaround:</b> None.	Monitoring	All platforms	AOS-W 8.0.1.0
AOS-131325 AOS-146748	159222 179137	<b>Symptom:</b> The number of clients displayed in the active-standby IP field on the Mobility Master dashboard is incorrect. <b>Scenario:</b> This issue occurs due to a cluster failover causing race condition. This issue is observed in Mobility Masters running AOS-W 8.1.0.0 or later versions. <b>Workaround:</b> None.	Base OS Security	All platforms	AOS-W 8.1.0.0
AOS-144684 AOS-184346	176339	<b>Symptom:</b> A few managed devices are getting log files that contain incorrect or garbled ESSID and BSSID values. <b>Scenario:</b> This issue is observed in managed devices running AOS-W 8.2.1.0 or later versions. <b>Workaround:</b> None.	Station Management	All platforms	AOS-W 8.2.1.0

**Table 7: Known Issues in AOS-W 8.5.0.3**

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-145410 AOS-146962	177352 179430	<p><b>Symptom:</b> A managed device crashes and reboots with the following error message: <b>Atleast 2000 MB free flash is recommended to keep system stable. Please clean up your flash file.</b></p> <p><b>Scenario:</b> This issue occurs when a managed device receives IP packets larger than one segment. This issue is observed in managed devices running AOS-W 8.2.0.2 or later versions.</p> <p><b>Workaround:</b> None.</p>	switch-Platform	All platforms	AOS-W 8.2.0.2
AOS-145566	177559	<p><b>Symptom:</b> A Mobility Master is unable to forward the traffic that is sourced from an IP interface in the gateway.</p> <p><b>Scenario:</b> This issue occurs when netdestinations are used in the routing ACL rule. This issue is observed in Mobility Masters running AOS-W 8.0.1.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Policy-Based Routing	All platforms	AOS-W 8.0.1.0
AOS-151022 AOS-188417	185176	<p><b>Symptom:</b> The output of the <b>show datapath uplink</b> command displays incorrect session count.</p> <p><b>Scenario:</b> This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	switch-Datapath	All platforms	AOS-W 8.1.0.0
AOS-151355	185602	<p><b>Symptom:</b> A few managed devices are unable to pass traffic to the nexthop VPN concentrator (VPNC) using policy-based routing.</p> <p><b>Scenario:</b> This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Policy-Based Routing	All platforms	AOS-W 8.0.1.0
AOS-151541 AOS-185425	185851	<p><b>Symptom:</b> An idle SSH login session to a managed device does not time out.</p> <p><b>Scenario:</b> This issue is observed in managed devices running AOS-W 8.2.1.1.</p> <p><b>Workaround:</b> None.</p>	Base OS Security	All platforms	AOS-W 8.2.1.1

**Table 7: Known Issues in AOS-W 8.5.0.3**

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-152326 AOS-187297 AOS-187406 AOS-187549	186957	<b>Symptom:</b> The beacon displays the country code information intermittently for 5 GHz non-DFS channel. <b>Scenario:</b> This issue occurs when 802.11h is enabled in the radio profile. This issue is observed in OAW-AP510 Series access points running AOS-W 8.3.0.0 or later versions. <b>Workaround:</b> None.	AP-Wireless	OAW-AP510 Series access points	AOS-W 8.4.0.2
AOS-153185	188148	<b>Symptom:</b> The <b>Dashboard &gt; Security &gt; Active rogue &gt; Locate</b> option does not function in the WebUI. <b>Scenario:</b> This issue is observed in Mobility Masters running AOS-W 8.3.0.1 or later versions. <b>Workaround:</b> None.	WebUI	All platforms	AOS-W 8.3.0.1
AOS-155037	190571	<b>Symptom:</b> A OAW-RAP fails to boot up. <b>Scenario:</b> This issue occurs in a OAW-RAP with EST key type <b>X9.62/SECG curve</b> . This issue is observed in OAW-AP303H access points running AOS-W 8.3.0.3 or later versions. <b>Workaround:</b> None.	CPsec	OAW-AP303H access points	AOS-W 8.3.0.3
AOS-155801	191726	<b>Symptom:</b> SNMP walk performed from OmniVista 3600 Air Manager does not produce correct results. <b>Scenario:</b> This issue is observed in managed devices running AOS-W 8.3.0.3. <b>Workaround:</b> None.	SNMP	All platforms	AOS-W 8.3.0.3
AOS-156085 AOS-157704	192119 194393	<b>Symptom:</b> A few managed devices are unable to get the switch-IP address during boot up after an upgrade. <b>Scenario:</b> This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions. <b>Workaround:</b> None.	Configuration	All platforms	AOS-W 8.1.0.0
AOS-156742 AOS-156977	193031 193319	<b>Symptom:</b> After pushing a complete configuration via API, the user is unable to make any change to IP Probe configuration. <b>Scenario:</b> This issue is observed in managed devices running AOS-W 8.0.1.0. <b>Workaround:</b> None.	Configuration	All platforms	AOS-W 8.0.1.0

**Table 7: Known Issues in AOS-W 8.5.0.3**

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157008	193358	<p><b>Symptom:</b> The output of the <b>show ap bss table</b> command displays incorrect MTU value for a OAW-RAP.</p> <p><b>Scenario:</b> This issue occurs when the default value of the <b>rap-gre-mtu</b> parameter under the <b>ap system-profile &lt;profile_name&gt;</b> command is changed to a new value. This issue is observed in APs running AOS-W 8.2.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	AP-Platform	All platforms	AOS-W 8.3.0.0
AOS-157011	193362	<p><b>Symptom:</b> The output of <b>show datapath papi counters</b> command displays invalid tunnel endpoint information.</p> <p><b>Scenario:</b> This issue is observed in Mobility Masters running AOS-W 8.3.0.3.</p> <p><b>Workaround:</b> None.</p>	switch-Datapath	All platforms	AOS-W 8.3.0.3
AOS-157492	194064	<p><b>Symptom:</b> VRRP authentication fails in a managed device.</p> <p><b>Scenario:</b> This issue is observed in managed devices running AOS-W 8.2.1.0.</p> <p><b>Workaround:</b> None.</p>	VRRP	All platforms	AOS-W 8.2.1.0
AOS-157795	194516	<p><b>Symptom:</b> A few managed devices are unable to process two <b>APN usb-init</b> string using the <b>uplink cellular apn</b> command with Huawei E3372 modem.</p> <p><b>Scenario:</b> This issue is observed in managed devices running AOS-W 8.3.0.6.</p> <p><b>Workaround:</b> None.</p>	switch-Platform	All platforms	AOS-W 8.3.0.6
AOS-182073 AOS-183743	—	<p><b>Symptom:</b> An AP crashes and reboots unexpectedly. The log files lists the reason for the event as <b>Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT.</b></p> <p><b>Scenario:</b> This issue is observed in OAW-AP315 access points running AOS-W 8.3.0.5.</p> <p><b>Workaround:</b> None.</p>	IPsec	OAW-AP315 access points	AOS-W 8.3.0.5

**Table 7: Known Issues in AOS-W 8.5.0.3**

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-182847	—	<p><b>Symptom:</b> A few users are unable to copy the <b>WPA Passphrase</b> field and <b>High-throughput</b> profile to a new SSID profile in the <b>Configuration &gt; System &gt; Profiles &gt; Wireless LAN &gt; SSID &gt; &lt;SSID_Profile&gt;</b> option of the WebUI.</p> <p><b>Scenario:</b> This issue occurs when a new SSID profile is created from an existing SSID profile in the WebUI. This issue is observed in managed devices running AOS-W 8.4.0.0 in a Mobility Master-Managed Device topology.</p> <p><b>Workaround:</b> None.</p>	WebUI	All platforms	AOS-W 8.4.0.0
AOS-183998 AOS-183999	—	<p><b>Symptom:</b> A few users are unable to configure the PPPoE password when they provision a OAW-RAP in the <b>Configuration &gt; Access Points &gt; Remote APs</b> page of the WebUI.</p> <p><b>Scenario:</b> This issue occurs because the <b>Retype password</b> field for PPPoE is missing from the <b>Uplink</b> option in the provisioning page of the WebUI. This issue is observed in OAW-RAPs running AOS-W 8.3.0.6.</p> <p><b>Workaround:</b> None.</p>	WebUI	All platforms	AOS-W 8.3.0.6
AOS-184135	—	<p><b>Symptom:</b> A few users are unable to download applications from Google Play Store.</p> <p><b>Scenario:</b> This issue occurs when the YouTube application is blocked. This issue is observed in stand-alone switches running AOS-W 8.4.0.0.</p> <p><b>Workaround:</b> None.</p>	switch-Datapath	All platforms	AOS-W 8.4.0.0
AOS-184801	—	<p><b>Symptom:</b> A few managed devices crash and reboot unexpectedly. The log files list the reason for the event as <b>Datapath exception</b>.</p> <p><b>Scenario:</b> This issue is observed in managed devices running AOS-W 8.4.0.0.</p> <p><b>Workaround:</b> None.</p>	switch -Datapath	All platforms	AOS-W 8.4.0.0
AOS-184977 AOS-188242 AOS-188378	—	<p><b>Symptom:</b> The output of basic commands such as <b>show version</b>, <b>show clock</b>, and <b>show image version</b> are unable to display any information and the default gateway details are missing in a managed device.</p> <p><b>Scenario:</b> This issue occurs when the <b>/tmp</b> directory runs out of memory because of too many logs from the Policy Manager. This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Routing	All platforms	AOS-W 8.4.0.0

**Table 7: Known Issues in AOS-W 8.5.0.3**

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-185103	—	<p><b>Symptom:</b> The <b>Outstanding Requests</b> parameter value is incremented unexpectedly in the output of the <b>show aaa authentication-server radius statistics</b> command.</p> <p><b>Scenario:</b> This issue is observed in managed devices running AOS-W 8.5.0.0 or later versions with EAP fragmentation enabled.</p> <p><b>Workaround:</b> Restart the <b>802.1x</b> process by issuing the following two commands:</p> <ul style="list-style-type: none"> <li>■ <b>show processes   include dot1x</b></li> <li>■ <b>process restart dot1x1</b></li> </ul>	802.1x	All platforms	AOS-W 8.5.0.1
AOS-186133	—	<p><b>Symptom:</b> A few managed devices display abnormally high multicast traffic in <b>Performance Summary &gt; All Radios</b> monitoring page.</p> <p><b>Scenario:</b> This issue is observed in OAW-AP320 Series access points running AOS-W 8.3.0.6.</p> <p><b>Workaround:</b> None.</p>	AP-Wireless	OAW-AP320 Series access points	AOS-W 8.3.0.6
AOS-186303	—	<p><b>Symptom:</b> A few OAW-RAPs reboot unexpectedly. The log file lists the reason for the event as <b>kernel panic: Fatal exception on PC is at netdev_run_todo+0x290/0x2b4</b>.</p> <p><b>Scenario:</b> This issue is observed in OAW-AP305 access points running AOS-W 8.4.0.2 or later versions.</p> <p><b>Workaround:</b> None.</p>	RAP+BOAP	OAW-AP305 access points	AOS-W 8.4.0.2
AOS-186411	—	<p><b>Symptom:</b> Users are unable to remove a VLAN from port channel trunk.</p> <p><b>Scenario:</b> This issue is observed in Mobility Masters running AOS-W 8.3.0.0 or later versions.</p> <p><b>Workaround:</b> Execute the <b>switchport trunk allowed vlan 1-4094</b> command to add the allowed VLAN range (1-4094). Then, execute the <b>switchport trunk allowed vlan remove 259</b> command to remove the VLAN from the port channel trunk.</p>	Interface	All platforms	AOS-W 8.3.0.0
AOS-186860	—	<p><b>Symptom:</b> RADIUS authentication requests are sent in IP address of the managed device although they are configured to go through the loopback IP.</p> <p><b>Scenario:</b> This issue is observed in managed devices running AOS-W 8.4.0.1.</p> <p><b>Workaround:</b> None.</p>	IPsec	All platforms	AOS-W 8.4.0.1

**Table 7: Known Issues in AOS-W 8.5.0.3**

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-187114	—	<p><b>Symptom:</b> The <b>Pending Changes</b> window displays additional changes when the user configures a new policy rule under <b>Configuration &gt; Roles &amp; Policies &gt; Policies</b> window in the WebUI.</p> <p><b>Scenario:</b> This issue is observed when the user configures a new rule for an existing policy under the <b>Policies</b> window and clicks the <b>Submit</b> button. This issue is observed in Mobility Masters running AOS-W 8.3.0.4.</p> <p><b>Workaround:</b> None.</p>	WebUI	All platforms	AOS-W 8.3.0.4
AOS-187395 AOS-188564	—	<p><b>Symptom:</b> The AAA test to the external server fails in the <b>Diagnostics &gt; Tools &gt; AAA Server Test</b> page of the WebUI.</p> <p><b>Scenario:</b> This issue occurs when the user enters the <b>"</b>, <b>%</b>, and <b>#</b> special characters in the <b>Password</b> field and clicks the <b>Test</b> option. As a result, the WebUI displays the <b>Authentication</b> field as <b>failed</b> and <b>Processing time (ms)</b> field as <b>N/A</b>. This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	WebUI	All platforms	AOS-W 8.4.0.2
AOS-187422 AOS-189258	—	<p><b>Symptom:</b> The output of <b>show log all</b> and <b>show audit-trail</b> commands displays the unencrypted password entered for non-profile commands such as <b>aaa test-server</b> command.</p> <p><b>Scenario:</b> This issue is observed in a Mobility Master Virtual Appliance running AOS-W 8.3.0.5.</p> <p><b>Workaround:</b> None.</p>	Configuration	All platforms	AOS-W 8.3.0.5
AOS-187479 AOS-188428	—	<p><b>Symptom:</b> The authentication server configuration details are not forwarded from the primary Mobility Master to the secondary Mobility Master in Layer-3 redundancy configuration.</p> <p><b>Scenario:</b> This issue is observed in a Mobility Master Virtual Appliance running AOS-W 8.4.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Configuration	All platforms	AOS-W 8.4.0.2
AOS-187510	—	<p><b>Symptom:</b> A managed device crashes and reboots unexpectedly.</p> <p><b>Scenario:</b> This issue occurs when the 802.1X processes crash after a cluster live upgrade on the managed device. This issue is observed in managed devices running AOS-W 8.4.0.2 or later versions in a cluster setup.</p> <p><b>Workaround:</b> None.</p>	802.1X	All platforms	AOS-W 8.4.0.2

**Table 7: Known Issues in AOS-W 8.5.0.3**

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-187820	—	<p><b>Symptom:</b> The output of the <b>show cpuload per-cpu</b> command displays the same CPU load statistics for each processor.</p> <p><b>Scenario:</b> This issue occurs after reboot of the switch. This issue is observed in managed devices running AOS-W 8.4.0.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	switch-Platform	All platforms	AOS-W 8.4.0.0
AOS-187911	—	<p><b>Symptom:</b> The <b>Wireless Clients</b> section of the <b>Dashboard &gt; Overview</b> page in the WebUI displays incorrect client usage values.</p> <p><b>Scenario:</b> This issue is observed in Mobility Masters running AOS-W 8.4.0.0 or later versions.</p> <p><b>Workaround:</b> Add a tooltip over the usage tab to mention that the current client usage value accounts for the last 15 min.</p>	WebUI	All platforms	AOS-W 8.4.0.0
AOS-188199	—	<p><b>Symptom:</b> A few clients are unable to connect to a switch in Alcatel-Lucent Central??? because the ClearPass Policy Manager rejects the client authentication request.</p> <p><b>Scenario:</b> This issue occurs when the branch gateway sends NAD-IP address or NAS-IP address as public IP address. This issue is observed in OAW-4008 switches running AOS-W 8.4.0.0.</p> <p><b>Workaround:</b> None.</p>	Base OS Security	OAW-4008 controllers	AOS-W 8.4.0.0
AOS-188467	—	<p><b>Symptom:</b> The AMON messages from a peer cluster display <b>wrong value for cl_cluster_incompatible_reason</b>.</p> <p><b>Scenario:</b> This issue occurs when the incompatible reason is not reset after an incompatibility with a peer cluster member is resolved and the cluster is re-formed. This issue is observed in managed devices running AOS-W 8.3.0.6 in a cluster topology.</p> <p><b>Workaround:</b> None.</p>	Cluster Manager	All platforms	AOS-W 8.3.0.6
AOS-188470	—	<p><b>Symptom:</b> PPPoE does not work when a OAW-RAP is provisioned using ZTP and the <b>Either ping is disabled on AP's uplink router or there are issues with AP's uplink connectivity</b> error is displayed.</p> <p><b>Scenario:</b> This issue is observed in OAW-AP203R access points running AOS-W 8.2.1.1 or later versions.</p> <p><b>Workaround:</b> None.</p>	RAP+BOAP	OAW-AP203R access points	AOS-W 8.2.1.1

**Table 7: Known Issues in AOS-W 8.5.0.3**

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-188478	—	<p><b>Symptom:</b> The OAW-RAP whitelist file does not contain the first MAC address entry.</p> <p><b>Scenario:</b> This issue occurs when the user runs the <b>show whitelist-db rap export-css &lt;filename&gt;</b> command to export the OAW-RAP whitelist file to the switch directory. This issue is observed in standalone switches running AOS-W 8.3.0.5 or later versions.</p> <p><b>Workaround:</b> None.</p>	Local Database	All platforms	AOS-W 8.3.0.5
AOS-188485	—	<p><b>Symptom:</b> The <code>&lt;ofald 237504&gt; &lt;ERRS&gt;  AP 32438@172.16.4.151 ofald   sdn  ERRS ofald_datapath_msg_rcv_cb:274 Invalid message type 126</code> error message is displayed every second in APs.</p> <p><b>Scenario:</b> This issue is observed in APs running AOS-W 8.4.0.0-FIPS in a Mobility Master-Managed Device topology.</p> <p><b>Workaround:</b> None.</p>	SDN	All platforms	AOS-W 8.4.0.0
AOS-189194	—	<p><b>Symptom:</b> The 5 GHz and 2.4 GHz antenna values are swapped after AP provisioning rules configuration is committed in the <b>Configuration &gt; Access Points &gt; Provisioning Rules</b> page of the WebUI.</p> <p><b>Scenario:</b> This issue occurs when the user selects the <b>Set Antenna Gain for Dual Band mode</b> option from the <b>Actions</b> drop-down list in the <b>Configuration &gt; Access Points &gt; Provisioning Rules</b> page, and enters the <b>5 GHz</b> and <b>2.4 GHz</b> field values in the WebUI. This issue is observed in Mobility Master Virtual Appliances running AOS-W 8.4.0.3 or later versions.</p> <p><b>Workaround:</b> None.</p>	WebUI	All platforms	AOS-W 8.5.0.0

**Table 7:** Known Issues in AOS-W 8.5.0.3

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-189471	—	<p><b>Symptom:</b> A few clients are unable to connect to APs that are configured with LACP and have allowed band of 5 GHz.</p> <p><b>Scenario:</b> This issue is observed in OAW-AP335 access points running AOS-W 8.5.0.0.</p> <p><b>Workaround:</b> None.</p>	AP Datapath	OAW-AP335 access points	AOS-W 8.5.0.0
AOS-189721	—	<p><b>Symptom:</b> The <b>Datapath</b> process crashes in a switch. The log files list the reason for the event as <b>Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)</b>.</p> <p><b>Scenario:</b> This issue is observed in OAW-4550 switches running AOS-W 8.4.0.2 or later versions.</p> <p><b>Workaround:</b> None.</p>	switch-Datapath	OAW-4550 switches	AOS-W 8.4.0.2
AOS-190071 AOS-190372	—	<p><b>Symptom:</b> A few users are unable to access the websites when WebCC is enabled on the user role.</p> <p><b>Scenario:</b> This issue occurs in a Per User Tunnel Node (PUTN) setup when the VLAN of user role is in trunk mode. This issue is observed in OAW-4005 switches running AOS-W 8.4.0.0.</p> <p><b>Workaround:</b></p> <ul style="list-style-type: none"> <li>■ Remove web category from the ACL rules and apply <b>any any any permit</b> policy.</li> <li>■ Disable WebCC on the user role.</li> <li>■ Change the VLAN of user role from trunk mode to access mode.</li> </ul>	WebCC	OAW-4005 switches	AOS-W 8.4.0.0

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



CAUTION

---

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

---

Topics in this chapter include:

- [Migrating from AOS-W 6.x to AOS-W 8.x on page 40](#)
- [Important Points to Remember and Best Practices on page 41](#)
- [Memory Requirements on page 41](#)
- [Backing up Critical Data on page 42](#)
- [Upgrading on page 44](#)
- [Downgrading on page 46](#)
- [Before You Call Technical Support on page 48](#)

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

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

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

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



NOTE

---

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

---

## Important Points to Remember and Best Practices

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

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any other changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of your network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** section of the WebUI, or by executing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W is currently on the managed device?
  - Are all managed devices running the same version of software?
  - Which services are used on the managed device (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If you encounter any issue 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, if required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses that you might require. For a detailed description of these new license modules, see the “Software Licenses” chapter in the *AOS-W 8.x.0.0 User Guide*.

## Memory Requirements

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

- Confirm that there is at least 100 MB of free memory available for an upgrade using the WebUI or CLI. Execute the **show memory** command to identify the amount of free memory available using the CLI. Do not proceed unless 100 MB of free memory is available. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Confirm that there is at least 150 MB of flash space available for an upgrade using the WebUI or CLI. Using the CLI, execute the **show storage** command to identify the amount of flash space available.



---

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

---

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

- **Crash Data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in [Backing up Critical Data on page 42](#) to copy the **crash.tar** file to an external server, and then execute the **tar clean crash** command to delete the file from the managed device.
- **Flash Backups:** Use the procedures described in [Backing up Critical Data on page 42](#) to back up the flash directory to a file named **flash.tar.gz**, and then execute the **tar clean flash** command to delete the file from the managed device.
- **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in [Backing up Critical Data on page 42](#) to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the managed device.

Use the following procedure to delete files and free up memory space:

### In the WebUI

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

### In the CLI

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

## Backing up Critical Data

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

- Configuration data
- WMS database
- Local user database
- Licensing database
- Custom captive portal pages
- x.509 certificates
- Logs

- Flashbackup

## Backing up and Restoring Compact Flash in the WebUI

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

1. In the Mobility Master node hierarchy, navigate to the **Maintenance > Configuration Management > Backup** page.
2. Click **Create Backup** to backup the contents of the compact flash file system to the **flashbackup.tar.gz file**.
3. Click **Copy Backup** to copy the file to an external server.  
You can copy the backup file from the external server to the compact flash file system using the file utility in the **Diagnostics > Technical Support > Copy Files** page.
4. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > Configuration Management > Restore** page and click **Restore**.

## Backing up and Restoring Compact Flash in the CLI

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

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

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

2. Execute the **backup** command to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.

```
(host) # backup flash
Please wait while we take the flash backup.....
File flashbackup.tar.gz created successfully on flash.
Please copy it out of the controller and delete it when done.
```

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

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

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

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

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

```
(host) # restore flash
Please wait while we restore the flash backup.....
Flash restored successfully.
Please reload (reboot) the controller for the new files to take effect.
```

# Upgrading

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

## In the WebUI



CAUTION

---

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash space available for an upgrade using the WebUI. For details, see [Memory Requirements on page 41](#).

---



NOTE

---

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

---

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

1. Download AOS-W from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Validate the SHA hash for a software image:
  - a. Download the **Alcatel.sha256** file from the download directory.
  - b. To verify the image, load the image onto a Linux system and execute the **sha256sum <filename>** command or use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
  - c. Verify that the output produced by this command matches the hash value found on the support site.



NOTE

---

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

---

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



NOTE

---

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

---

9. Select the **Save Current Configuration** option.

10. Click **Upgrade**.

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

11. Click **OK**.

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

12. When the reboot process is complete, log in to the WebUI and navigate to the **Dashboard > WLANs** page to verify the upgrade.

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

1. Log in to the WebUI to verify all your switches are up after the reboot.
2. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients.
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 [Memory Requirements on page 41](#) for information on creating a backup. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses.

## In the CLI



---

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash space available for an upgrade using the CLI. For details, see [Memory Requirements on page 41](#).

---

## Upgrading From a Recent Version of AOS-W

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

1. Download AOS-W from the customer support site.
2. Open an SSH session on your master (and local) switches.
3. Execute the **ping** command to verify the network connection from the target switch to the SCP/FTP/TFTP server.

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

or

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

or

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

4. Execute the **show image version** command to check if the AOS-W images are loaded on the switch's flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

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

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

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

or

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

or

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

or

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

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

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

7. Reboot the switch.

```
(host)# reload
```

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

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

When the 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 42](#) for information on creating a backup.

## Downgrading

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

### Before You Begin

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

1. Back up your switch. For details, see [Backing up Critical Data on page 42](#).
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W configuration file.
4. Set the switch to boot from the system partition that contains the previously running AOS-W image.

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

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

## Downgrading Using the WebUI

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

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the switch by navigating to the **Diagnostics > Technical Support > Copy Files** page.
  - a. For **Select source file** option, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.
  - b. For **Select destination file** option, enter a file name (other than default.cfg) for Flash File System.
2. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Software Management > Upgrade** page. If there is no previous software image stored on your system partition, load it into the backup system partition by performing the following steps:



---

You cannot load a new image into the active system partition

---

- a. Enter the FTP/TFTP server address and image file name.
  - b. Select the backup system partition.
  - c. Click **Upgrade**.
3. Navigate to the **Maintenance > Software Management > Boot Parameters** page.
  - a. Select the system partition that contains the pre-upgrade image file as the boot partition.
  - b. Click **Apply**.
4. Navigate to the **Maintenance > Software Management > Reboot** page. Select **Save configuration before reboot** option and click **Reboot**. The switch reboots after the countdown period.
5. When the boot process is complete, verify that the switch is using the correct software by navigating to the **Maintenance > Software Management > About** page.

## Downgrading Using the CLI

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

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

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

or

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

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

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

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

```
#show image version
```

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

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

5. Reboot the switch.

```
(host) # reload
```

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

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

## Before You Call Technical Support

Before you call Technical Support, follow these steps:

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

7. Provide the date and time (if possible) of when the problem first occurred. If the problem is reproducible, list the exact steps taken to re-create the problem.
8. Provide any wired or wireless sniffer traces taken during the time of the problem.
9. Provide the Alcatel-Lucent device site access information, if possible.

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+.

---

**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.

**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.

**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.

**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.

**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.

**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.

**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.

**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.

**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: AName.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. GARP 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 policies configured by a network administrator.

**PDU**

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

**PEAP**

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

**PEF**

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

---

**PEFNG**

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

**PEFV**

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

**PFS**

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

**PHB**

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

**PIM**

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

**PIN**

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

**PKCS#n**

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

**PKI**

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

**PLMN**

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

**PMK**

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

---

**PoE**

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

**PoE+**

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

**POST**

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

**PPP**

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

**PPPoE**

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

**PPTP**

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

**private key**

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

**PRNG**

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

**PSK**

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

**PSU**

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

---

**public key**

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

**PVST**

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

**PVST+**

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

**QoS**

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

**RA**

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

**Radar**

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

**RADIUS**

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

**RAM**

Random Access Memory.

**RAPIDS**

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

**RARP**

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

**Regex**

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

---

**Registration Authority**

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

**Remote AP**

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

**REST**

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

**RF**

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

**RFC**

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

**RFID**

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

**RIP**

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

**RJ45**

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

**RMA**

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

---

**RMON**

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

**RoW**

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

**RSA**

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

**RSSI**

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

**RSTP**

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

**RTCP**

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

**RTLS**

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

**RTP**

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

**RTS**

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

**RTSP**

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

**RVI**

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

---

**RW**

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

**SA**

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

**SAML**

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

**SCEP**

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

**SCP**

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

**SCSI**

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

**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.

**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.

---

**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.

**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.

**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.

---

**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.

**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.

**UAM**

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

**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.

**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.

---

**walled garden**

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

**WAN**

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

**WASP**

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

**WAX**

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

**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.

**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.

**WIDS**

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

**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.