AOS-W 8.2.2.5

Alcatel·Lucent
Enterprise

Release Notes

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Use the following links to navigate to the corresponding topics:

- New Features and Enhancements on page 8 describes the new features and enhancements introduced in this release.
- Supported Platforms on page 11 describes the hardware platforms supported in this release.
- Regulatory Updates on page 15 lists the regulatory updates in this release.
- Resolved Issues on page 16 lists the issues resolved in this release.
- Known Issues and Limitations on page 18 lists the issues identified in this release.
- Upgrade Procedure on page 43 describes the procedures for upgrading your WLAN network to the latest AOS-W version.
- Glossary of Terms on page 53 lists the acronyms and abbreviations.

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

Related Documents

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

- *AOS-W Release Notes*
- *AOS-W Getting Started Guide*
- *AOS-W User Guide*
- *AOS-W CLI Reference Guide*
- *AOS-W Migration Guide*
- *AOS-W API Guide*
- *AOS-W 8.x Syslog Message Guide*
- *Alcatel-Lucent Mobility Master Licensing Guide*
- *Alcatel-Lucent Mobility Master and VMC Installation Guide*
- *Alcatel-Lucent Wireless Access Point Installation Guide*

Supported Browsers

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

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

Contacting Support

Table 2: *Contact Information*

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

This chapter describes the features and/or enhancements introduced in AOS-W 8.2.2.5.

Base OS Security

VIA

The maximum number of entries for tunneled network is 32 and the maximum number of entries for white-listing is 16.

CLI Enhancements

Show user-table

If the **show user-table** command is executed from the **[mynode]** or **[mm]** prompts of the Mobility Master CLI, the following alert message is displayed:

This command is not applicable on master switch

IPv6 Support

IPv6 Firewall Code Enhancements

The IPv6 firewall code has been updated to include TCP sequence number enforcement and the associated statistics.

TCP Syn Threshold Limit

Starting from AOS-W 8.2.2.5, you can define the TCP syn connection rate (per 30 seconds) for IPv6 traffic. When the TCP syn connection rate exceeds the defined rate, new TCP syn connections are dropped. New TCP syn connections are allowed when the number of open TCP syn connections drop below the defined limit.

To enable the TCP syn connection for IPv6 traffic, execute the following commands:

```
(host) [mynode] (config) # ipv6 firewall
(host) [mynode] (config-submode)# enforce-tcp-sequence
```

To define the number of TCP syn connections, execute the following command:

```
(host) [mynode] (config-submode) # attack-rate tcp-syn <1-16384>
```

To view the number of dropped packets of TCP syn connection, execute the following command:

```
(host) [mynode] (config-submode) # show datapath frame
```

```
-------------------------------------------------------
SUM/
CPU    Addr    Description Value

-------------------------------------------------------
       [000]   Allocated Frames 4311
       [001]   Max Allocated Frames 5513
       [003]   Unknown Unicast 481
       [010]   IP Reassembled Datagrams 8
       [014]   IP Reassembly Failures 2
       [038]   Flood Frames 125
       [049]   Drop due to max half syns 5831

-------------------------------------------------------

G      [000]   BPDUs Received 35

-------------------------------------------------------
```

Management Access

FIPS X509 Certificate Enhancements

The following are the enhancements for X509 server certificates in the FIPS mode:

- When OCSP is selected for certificate verification and the certificate in OCSP response does not have the OCSP signing purpose bit set in extended key usage, the OCSP response validation fails.
- When CRL is selected and the CA certificate to sign a CRL is not set to cRLsign key usage bit, the CRL validation fails.
- When a signed public key that is generated using CSR is imported into a managed device , all the associated CAs and sub-CAs must be available in the managed device's certificate manager store and imported individually. The import fails if the CAs and sub-CAs are bundled.

Web Server

Supported SSL/TLS Protocol in FIPS Mode of Operation

Starting from AOS-W 8.2.2.5, the SSL or TLS protocol of the FIPS version supports only TLSv1.2 for secure communication with the web server. Use the **show web-server profile** command to display the configured TLS version. The output on execution of this command is as follows:

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

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

WebUI

WebUI Support for Called Station ID in RADIUS Server Profile

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

This chapter describes the hardware and virtual platforms supported in this AOS-W release.

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 8.2.2.5*

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 8.2.2.5*

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
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 the AOS-W release.

Table 5: *Supported AP Platforms in AOS-W 8.2.2.5*

AP Family	AP Model
OAW-AP90 Series	OAW-AP92, OAW-AP93
OAW-AP93H Series	OAW-AP93H
OAW-AP100 Series	OAW-AP104, OAW-AP105
OAW-AP103 Series	OAW-AP103
OAW-AP103H Series	OAW-AP103H
OAW-AP110 Series	OAW-AP114, OAW-AP115
OAW-AP130 Series	OAW-AP134, OAW-AP135
OAW-AP170 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

Table 5: *Supported AP Platforms in AOS-W 8.2.2.5*

AP Family	AP Model
OAW-AP207 Series	OAW-AP207
OAW-AP203R Series	OAW-AP203R, OAW-AP203RP
OAW-AP210 Series	OAW-AP214, OAW-AP215
OAW-AP220 Series	OAW-AP224, OAW-AP225
OAW-AP228 Series	OAW-AP228
OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277
OAW-AP300 Series	OAW-AP304, OAW-AP305
OAW-AP303H Series	OAW-AP303H
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP320 Series	OAW-APAP-324, OAW-AP325
OAW-AP330 Series	OAW-AP334, OAW-AP335
OAW-AP360 Series	OAW-AP365, OAW-AP367

Table 5: *Supported AP Platforms in AOS-W 8.2.2.5*

AP Family	AP Model
OAW-RAP 3 Series	OAW-RAP3WN, OAW-RAP3WNP
OAW-RAP100 Series	OAW-RAP108, OAW-RAP109
OAW-RAP 155 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 support.arubanetworks.com.

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

- DRT-1.0_69842

This chapter describes the issues resolved in this AOS-W release.

Since we have migrated to a new defect tracking tool, we will list both, the old and the new bug ids for tracking purposes.

Resolved Issues

The following resolved issues were observed in AOS-W 8.2.2.5.

Table 6: *Resolved Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-150202	184070	**Symptom:** VIA clients were unable to connect to Suite-B (AES-GCM) cryptographic algorithms with ECDSA certificates enabled on a managed device. The fix ensures that the VIA clients are able to connect to the managed device. **Scenario:** This issue occurred due to improper interaction of advanced cryptographic license with IKE module. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	IPsec	All platforms	AOS-W 8.2.0.0
AOS-158180 AOS-158565 AOS-182719 AOS-183629 AOS-184955 AOS-185312 AOS-185342 AOS-185428	195080 195592	**Symptom:** The licenses within the AP licensing pool were consumed every time the mesh point was rebooted or was disconnected from its parent. The fix ensures that the license count does not get exhausted. **Scenario:** This issue was observed in APs in mesh portal and mesh point mode running AOS-W 8.2.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.2.0.0
AOS-183640 AOS-184351 AOS-184539 AOS-184540		**Symptom:** A leak in the **MDNS** process was observed when the **show airgroup ap** or **tar logs** command was executed. This issue is resolved by fixing the memory leak in the **MDNS** process. **Scenario:** This issue occurred because of a memory leak in the **MDNS** process and this leak was significantly high in a large network with over 1000 APs. This issue was observed in Mobility Master Virtual Appliance running AOS-W 8.3.0.0 or later versions.	AirGroup	All platforms	AOS-W 8.3.0.0

This chapter describes the known issues and limitations identified in AOS-W 8.2.2.5.

Since we have migrated to a new defect tracking tool, we will list both, the old and the new bug ids for tracking purposes.

Known Issues

The following known issues are observed in AOS-W 8.2.2.5.

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-123169	148402	**Symptom:** The **mDNS** process crashes and reboots unexpectedly on a managed device. The log files lists the reason for the event as **Reboot Cause: User reboot (Intent:cause:register 78:86:50:2)**. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.1.0 in a Mobility Master-Managed Device topology. **Workaround:** None.	AirGroup	All platforms	AOS-W 8.0.1.0
AOS-131860	159921	**Symptom:** The **Dashboard > WAN** page of the Mobility Master displays the WAN uplink status incorrectly. **Scenario:** This issue is observed in managed devices running AOS-W 8.1.0.0 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.1.0.0
AOS-131862	159923	**Symptom:** The **Configuration > Services > WAN** page of the managed device does not have the **Policy-Based Routing** and **NextHop Configuration** accordions in the WebUI. **Scenario:** This issue is observed in managed devices running AOS-W 8.1.0.0. **Workaround:** None.	WebUI	All platforms	AOS-W 8.1.0.0

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-132207	160389	**Symptom:** The **Dashboard > WAN> <node>** page of the Mobility Master displays only 5 uplinks. **Scenario:** This issue is observed in a Branch office setup running AOS-W 8.1.0.0 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.1.0.0
AOS-132332	160551	**Symptom:** An AP keeps declaring a stale IP as the master and fails to come up even after purging the stale master IP from the AP boot environment variables. **Scenario:** This issue occurs because the AP restores all the cleared variables due to a backup restore feature. This issue is observed in APs running AOS-W 8.1.0.0 or later versions. **Workaround:** Run the **bootenv_backup.sh** script to clear the saved record.	AP-Platform	All platforms	AOS-W 8.1.0.0
AOS-133998	162623	**Symptom:** The output of the **show ap arm history ap-name <ap-name>** command does not display the radar detection event for an AP. **Scenario:** This issue is observed in OAW-AP203H access points running AOS-W 8.2.0.0. **Workaround:** None.	ARM	OAW-AP203H access points	AOS-W 8.2.0.0
AOS-135738 AOS-154405	164796 189740	**Symptom:** An AP does not disable one of its ethernet ports when the power supply, POE-AF is applied. **Scenario:** This issue is observed in OAW-AP220 Series, OAW-AP320 Series, OAW-AP330 Series, and OAW-AP340 Series access points running AOS-W 8.1.0.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 8.1.0.0
AOS-136038 AOS-136045	165161 165168	**Symptom:** The **profmgr** process in a managed device crashes unexpectedly. **Scenario:** This issue occurs when **PAP** is enabled in **VIA** authentication profile. This issue is observed in managed devices running AOS-W 8.1.0.2 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.1.0.2

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-137345 AOS-156729	166773 193017	**Symptom:** The **profmgr** process in a Mobility Master crashes unexpectedly. **Scenario:** This issue occurs when the device configuration settings are replaced with new configuration settings. This issue is observed in Mobility Masters running AOS-W 8.0.1.0 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.0.1.0
AOS-137352 AOS-140496	166780 170911	**Symptom:** The traffic from a Facebook session is not getting denied at the datapath level of the managed device. **Scenario:** This issue is observed in managed devices running AOS-W 8.1.0.3 or later versions in a cluster setup. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 8.1.0.3
AOS-137877 AOS-139950	167410 170131	**Symptom:** A managed device does not display equal distribution of AP load in the WebUI and the CLI output. **Scenario:** This issue occurs in a cluster topology with load balancing enabled. This issue is observed in managed devices running AOS-W 8.3.0.0. **Workaround:** None.	Cluster-Manager	All platforms	AOS-W 8.3.0.0
AOS-138015	167572	**Symptom:** A user role that is configured from the CLI and WebUI in uppercase is converted to lowercase in a managed device. **Scenario:** This issue is observed in managed devices running AOS-W 8.1.0.1 or later versions. **Workaround:** None.	Role	All platforms	AOS-W 8.1.0.1
AOS-138468	168180	**Symptom:** The **profmgr** process in a managed device crashes when a single instance default profile is modified in the disaster recovery mode. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.0.1.0
AOS-138677	168457	**Symptom:** The license count in **Mobility Master > Licenses** page in the WebUI does not reflect the ACR license usage. **Scenario:** This issue occurs when the license count is not communicated to the applications running on Standby Mobility Master. This issue is observed in Mobility Masters running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	Licensing	All platforms	AOS-W 8.2.0.0

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-140806 AOS-157745	171339 194445	**Symptom:** Managed Devices reboot with the initial device configuration even though the updated configuration changes are available in the Mobility Master. **Scenario:** This issue is observed in managed devices running AOS-W 8.1.0.4 or later versions in a Mobility Master-Managed Device topology in a multi-version deployment. **Workaround:** None.	Configuration	All platforms	AOS-W 8.1.0.4
AOS-140825 AOS-145318	171379 177221	**Symptom:** An AP reported multiple crashes of the **SAPD** process. **Scenario:** This issue occurs when the wireless driver sends packets with invalid length to the AP. This issue is observed in OAW-AP325 access points running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	Air Management-IDS	OAW-AP325 access points	AOS-W 8.0.0.0
AOS-140985 AOS-141330	171593 172044	**Symptom:** An AP uses an incorrect channel, bandwidth, or EIRP that does not match the configuration in **rf dot11a-radio-profile**, **rf dot11g-radio-profile** or **ap regulatory-domain-profile** commands. Also, the AP goes into APM mode and is unable to recover back to AP mode. **Scenario:** This issue occurs due to: ■ message loss between AP and managed device. ■ unavailability of channel in a configured bandwidth. This issue is observed in APs running AOS-W 8.2.0.0. **Workaround:** ■ Reboot the AP. ■ Execute the **airmatch ap freeze** command to manually change the channel.	AirMatch	All platforms	AOS-W 8.2.0.0
AOS-141001	171611	**Symptom:** A crypto map is incorrectly picked during IKE and IPsec negotiation on a managed device if the **vpn-peer peer-mac** command is configured along with **masterip** and **vpnip** commands pointing to the same MAC address. **Scenario:** This issue is observed in managed devices running AOS-W 8.1.0.4 or later versions. **Workaround:** Execute the **no vpn-peer peer-mac** command on the managed device.	IPsec	All platforms	AOS-W 8.1.0.4

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-141177 AOS-145205	171840 177067	**Symptom:** A downloaded role becomes invalid in a Switch. **Scenario:** This issue occurs when an access-list name is configured using uppercase characters. This issue is observed in managed devices running AOS-W 8.2.0.0. **Workaround:** None.	Role/VLAN Derivation	All platforms	AOS-W 8.2.0.0
AOS-141408	172137	**Symptom:** Users are unable to delete a routing ACL from the managed device even though it is not referenced by VLAN interface or tunnels. **Scenario:** This issue is observed in managed devices running AOS-W 8.1.0.0. **Workaround:** None.	Policy-Based Routing	All platforms	AOS-W 8.1.0.0
AOS-141465	172217	**Symptom:** Write memory does not show the configurations committed. **Scenario:** This issue occurs when a user configures ACLs, VLANs, and interface configuration and issues the **write memory** command. This issue is observed in managed devices running AOS-W 8.2.0.1 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.2.0.1
AOS-141708	172534	**Symptom:** WEP clients are unable to pass traffic after a cluster failover and switchover to standby mode. **Scenario:** This issue occurs when the clients are connected to static or dynamic WEP-enabled WLAN in a cluster deployment. This issue is observed in a cluster set up running AOS-W 8.1.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.1.0.0
AOS-141831	172680	**Symptom:** The MIB files and IDS logs have references to an unnecessary URL. **Scenario:** This issue is observed in MIB files and IDS logs of managed devices running AOS-W 8.2.0.0. **Workaround:** None.	SNMP	All platforms	AOS-W 8.2.0.0
AOS-141973 AOS-146393	172857 178662	**Symptom:** The **BOCMGR** process in a Mobility Master crashes unexpectedly. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.2.0.2 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 8.2.0.2

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-142535	173554	**Symptom:** The IDS logs and SNMP traps include WVE ID hyperlinks that are invalid. **Scenario:** This issue is not limited to any specific Switch model or AOS-W release version. **Workaround:** None.	Air Management-IDS	All platforms	AOS-W 8.0.0.0
AOS-142546	173570	**Symptom:** The text banner is not displayed at the login prompt of the WebUI. **Scenario:** This issue is observed in a Mobility Master Virtual Appliance running AOS-W 8.2.0.1. **Workaround:** None.	WebUI	All platforms	AOS-W 8.2.0.1
AOS-142968 AOS-143134 AOS-144431 AOS-145646 AOS-146413 AOS-148222 AOS-152443 AOS-158329 AOS-177195 AOS-177687 AOS-178219	174100 174320 175992 177665 178689 181469 187116 195288 173924 176293 179464	**Symptom:** An AP does not support fast recovery. **Scenario:** This issue is observed in OAW-AP303H, OAW-AP305, OAW-AP315, OAW-AP325, and OAW-AP335 access points running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP303H, OAW-AP305, OAW-AP315, OAW-AP325, and OAW-AP335 access points	AOS-W 8.2.0.0
AOS-143095 AOS-154432	174270 189772	**Symptom:** Managed Devices display a large number of **PAPI_open_udp_socket** error messages when the **show log all | include PAPI_open** command is executed. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions. **Workaround:** None.	Controller-Platform	All platforms	AOS-W 8.0.1.0

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-143484	174788	**Symptom:** A Mobility Master incorrectly allows users to execute the **aaa user delete** command from the **/mm** or **/mm/mynode** levels. However, the command is not effective because it is applicable only at the managed device level **(/md/<device>)**. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.0.0.0 or later versions. **Workaround:** Execute the **aaa user delete** command from a managed device.	Base OS Security	All platforms	AOS-W 8.0.0.0
AOS-143747	175138	**Symptom:** The **Configurations > Services > Guest provisioning** page appears blank and non-editable. **Scenario:** This issue occurs when a user enters the **&** character in the email fields and submits the changes. This issue is observed in managed devices running AOS-W 8.2.0.2 or later versions. **Workaround:** None.	Guest Provisioning	All platforms	AOS-W 8.2.0.2
AOS-143898 AOS-158367	175333 195340	**Symptom:** A client is unable to send or receive traffic. **Scenario:** This issue is observed in OAW-AP325 access points running AOS-W 8.2.2.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP325 access points	AOS-W 8.2.2.0
AOS-144289 AOS-146918	175829 179365	**Symptom:** A managed device fails to establish an IPsec tunnel with a Mobility Master when the managed device resolves master **FQDN** to an incorrect IP address. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.0.1.0 or later versions. **Workaround:** None.	IPsec	All platforms	AOS-W 8.0.1.0
AOS-144329 AOS-152686	175881 187479	**Symptom:** The **datapath** process in a managed device crashes unexpectedly. **Scenario:** This issue occurs when the AP toggles between dual-band mode and dual 5 GHz mode. This issue is observed in managed devices running AOS-W 8.3.0.0. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 8.3.0.0

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-144456	176029	**Symptom:** The CLI help text for the **tunnel** parameter in the **via connection-profile** command does not show the maximum number of VIA tunneled networks that can be configured. **Scenario:** Without this help text, user is unable to know the maximum number of allowed VIA tunneled network configurations. This issue is not limited to any specific platform or AOS-W version. **Workaround:** None.	Configuration	All platforms	AOS-W 8.2.0.0
AOS-144500 AOS-145987	176087 178109	**Symptom:** Users are unable to configure netdestination or netservice using WebUI. **Scenario:** This issue is observed in Mobility Masters or managed devices running AOS-W 8.4.0.0. **Workaround:** None.	WebUI	All platforms	AOS-W 8.4.0.0
AOS-144522	176118	**Symptom:** A user is unable to save the changes that are made in the **Guest Email** tab under **Mobility Master>Configuration** > **Services** > **Guest Provisioning** > **Guest Email** page of the WebUI. **Scenario:** This issue occurs when a user edits and saves the changes that are already configured in the WebUI. This issue is observed in Mobility Masters running AOS-W 8.2.0.2 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.2.0.2
AOS-144676 AOS-145471	176330 177428	**Symptom:** The **Diagnostics > Technical Support > Copy Files** page of the WebUI displays a success message even though the TFTP file transfer fails. **Scenario:** This issue occurs when a user copies a file using TFTP. This issue is observed in Mobility Masters running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.2.0.0
AOS-145098	176930	**Symptom:** An AirGroup server that is connected as a Per User Tunneled Node client is not showing up as an AirGroup server on the Mobility Master. **Scenario:** This issue occurs when a tunneled_node GSM channel is used for user subscription. This issue is observed in managed devices running AOS-W 8.2.1.0 or later versions. **Workaround:** None.	SDN-Platform	All platforms	AOS-W 8.2.1.0

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-145102 AOS-145544	176935 177529	**Symptom:** The **profmgr** process in a managed device crashes when the user attempts to delete the expired evaluation licenses from the **Configuration >System >Licensing** page of the WebUI. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.3.0.0
AOS-145241 AOS-152388	177113 187050	**Symptom:** A configuration failure occurs when the ACL configuration is removed from a managed device. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.2.0.0
AOS-145303	177204	**Symptom:** The following streaming API and the CLI command on a managed device returns a value of 0 for Minimum RTT: ■ The **stats_ip_probe_uplink** streaming API ■ The **show ip health-check verbose** CLI command **Scenario:** This issue occurs in managed devices with **Uplink Health-check** configuration enabled. This issue is observed in OAW-40xx Series and OAW-4x50 Series Switches running AOS-W 8.0.1.0 or later versions. **Workaround:** None.	Switch-Datapath	OAW-40xx Series and OAW-4x50 Series Switches	AOS-W 8.0.1.0
AOS-145310 AOS-146256	177211 178472	**Symptom:** A mesh point fails to get an IP address. **Scenario:** This issue occurs when the Mesh Private VLAN is in another VLAN. This issue is observed in APs running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	Mesh	All platforms	AOS-W 8.3.0.0
AOS-145529	177509	**Symptom:** A user is unable to ping the servers from a managed device. **Scenario:** This issue occurs when the managed device obtains configuration after a reload. This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 8.0.1.0

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-145538	177522	**Symptom:** The **Controller discovery** field in **Campus APs** and **Remote APs** pages of the WebUI displays an irrelevant option. **Scenario:** This issue occurs when users provision APs by using the **Controller discovery** field in **Campus APs** or **Remote APs** page of the WebUI. This issue is observed in managed devices running AOS-W 8.2.0.2 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.2.0.2
AOS-145566	177559	**Symptom:** A Mobility Master is unable to forward the traffic that is sourced from an IP interface in the gateway. **Scenario:** 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. **Workaround:** None.	Policy-Based Routing	All platforms	AOS-W 8.0.1.0
AOS-145612	177618	**Symptom:** The **sapd** process crashes in an AP. **Scenario:** This issue occurs when two APs have the same AP name. This issue is observed in APs running AOS-W 8.2.0.2 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 8.2.0.2
AOS-145822 AOS-147161	177898 179840	**Symptom:** Clients are unable to obtain IP addresses and the DHCP requests are not sent to the DHCP server. **Scenario:** This issue occurs when uplink load balancing is enabled on a managed device. This issue is observed in managed devices running AOS-W 8.2.1.0. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 8.2.1.0
AOS-145910	178014	**Symptom:** Managed devices send RADIUS accounting request packets to ClearPass without class attributes. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.0.2. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.2.0.2
AOS-146042 AOS-151140	178173 185322	**Symptom:** The log file of a Mobility Master Virtual Appliance displays the **OID not increasing** SNMP error message. **Scenario:** This issue is observed in a Mobility Master Virtual Appliance running AOS-W 8.2.0.2. **Workaround:** None.	SNMP	All platforms	AOS-W 8.2.0.2

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-146143 AOS-156175	178322 192241	**Symptom:** The **datapath** process in a Mobility Master crashes when OpenFlow is enabled and disabled multiple times from the Mobility Master. **Scenario:** This issue is observed in OAW-4850 Switches running AOS-W 8.2.0.2 or later versions in a cluster setup. **Workaround:** None.	Switch-Datapath	OAW-4850 Switches	AOS-W 8.2.0.2
AOS-146200	178394	**Symptom:** When an incorrect password is entered in an external captive portal, **errmsg=Authentication%20failed** is appended incorrectly to the URL and the login page does not load correctly. **Scenario:** This issue occurs when external captive portal is used with a non-ClearPass Policy Manager server. This issue is observed in managed devices running AOS-W 8.2.1.0 or later versions. **Workaround:** None.	Captive Portal	All platforms	AOS-W 8.2.1.0
AOS-146425	178709	**Symptom:** The **Ipsec-map name** drop-down list does not display the system-generated IPsec map in the WebUI. **Scenario:** This issue occurs when the user creates a new policy rule in the **Configuration** > **Roles & Policies** > **Policies** > **<policy_name>** > **<new_policy_rule>** page, and selects **Forward to ipsec-map** option from the **Action** drop-down list in the WebUI. This issue is observed in Mobility Masters running AOS-W 8.2.1.0. **Workaround:** None.	WebUI	All platforms	AOS-W 8.2.1.0
AOS-146445 AOS-146477 AOS-146480	178782 178734 178785	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:4)**. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.0 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 8.2.1.0
AOS-146459 AOS-147238 AOS-147239 AOS-153832	178760 179949 179950 189003	**Symptom:** OAW-IAPs connecting to a managed device obtain IP address in the reverse order. **Scenario:** This issue occurs when a MAC address of an OAW-IAP is configured with a remote IP address in the remote whitelist database using the **whitelist-db rap add mac-address <mac-address>** command. This issue is observed in Mobility Controller Virtual Appliance running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	CPsec	All platforms	AOS-W 8.3.0.0

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-146478 AOS-157171	178783 193572	**Symptom:** A managed device reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (Heartbeat Initiated) (Intent:cause:register 53:86:50:4)**. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.0 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 8.2.1.0
AOS-146571	178905	**Symptom:** The role name is incorrectly displayed in the edit rule table in **Configuration > Roles & Policies > Roles > Global Rules** page of the WebUI. **Scenario:** This issue is observed in a managed devices running AOS-W 8.2.1.0. **Workaround:** None.	WebUI	All platforms	AOS-W 8.2.1.0
AOS-146588 AOS-146778	178936 179171	**Symptom:** The **General Information** > **Networking** page in a Virtual OmniAccess Mobility Controller does not display the information about DNS server and IP address. **Scenario:** This issue is observed in a Mobility Master Virtual Appliance running AOS-W 8.3.0.0. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 8.3.0.0
AOS-146663	179027	**Symptom:** Active VRRP managed devices are not forwarding traffic upstream through the GRE tunnel. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.0 in a cluster setup. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 8.2.1.0
AOS-146670 AOS-157311 AOS-182295	179034 193759	**Symptom:** Clients experience poor performance with OAW-AP305 access points. **Scenario:** The issue occurs in OAW-AP305 access points running AOS-W 8.3.0.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP305 access points	AOS-W 8.3.0.0
AOS-146720	179107	**Symptom:** A stand-alone Switch displays the **Module licensemgr is busy. Please try later** error message while adding licenses. **Scenario:** This issue is observed in stand-alone Switches running AOS-W 8.1.0.4 in a master-local topology. **Workaround:** None.	Licensing	All platforms	AOS-W 8.1.0.4

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-146829	179248	**Symptom:** No error message is displayed when an SNMP community / user string is configured with less than 5 characters. **Scenario:** This issue is observed in the managed devices running in AOS-W 8.2.1.0-FIPS. **Workaround:** None.	SNMP	All platforms	AOS-W 8.2.1.0
AOS-146845	179267	**Symptom:** The WebUI shows the **Invalid MAC address** error when adding a MAC address in the **Managed Network** > **Configuration** > **Access Points** > **Whitelist** page. **Scenario:** This issue is observed in a Mobility Master Virtual Appliance running AOS-W 8.3.0.0. **Workaround:** None.	WebUI	All platforms	AOS-W 8.3.0.0
AOS-146989	179483	**Symptom:** A user is unable to delete **folder _config1** folder on the Mobility Master WebUI. **Scenario:** This issue occurs due to dummy nodes created in the datastore that are not deleted after executing a configuration difference. This issue is observed in a Mobility Master Virtual Appliance running AOS-W 8.2.1.0. **Workaround:** None.	Configuration	Mobility Master Virtual Appliance	AOS-W 8.2.1.0
AOS-147039 AOS-156717	179627 193004	**Symptom:** The **FPAPPs** process is stuck in a managed device. **Scenario:** This issue occurs when the initial full-setup wizard is used to switch a OAW-4450 Switch that is running in stand-alone mode to a managed device and an invalid netmask is entered. This issue is observed in OAW-4450 Switches running AOS-W 8.2.1.0. **Workaround:** None.	L2 Forwarding	OAW-4450 Switches	AOS-W 8.2.1.0
AOS-147511	180406	**Symptom:** Clients are receiving IPv6 router advertisements randomly from different VLANs. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.0 or later versions. **Workaround:** None.	IPv6	All platforms	AOS-W 8.2.1.0

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-147552	180489	**Symptom:** CLI-based upgrade of a stand-alone Switch fails with the **Timed out, Try again** error message. **Scenario:** This issue occurs in a slow network connection when the **copy scp** command fails to download the AOS-W image after 15 minutes. This issue is observed in managed devices running AOS-W 8.2.1.0 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.2.1.0
AOS-148349	181630	**Symptom:** User is not able to disable the **openflow-profile** on a managed device. **Scenario:** This issue occurs when user disables the **openflow profile** at a configuration level lower than /md. This issue is observed in managed devices running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	SDN	All platforms	AOS-W 8.2.1.1
AOS-148450	181773	**Symptom:** Managed devices reboot unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.0 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 8.2.1.0
AOS-148894	182352	**Symptom:** An AP does not take the EIRP settings from the radio profile and broadcasts with high EIRP. **Scenario:** This issue is observed in APs running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	AirMatch	All platforms	AOS-W 8.2.1.1
AOS-149084	182604	**Symptom:** The **Illegal operation on the interface** error is observed when the user tries to add or remove a trusted VLAN on the managed device. **Scenario:** This issue occurs when the user tries to configure the GigabitEthernet interface with a valid port range. This issue is observed in managed devices running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	VLAN	All platforms	AOS-W 8.2.0.0

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-149214	182780	**Symptom:** The output of few **show datapath** commands displays the MAC address in upper case. **Scenario:** This issue occurs when the following show datapath commands are issued. This issue is not restricted to any Switch or AOS-W versions. ■ **show datapath route-cache** ■ **show datapath station** ■ **show datapath bridge** ■ **show datapath firewall-agg-sess** ■ **show datapath tunnel** ■ **show datapath tunnel station-list** ■ **show datapath user** ■ **show datapath user rad-counter** **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 8.2.1.0
AOS-149407	183034	**Symptom:** Clients get disconnected after roaming although auto connect is enabled. **Scenario:** This issue is observed in APs running AOS-W 8.0.1.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 8.0.1.0
AOS-149578 AOS-154680	183246 190113	**Symptom:** Managed devices get converted to master node automatically when a power outage occurs while a configuration change is received from the Mobility Master. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.0.1.0
AOS-149983 AOS-153622	183788 188706	**Symptom:** A few APs that are displayed as up when the **show ap database** command is executed are not displayed in the **Dashboard > Infrastructure > Access Points** page of the Mobility Master WebUI. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.3.0.0. **Workaround:** None.	AP-Platform	All platforms	AOS-W 8.3.0.0

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-150398	184327	**Symptom:** A client is displayed on the wrong managed device after association when there is no traffic flow from the client. **Scenario:** This issue occurs when the **fdb-update-on-assoc** parameter is enabled in an L2 cluster. This issue is observed in managed devices running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	Station Management	All platforms	AOS-W 8.2.1.1
AOS-150496 AOS-150883 AOS-158128	184454 184972 195001	**Symptom:** The IP OSPF message-digest key gets erased. **Scenario:** This issue occurs when the managed device enters or returns from the disaster recovery mode. This issue is observed in managed devices running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 8.2.1.1
AOS-150721	184754	**Symptom:** The certificate expiration date is not calculated correctly and displays the current date as the expiration validity date. **Scenario:** This issue occurs when the day light savings is not considered in the timezone calculation. This issue is observed in managed devices running AOS-W 8.2.1.0 or later versions. **Workaround:** None.	Certificate Manager	All platforms	AOS-W 8.2.1.0
AOS-150748	184786	**Symptom:** APs are not broadcasting on Virtual APs and are displaying **D** flag in the output of the **show ap database** command, indicating that the AP configuration either has errors or is missing. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.0.2 or later versions in a cluster setup. **Workaround:** Ensure the VLAN name binding on **virtual-ap** profile is same as the name of named VLAN.	AP-Platform	All platforms	AOS-W 8.2.0.2
AOS-150797	184849	**Symptom:** Clients are unable to make or receive calls. A **Network busy** error message is displayed. **Scenario:** This issue occurs when WMM is disabled on the managed device. This issue is observed in OAW-AP315 access points running AOS-W 8.2.1.1. **Workaround:** None.	WMM	OAW-AP315 access points	AOS-W 8.2.1.1

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-150844	184903	**Symptom:** AMON messages related to uplink load balancing are not forwarded to Central. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions. **Workaround:** None.	AMON	All platforms	AOS-W 8.0.1.0
AOS-151012 AOS-146980	185165	**Symptom:** A managed device crashes unexpectedly. The log file lists the reason for this event as **Reboot Cause: Reboot by Upgrade Manager Intent:cause:register 60:86:50:60).** **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 8.2.1.1
AOS-151080 AOS-156468 AOS-157172	185255 192649 193573	**Symptom:** A license is not sent to a managed device. **Scenario:** This issue occurs when an external Mobility Master or a stand-alone Switch is used as a licensing server. This issue is observed in managed devices running AOS-W 8.3.0.3. **Workaround:** None.	Licensing	All platforms	AOS-W 8.3.0.3
AOS-151110 AOS-155015 AOS-180155 AOS-182098	185286 187984 190542	**Symptom:** A radio experiences a high number of resets in APs. **Scenario:** This issue occurs when the APs are in Air Monitor mode. This issue is observed in OAW-AP335 access points running AOS-W 8.2.0.0 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP335 access points	AOS-W 8.2.0.0
AOS-151282	185506	**Symptom:** A managed device is unable to synchronize its AP whitelist on Mobility Master with the Activate whitelist database. **Scenario:** This issue occurs when the managed device is unable to contact the Mobility Master to establish IPsec tunnels. This issue is observed in managed devices running AOS-W 8.0.1.0. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 8.0.1.0
AOS-151350	185597	**Symptom:** The output of the **show switches** command displays the IPv6 address of a standby Mobility Master as **none**. **Scenario:** This issue occurs when the **show switches** command is executed on a Mobility Master. This issue is observed in Mobility Masters running AOS-W 8.2.1.1. **Workaround:** None.	Configuration	All platforms	AOS-W 8.2.1.1

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-151355	185602	**Symptom:** Managed Devices are unable to pass traffic to the nexthop VPN concentrator (VPNC) using policy-based routing. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.1.0 or later versions. **Workaround:** None.	Policy-Based Routing	All platforms	AOS-W 8.0.1.0
AOS-151413 AOS-152871 AOS-153240 AOS-153948 AOS-153981 AOS-155577	185679 187734 188214 189144 189191 191414	**Symptom:** An AP crashes and reboots unexpectedly. **Scenario:** This issue is observed in APs running AOS-W 8.2.2.0 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 8.2.2.0
AOS-151652	186018	**Symptom:** Mobility Master sends a large number of authorization requests to the ClearPass Policy Manager for the AirGroup users. **Scenario:** This issue occurs as the IPv6 addresses are aging out. This issue is observed in Mobility Master running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	SDN	All platforms	AOS-W 8.2.1.1
AOS-151759	186146	**Symptom:** The output of the **show ap debug port status ap-name <ap-name>** command displays the status of **PortFast** parameter as **unknown**. **Scenario:** This issue is observed in OAW-AP303H access points running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	AP-Platform	OAW-AP303H access points	AOS-W 8.2.1.1
AOS-152076 AOS-150739	186605 184774 185405	**Symptom:** A managed device fails to establish IPsec tunnel on its primary uplink. **Scenario:** This issue occurs because the socket descriptor slots are not reused when the IP address is flapped in the **isakmpd** process. This issue is observed in managed devices running AOS-W 8.0.1.0. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 8.0.1.0

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-152500	187191	**Symptom:** Wireless clients are not added as OpenFlow hosts in the Mobility Master. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	SDN	All platforms	AOS-W 8.2.1.1
AOS-152631	187390	**Symptom:** VoIP clients face connectivity issues when IPv6 is enabled. **Scenario:** This issue occurs when UCC flows are processed using the IPv6 address instead of the IPv4 address of the managed device in an IPv6 cluster. This issue is observed in managed devices running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	UCC	All platforms	AOS-W 8.2.1.1
AOS-152941 AOS-153955	187831 189158	**Symptom:** In the WebUI, the **Diagnostics > Technical support > Copy files** fails to copy flash to an scp server. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.0.0.0
AOS-153090	188025	**Symptom:** PEFNG license count is displayed incorrectly in the **Mobility Master > Configuration > License > License usage > PEF** column of the WebUI. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 8.2.1.1
AOS-153365 AOS-174754 AOS-175325	164533 188374	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**. **Scenario:** This issue is observed in OAW-AP225 access points running AOS-W 8.2.1.0. **Workaround:** None.	AP-Wireless	OAW-AP225 access points	AOS-W 8.2.1.0
AOS-153460	188497	**Symptom:** A OAW-4750 Switch sends **RSSI AMON** messages even though the location is disabled in the management server profile. **Scenario:** This issue is observed in OAW-4750 Switches running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	AMON	OAW-4750 Switches	AOS-W 8.2.1.1

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-153876 AOS-155448	189052 191171	**Symptom:** A RADIUS server IP address changes to an incorrect IP address on all managed devices. **Scenario:** This issue is observed when managed devices reboot after full synchronization. This issue is observed in managed devices running AOS-W 8.3.0.3. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.3.0.3
AOS-154246	189552	**Symptom:** IP access restrictions on VLAN interface is not working as expected and is not blocking expected traffic. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.2.1 or later versions. **Workaround:** None.	VLAN	All platforms	AOS-W 8.2.2.1
AOS-154386 AOS-157543	189716 194143	**Symptom:** A default crypto isakmp policy with a value above 10000 can be created but not deleted. **Scenario:** This issue is observed in a Mobility Master Virtual Appliance running AOS-W 8.2.2.1. **Workaround:** None.	IPsec	All platforms	AOS-W 8.2.2.1
AOS-154564 AOS-155770 AOS-156549	189952 191667 192768	**Symptom:** The **SNMP** process crashes in a managed device. **Scenario:** This issue occurs when the **SNMP** process receives a request to query the table, **wlsxSwitchAccessPointTable**. This issue is observed in OAW-4750XM Switches running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	SNMP	OAW-4750XM Switches	AOS-W 8.2.1.1
AOS-154647	190062	**Symptom:** Output of the **show datapath frame all** command does not display any values. **Scenario:** This issue is observed in OAW-4750XM Switches running AOS-W 8.2.1.1. **Workaround:** None.	Switch-Datapath	OAW-4750XM Switches	AOS-W 8.2.1.1

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-155081	190642	**Symptom:** Post configuration changes, values of **show configuration committed** and **show configuration effective** commands are different. **Scenario:** This issue occurs if Iterator is not reset after handling auth-servers list in gdata. This issue is observed in a managed devices running AOS-W 8.2.1.0 **Workaround:** None.	Configuration	All platforms	AOS-W 8.2.1.0
AOS-155300 AOS-155345	190957 191022	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for this event as **Hardware Watchdog Reset (Intent:cause:register 54:86:0:8020)**. **Scenario:** This issue is observed in OAW-4850 Switches running AOS-W 8.3.0.3 or later versions. **Workaround:** None.	Switch-Datapath	OAW-4850 Switches	AOS-W 8.3.0.3
AOS-155396 AOS-155629	191092 191483	**Symptom:** Multiple processes in a managed device crash unexpectedly. **Scenario:** The issue occurs due to a memory leak and high CPU utilization on the managed devices. This issue is observed in managed devices running AOS-W 8.2.0.2 or later versions. **Workaround:** None.	SDN	All platforms	AOS-W 8.2.0.2
AOS-155877	191816	**Symptom:** A managed device crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Kernel Panic (Intent:cause:register 12:86:0:20).** **Scenario:** This issue is observed in OAW-4450 stand-alone Switches running AOS-W 8.2.2.0 or later versions. **Workaround:** None.	Switch-Platform	OAW-4450 stand-alone Switches	AOS-W 8.2.2.0
AOS-155879	191818	**Symptom:** User is unable to delete or edit guest provisioning user on WebUI and CLI. **Scenario:** This issue occurs due to a trailing space that is added when adding a user. This issue is observed in Mobility Master Virtual Appliance running AOS-W 8.2.0.2. **Workaround:** None	Base OS Security	All platforms	AOS-W 8.2.0.2

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-155927	191876	**Symptom:** Clients are getting de-authenticated when the User Anchor Controller (UAC) is down. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.1 or later versions. **Workaround:** None.	Station Management	All platforms	AOS-W 8.2.1.1
AOS-156027	192034	**Symptom:** Access point stops broadcasting on 2.4 GHz radios. **Scenario:** This issue is observed in OAW-AP105 access points connected to OAW-4650 Switches running AOS-W 8.2.0.0. **Workaround:** None.	AP-Wireless	OAW-AP105 access points	AOS-W 8.2.0.0
AOS-156162 AOS-158131	192223 195005	**Symptom:** Managed devices are rebooting intermittently. The log file lists the reason for the event as **dds process died**. **Scenario:** This issue is observed in managed devices running AOS-W 8.3.0.3 or later versions. **Workaround:** None.	HA-Lite	All platforms	AOS-W 8.3.0.3
AOS-156267	192349	**Symptom:** The **mDNS** process running in a managed device consumes more memory than the typical threshold limit. **Scenario:** This issue is observed in managed devices running AOS-W 8.4.0.0. **Workaround:** None.	AirGroup	All platforms	AOS-W 8.4.0.0
AOS-156742 AOS-156977	193031 193319	**Symptom:** After pushing a complete configuration via API, the user is unable to make any change to IP Probe configuration. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.1.0. **Workaround:** None.	Configuration	All platforms	AOS-W 8.0.1.0
AOS-156788 AOS-157820	193096 194558	**Symptom:** Users are unable to view Chromecast devices. **Scenario:** This issue occurs when the 802.1x username and the username shared in the ClearPass Policy Manager list use different cases. This issue is observed in AirGroup that is enabled with CPPM-based policies running AOS-W 8.4.0.0. **Workaround:** Ensure usernames in both places are created in the same case.	AirGroup	All platforms	AOS-W 8.4.0.0

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-156838	193158	**Symptom:** User is unable to reprovision an AP. **Scenario:** This issue occurs when a special character in a German keypad is used in the AP name. This issue is observed in APs connected to managed devices running AOS-W 8.2.2.1. **Workaround:** Hard reset the access point.	Configuration	All platforms	AOS-W 8.2.2.1
AOS-156874 AOS-156918 AOS-157515	193195 193249 194093	**Symptom:** Managed devices crash and reboot unexpectedly. The log file lists the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in OAW-4750XM Switches running AOS-W 8.2.2.0 or later versions. **Workaround:** None.	Switch-Datapath	OAW-4750XM Switches	AOS-W 8.2.2.0
AOS-156878	193199	**Symptom:** A Switch crashes when collecting support logs. **Scenario:** This issue occurs when the **show openflow debug ports** command is executed. This issue is observed in OAW-4750 Switches running AOS-W 8.2.2.1. **Workaround:** None.	SDN-Platform	OAW-4750 Switches	AOS-W 8.2.2.1
AOS-157056	193423	**Symptom:** The **Authentication** module on a managed device crashes and the APs reboot. **Scenario:** This issue occurs when clients that are in bridge forwarding mode, communicate with a managed device, in the split-tunnel-mode. This issue is observed in managed devices running AOS-W 8.2.1.0. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.2.1.0
AOS-157162	193561	**Symptom:** A UAC tunnel is not formed in a cluster. The log file lists the reason for the event as **Dynamic BSS tunnel could not be setup /Denied; AP not found in STM**. **Scenario:** This issue is observed in OAW-4750 Switches running AOS-W 8.2.2.3 in a cluster setup. **Workaround:** None.	Cluster Manager	OAW-4750 Switches	AOS-W 8.2.2.3
AOS-157288	193726	**Symptom:** The REST API returns the output in XML format instead of JSON format. **Scenario:** This issue occurs when the **show ap arm state** command is executed. This issue is observed in managed devices running AOS-W 8.2.1.0. **Workaround:** None.	ARM	All platforms	AOS-W 8.2.1.0

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-157293	193731	**Symptom:** A VLAN is not preserved and a client gets an IP address from a different VLAN that is configured in the VLAN pool. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.2.2. **Workaround:** None.	Station Management	All platforms	AOS-W 8.2.2.2
AOS-157308 AOS-158209	193755	**Symptom:** The **wlsxWlanRadioTable** SNMP does not show all radio types. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.0. **Workaround:** None.	Station Management	All platforms	AOS-W 8.2.1.0
AOS-157563 AOS-158459	194178 195465	**Symptom:** A managed device reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (Fpapps Initiated) (Intent:cause:register 51:86:50:4)**. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.1. **Workaround:** None.	Controller-Datapath	All platforms	AOS-W 8.2.1.1
AOS-157584	194205	**Symptom:** A client that is connected to the ENET port of an AP and having both IPv4 and IPv6 addresses loses the bandwidth-contract. **Scenario:** This issue occurs when the IPv6 entry is timed-out. This issue is observed in managed devices running AOS-W 8.2.2.3. **Workaround:** None.	IPv6	All platforms	AOS-W 8.2.2.3
AOS-157815	194552	**Symptom:** A managed device drops the tunneled node GRE packets for an AP. **Scenario:** This issue is observed in managed devices running AOS-W 8.1.0.0. **Workaround:** None.	Tunnel-Node-Manager	All platforms	AOS-W 8.1.0.0
AOS-158093	194946	**Symptom:** The WEP key ID of multicast packets in a managed device is incorrect. **Scenario:** This issue occurs when AirMatch changes the channel. This issue is observed in managed devices running AOS-W 8.2.2.1. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.2.2.1

Table 7: *Known Issues in AOS-W 8.2.2.5*

New Bug ID	Old Bug ID	Description	Component	Platform	Reported Version
AOS-158299	195239	**Symptom:** The **profmgr** process crashes and the Mobility Master restarts unexpectedly. **Scenario:** This issue is observed in Mobility Masters running AOS-W 8.0.1.0. **Workaround:** None.	Configuration	All platforms	AOS-W 8.0.1.0
AOS-158311	195264	**Symptom:** A managed device does not prompt an error or show restriction when configuring a VRRP authentication key. **Scenario:** This issue occurs when the VRRP authentication key contains more than 8 characters. This issue is observed in managed devices running AOS-W 8.2.1.0. **Workaround:** None.	VRRP	All platforms	AOS-W 8.2.1.0
AOS-158455	195461	**Symptom:** The output for the **show configuration system-commands pending** command lists the committed configuration. **Scenario:** This issue is observed in managed devices running AOS-W 8.2.1.0. **Workaround:** None.	Configuration	All platforms	AOS-W 8.2.1.0
AOS-158497	195513	**Symptom:** An AP reboots unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: softlockup: hung tasks**. **Scenario:** This issue is observed in OAW-AP303H access points running AOS-W 8.2.2.3. **Workaround:** None.	AP Datapath	OAW-AP303H access points	AOS-W 8.2.2.3
AOS-182091 AOS-183253 AOS-183255		**Symptom:** The **mDNS** process in a managed device crashes unexpectedly. **Scenario:** This issue occurs because of memory corruption. This issue is observed in a Mobility Master Hardware Appliance running AOS-W 8.2.2.3. **Workaround:** None.	AirGroup	All platforms	AOS-W 8.2.2.3

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

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

Topics in this chapter include:

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

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

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

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

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

Important Points to Remember and Best Practices

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

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

Memory Requirements

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

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

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

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

- **Crash Data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 45 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 45 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 45 to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the managed device.

The following procedure deletes a file.

In the WebUI

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

In the CLI

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

Backing up Critical Data

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

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

- Flashbackup

Backing up and Restoring Compact Flash in the WebUI

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

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

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

Backing up and Restoring Compact Flash in the CLI

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

1. Make sure you are in the **enable** mode in the CLI, and execute the following command:
   ```
   (host) # write memory
   ```
2. Execute the **backup** command to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.
   ```
   (host) # backup flash
   Please wait while we take the flash backup.......
   File flashbackup.tar.gz created successfully on flash.
   Please copy it out of the controller and delete it when done.
   ```
3. Execute the **copy** command to transfer the backup flash file to an external server or storage device.
   ```
   (host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword> <remote directory>
   (host) copy flash: flashbackup.tar.gz usb: partition <partition-number>
   ```
   You can later transfer the backup flash file from the external server or storage device to the compact flash file system by executing the **copy** command.
   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   (host) # copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
   ```
4. Execute the **restore** command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system.
   ```
   (host) # restore flash
   Please wait while we restore the flash backup........
   Flash restored successfully.
   Please reload (reboot) the controller for the new files to take effect.
   ```

Upgrading

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

AOS-W 8.2.0.1 Upgrade Notes

Before you upgrade Mobility Master from AOS-W 8.0.0.0 to AOS-W 8.1.0.0, take a note of the following points:

- AOS-W 8.1.0.0 supports only a maximum of 3 network adapters for Mobility Master and 4 network adapters for Mobility Master Virtual Appliance. If you have 4 network adapters on your AOS-W 8.0.0.0 Mobility Master Virtual Appliance, you must remove one before upgrading to AOS-W 8.1.0.0 to avoid upgrade failure. To remove a network adapter from AOS-W 8.0.0.0 Mobility Master Virtual Appliance:

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

  1. Log in to the vSphere client.
  2. Select the Mobility Master VM instance and click **Shut down the virtual machine**.
  3. Click **Edit Virtual machine settings**.
  4. From the **Hardware** tab, select and remove a network adapter that is not active.
- Before upgrading to AOS-W 8.1.0.0 from AOS-W 8.0.0.0, ensure that you configure the MAC address of the management interface as the peer MAC address, if the peer is a Mobility Master Virtual Appliance or Mobility Master. Before reloading the new image on Mobility Master, alter the peer MAC address using the following procedure in the WebUI:
  1. From the **Managed Network** node hierarchy, select the managed device.
  2. Navigate to **Configuration > Controllers** and enter the management interface MAC address in the **Peer MAC address of master** field.
  3. Click **Submit** and click **Continue** in the reload popup.
  4. Click **Pending Changes**.
  5. In the **Pending Changes** window, select the check box and click **Deploy changes**.

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

  ```
  (host) [<device-mac-address>] (config) #masterip <ipaddr> ipsec <key> peer-mac-1 <mgmt-interface-mac> peer-mac-2 <mgmt-interface-mac> interface vlan <id>
  ```
- Before upgrading to AOS-W 8.2.1.0, you must share the licenses within the global licensing pool by executing the **license-pool-profile-root** command:

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

In the WebUI

CAUTION

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash space available for an upgrade using the WebUI. For details, see Memory Requirements on page 44.

NOTE

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

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

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

NOTE

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

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

NOTE

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

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

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

11. Click **OK**.

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

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

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

1. Log in to the WebUI to verify all your Switches are up after the reboot.
2. Navigate to the **Dashboard > Access Points** page to determine if your APs are up and ready to accept clients. In addition, verify that the number of access points and clients are what you would expect.
3. Verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 45 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 44.

Upgrading From a Recent Version of AOS-W

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

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

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

   or

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

   or

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

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

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

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

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

or

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

or

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

or

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

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

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

7. Reboot the Switch.

   ```
   (host)# reload
   ```

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

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

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

1. Log in to the CLI to verify that all your Switches are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of access points and clients are what you expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 45 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 45.
2. Verify that the control plane security is disabled.
3. Set the Switch to boot with the previously saved pre-AOS-W configuration file.
4. Set the Switch to boot from the system partition that contains the previously running AOS-W image.

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

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

Downgrading Using the WebUI

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

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the Switch by navigating to the **Diagnostics > Technical Support > Copy Files** page.
   a. For **Select source file** option, select FTP or TFTP server, and enter the IP address of the FTP or TFTP server and the name of the pre-upgrade configuration file.
   b. For **Select destination file** option, enter a file name (other than default.cfg) for Flash File System.
2. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Software Management > Upgrade** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition) by performing the following steps:
   a. Enter the FTP/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
3. Navigate to the **Maintenance > Software Management > Boot Parameters** page.
   a. Select the system partition that contains the pre-upgrade image file as the boot partition.
   b. Click **Apply**.
4. Navigate to the **Maintenance > Software Management > Reboot** page. Select **Save configuration before reboot** option and click **Reboot**. The Switch reboots after the countdown period.
5. When the boot process is complete, verify that the Switch is using the correct software by navigating to the **Maintenance > Software Management > About** page.

Downgrading Using the CLI

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

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

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

   or

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

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

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

3. Execute the **show image version** command to view the partition on which your previous software image is stored. You cannot load a new image into the active system partition (the default boot).
   ```
   #show image version
   ```
4. Set the backup system partition as the new boot partition.
   ```
   (host) # boot system partition 1
   ```
5. Reboot the Switch.
   ```
   (host) # reload
   ```
6. When the boot process is complete, verify that the Switch is using the correct software.
   ```
   (host) # show image version
   ```

Before You Call Technical Support

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

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

Appendix A
Glossary of Terms

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

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

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

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

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

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

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

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

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

802.11b

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

802.11d

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

802.11e

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

802.11g

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

802.11h

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

802.11i

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

802.11j

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

802.11k

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

802.11m

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

802.11n

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

802.11r

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

802.11u

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

802.11v

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

802.1Q

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

802.1X

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

802.3af

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

802.3at

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

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: APname.Floor.Building.Campus.

frequency allocation

Use of radio frequency spectrum as regulated by governments.

FSPL

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

FTP

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

GARP

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

GAS

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

gateway

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

Gbps

Gigabits per second.

GBps
Gigabytes per second.

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

GHz
Gigahertz.

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

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

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

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

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

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

H2QP
Hotspot 2.0 Query Protocol.

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

hotspot

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

HSPA

High-Speed Packet Access.

HT

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

HTTP

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

HTTPS

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

IAS

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

ICMP

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

IDS

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

IEEE

Institute of Electrical and Electronics Engineers.

IGMP

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

IGMP snooping

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

IGP

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

IGRP

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

IKE

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

IKEv1

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

IKEv2

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

IoT

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

IPM

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

IPS

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

IPsec

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

IPSG

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

IrDA

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

ISAKMP

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

ISP

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

JSON

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

Kbps

Kilobits per second.

KBps

Kilobytes per second.

keepalive

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

L2TP

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

LACP

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

LAG

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

LAN

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

LCD

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

LDAP

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

LDPC

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

LEAP

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

LED

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

LEEF

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

LI

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

LLDP

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

LLDP-MED

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

LMS

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

LNS

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

LTE

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

MAB

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

MAC

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

MAM

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

Mbps

Megabits per second

MBps

Megabytes per second

MCS

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

MD4

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

MD5

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

MDAC

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

MDM

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

mDNS

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

MFA

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

MHz

Megahertz

MIB

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

microwave

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

MIMO

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

MISO

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

MLD

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

MPDU

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

MPLS

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

MPPE

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

MS-CHAP

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

MS-CHAPv1

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

MS-CHAPv2

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

MSS

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

MSSID

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

MSTP

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

MTU

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

MU-MIMO

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

MVRP

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

mW

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

NAC

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

NAD

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

NAK

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

NAP

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

NAS

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

NAT

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

NetBIOS

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

netmask

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

NFC

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

NIC

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

Nmap

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

NMI

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

NMS

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

NOE

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

NTP

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

OAuth

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

OCSP

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

OFDM

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

OID

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

OKC

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

onboarding

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

OpenFlow

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

OpenFlow agent

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

Optical wireless

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

OSI

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

OSPF

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

OSPFv2

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

OUI

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

OVA

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

OVF

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

PAC

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

PAP

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

PAPI

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

PBR

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

PDU

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

PEAP

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

PEF

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

PEFNG

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

PEFV

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

PFS

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

PHB

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

PIM

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

PIN

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

PKCS#n

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

PKI

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

PLMN

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

PMK

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

PoE

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

PoE+

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

POST

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

PPP

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

PPPoE

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

PPTP

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

private key

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

PRNG

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

PSK

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

PSU

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

public key

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

PVST

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

PVST+

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

QoS

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

RA

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

Radar

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

RADIUS

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

RAM

Random Access Memory.

RAPIDS

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

RARP

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

Regex

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

Registration Authority

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

Remote AP

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

REST

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

RF

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

RFC

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

RFID

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

RIP

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

RJ45

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

RMA

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

RMON

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

RoW

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

RSA

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

RSSI

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

RSTP

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

RTCP

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

RTLS

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

RTP

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

RTS

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

RTSP

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

RVI

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

RW

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

SA

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

SAML

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

SCEP

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

SCP

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

SCSI

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

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.