AOS-W 8.2.1.0

Alcatel·Lucent
Enterprise

Release Notes

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 02	Added OAW-AP90 Series access points in the **Supported Platforms** section.
Revision 01	Initial release.

This release of AOS-W includes new features and enhancements and fixes to issues identified in previous releases.

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

Use the following links to navigate to the corresponding topics:

- New Features and Enhancements on page 1 describes the new features and enhancements introduced in this release.
- Supported Hardware Platforms on page 1 describes the hardware platforms supported in this release.
- Regulatory Updates on page 1 lists the regulatory updates in this release.
- Resolved Issues on page 1 lists the issues resolved in this release.
- Known Issues on page 1 lists the issues identified in this release.
- Upgrade Procedure on page 61 describes the procedures for upgrading your WLAN network to the latest AOS-W version.
- Glossary of Terms on page 71 lists the acronyms and abbreviations.

Related Documents

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

- *AOS-W 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 Mac OS
- Apple Safari 8.0 or later on Mac OS
- Google Chrome

Contacting Support

Table 2: *Contact Information*

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

The following feature enhancements are introduced in this AOS-W release.

AirMatch

New Commands

The following commands are introduced in AOS-W 8.2.1.0:

- **show airmatch network-tech-support**—This command collects the output for all the radios that are in the same partition for a specified Radio AP name. This command also lists and describes the AP Radios that will be handled further.

The following example displays a partial output of the **show airmatch network-tech-support ap-name F-16-a-QCA** command:

```
(host) [mynode]#show airmatch network-tech-support ap-name F-16-a-QCA
 Summary of included radios
 AP Name: F-16-a-QCA Radio: ac:a3:1e:59:b4:c0 Band: 2GHz RF domain: 001 partition: 000
 Num radios: 40 New radios: false

   Radio             AP Name

   ----------------- -----------
   ac:a3:1e:59:b4:c0 F-16-a-QCA
   a8:bd:27:d0:69:e0 F-PP-a-QCA
   9c:1c:12:8c:6e:a0 Fremont-sniffer-225
   ac:a3:1e:59:9e:00 F-12
   70:3a:0e:52:22:40 F-PP-b
   ac:a3:1e:59:c7:80 F-16-c-QCA
   ac:a3:1e:59:97:e0 F-RVR-d
   ac:a3:1e:59:98:20 F-Multiclient-a
   70:3a:0e:52:23:a0 F-17-QCA
   a8:bd:27:d0:5e:80 F-19-a
```

```
70:3a:0e:52:28:e0 F-15-a
18:64:72:7e:af:20 F-15-b-QCA
a8:bd:27:59:fc:e0 F-19-c
a8:bd:27:59:fc:00 F-18-c
a8:bd:27:59:f4:e0 F-18-b
ac:a3:1e:59:aa:a0 F-13
a8:bd:27:d0:5f:c0 F-19-b
ac:a3:1e:53:b8:00 F-16-b-QCA
ac:a3:1e:59:b7:40 F-RVR-g
a8:bd:27:59:fb:e0 a8:bd:27:cd:9f:be
18:64:72:fd:67:a0 18:64:72:c7:d6:7a
18:64:72:d3:81:00 F-11-BRCM
ac:a3:1e:59:9e:80 F-front-door-1
9c:1c:12:87:33:60 F-4-BRCM
ac:a3:1e:59:9d:00 F-RVR-e
ac:a3:1e:59:9a:c0 F-14-QCA
70:3a:0e:6e:5e:20 F-RVR-b
a8:bd:27:d0:94:a0 F-18-a
ac:a3:1e:59:a0:00 1344-2-AP04
18:64:72:7e:c5:c0 F-15-c-QCA
```

- **show airmatch tech-support** —This command collects the output for the AP or the radio.

The following example displays a partial output of the **show airmatch tech-support mac ac:a3:1e:59:b4:c0** command:

```
(host) [mynode] #show airmatch tech-support mac ac:a3:1e:59:b4:c0
```

```
show airmatch debug reporting-radio MAC ac:a3:1e:59:b4:c0

Field                Value
-----                -----
Band                 2GHz
AP Ethernet MAC      ac:a3:1e:cd:9b:4c
Radio MAC            ac:a3:1e:59:b4:c0
AP Name              F-16-a-QCA
AP Model             AP-325
LMS IP               192.168.200.15
Switch IP            192.168.200.15
Last Update          2017-11-16 02:57:57
Channel              7
Bandwidth            20MHz
Channel Reason       AirMatch - Solver
Channel Update Time  2017-11-14 10:42:53
EIRP                 10.0 (dBm)
EIRP Reason          AirMatch - Solver
EIRP Update Time     2017-11-16 02:55:19
Is Active            true
Is Static Chan       false
Is Static EIRP       false
Is Static CSR        false
Deploy Hour          N/A
Retries              5
Last Retry Time      2017-11-14 09:00:38
Local Time           PST8PDT,M3.2.0,M11.1.0
```

- **show airmatch debug advanced stat** —This command displays detailed statistics about the APs or radios on a Mobility Master.

The following example indicates the AirMatch statistics related to the APs:

```
(host)#show airmatch debug advanced stat ap
```

```
Field Value
----- -----
Number of APs 2304
+----------------------------------+
|Number of 5GHz Radios per AP model|
+----------------------------------+
AP Model Count
-------- -----
AP-205H 1224
AP-224 47
AP-225 976
AP-275 55
AP-365 1
+-----------------------------------+
|Number of 2.4GHz Radios per AP model|
+-----------------------------------+
AP Model Count
-------- -----
AP-205H 1224
AP-224 47
AP-225 976
AP-275 56
AP-365 1
```

- **show airmatch debug db-dump status** —This command collects information about the status of the AirMatch debug database dump.

The following example indicates the status of the AirMatch debug database dump:

```
(host)#show airmatch debug db-dump status

dbdump status info
------------------
Field                Value
-----                -----
dbdump status        SUCCESS
Begin time           2018-03-19 15:58:50
End time             2018-03-19 15:58:53
```

AP-Wireless

No Support for Cell Size Reduction

Starting from AOS-W 8.2.1.0, the **cell-size-reduction** parameter in the **rf dot11a-radio-profile** and **rf dot11g-radio-profile** commands does not take effect for 300 Series access points. If the **cell-size-reduction** parameter has any configured value, the 300 Series access points disregard the value.

Base OS Security

Enable Telnet

To enable telnet on managed devices, execute the following commands:

```
(host) [mynode] (config) #firewall cp
(host) [mynode] (config-submode) #ipv4 permit any proto 6 ports 23 23
(host) [mynode] (config-submode) #!
(host) [mynode] (config-submode) #exit
(host) [mynode] (config) #exit
```

Modified Command

Starting from AOS-W 8.2.1.0, the output of the **show netdestination** command displays the netdestination ID along with the netdestination name. The following sample shows the output of the **show netdestination** command:

```
(host) [mynode] #show netdestination
Name: sep23-ipv4
Destination ID: 34
Position  Type  IP addr   Mask-Len/Range
--------  ----  -------   --------------
1         host  1.1.1.1   32
2         name  0.0.0.8   google.com
```

Certificate Manager

Successful Download Message

Starting from AOS-W 8.2.1.0, Mobility Master continuously tries to synchronize the certificates to a managed device until it is successful. If the synchronization fails, the failure logs are listed under the **show switches** command as **CONFIG-FAILURE**. To view the list of failed certificate synchronizations, execute the **show configuration failure** command.

Switch-Datapath

Datapath Route Limits

Starting from AOS-W 8.2.1.0, the datapath route limits are increased to match the route limits of the control plane.

Table 3: *New Datapath Route Limits*

Switch Family	New Datapath Limits
OAW-4005	4K
OAW-4008	4K
OAW-4024	4K
OAW-4030	8K
OAW-4450	16K
OAW-4550	16K
OAW-4650	16K
OAW-4750	32K
OAW-4750XM	32K
OAW-4850	32K

Switch-Platform

NTP Authentication Option

Starting from AOS-W 8.2.1.0, a new NTP authentication option using SHA1 digest is available. A new parameter, **sha1**, is introduced in the **ntp authentication-key** command. You can configure this option in the CLI as shown in the following example:

```
(host)[mynode](config) #ntp authentication-key <keyid> sha1 <keyvalue>
```

The authentication key ID must be in the range of 1–65534. The key value must be up to 255 ASCII characters.

The **show ntp authentication-keys** command helps you verify the NTP authentication key type. The output of this command displays the SHA1 key type and the secret field (in encoded format), when SHA1 authentication is configured. The following example shows the output of the **show ntp authentication-keys** command:

```
(host) [mynode] # show  ntp authentication-keys
Key Id     Key Type     Secret
------     --------     ------
41          sha1        ********
```

Retrieving Crash Information from Managed Devices

To access the crash files after upgrading a managed device to AOS-W 8.2.1.0, you must clear the old crash files. Remember the following important points regarding the old crash files cleanup:

- Before you upgrade to AOS-W 8.2.1.0, ensure that you clean up the old crash files if any, using the **tar crash** command.
- If you have upgraded a managed device to AOS-W 8.2.1.0 before cleaning up the old crash files and if there are no new crashes after the upgrade, you must still clean up the old crash files using the **tar crash** command.
- If you execute the **tar crash** command:
  - before cleaning up the old crash files, the **crash.tar** and **crash1.tar** files are created.
  - after cleaning up the old crash files, only the **crash.tar** file is created.

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

DHCP

Enhancements to Specify Option 43 as a Hex String

Starting from AOS-W 8.2.1.0, support for specifying option code with hex data string is introduced. The following example shows the output of the **ip dhcp pool** command:

```
(host) [mynode] (config-submode)# option 43
hex                     Hex String. Max hex characters allowed is 22.
ip                      Specify IP address
text                    Option string(Max 512 Characters allowed)
```

OSPF

Enhancements to show ip route Command

Starting from AOS-W 8.2.1.0, the output of the **show ip route** command is modified to display the administrative distance and cost in **[AD/Cost]** format. In the previous releases, the information was in **[Cost/AD]** format.

Following is the modified output of the **show ip route** command. **[1/0]** in the following output represents the **[AD/Cost]**, respectively.

```
Codes: C - connected, O - OSPF, R - RIP, S - static
M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN/Branch
Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10
Gateway of last resort is 10.7.73.77 to network 0.0.0.0 at cost 1
S*    0.0.0.0/0   [1/0] via 10.7.73.77*
S     172.0.0.0/8   [1/0] via 172.16.1.253*
```

Enhancements to show ip ospf interface Command

Starting from AOS-W 8.2.1.0, the output of the **show ip ospf interface vlan** command displays the **Tx Err** and **Rx Err** parameters to indicate any errors in the transmitted and received packets. This information is helpful to analyze defects based on the tech-support logs.

The following example displays the output of the **show ip ospf interface vlan 1** command:

```
Vlan 1 is up, line protocol is up
Internet Address 170.1.0.1, Mask 255.255.255.0, Area 2.0.1.1
Router ID 16.1.0.2, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DROTHER, Priority 0
Designated Router id 0.0.0.0, Interface Address 170.1.0.1
Backup designated Router id 0.0.0.0, Interface Address 170.1.0.1
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
Neighbor Count is 0
Tx Stat: Hellos 7 DbDescr 0 LsReq 0 LsUpdate 0 LsAck 0 Pkts 7
Tx Err:  BufNull 0 BufCorrupt 0 NoMem 0 SendFail 0
Rx Stat: Hellos 0 DbDescr 0 LsReq 0 LsUpdate 0 LsAck 0 Pkts 0
LoopSend 0 RxVirtualLink 0
Rx Err:  DisCd 0 BadVer 0 BadNet 0 BadArea 0 BadDstAdr 0 BadAuType 0
BadAuth 0 BadNeigh 0 BadPckType 0 BadVirtLink 0
IntfDown 0 MySource 0 Legal 0
```

SNMP

Enhancement to SNMP Authentication Failed Trap

Starting from AOS-W 8.2.1.0, the **SNMP Authentication Failure** trap includes the IPv4 address of the source that fails authentication.

VRRP

Support for Unique Local Address Configuration on VRRP

Starting from AOS-W 8.2.1.0, you can configure a unique local address as the VRRP IPv6 address on the Mobility Master and the managed devices.

WebCC

Support for Clearing WebCC Statistics on Managed Devices

Starting from AOS-W 8.2.1.0, you can clear the WebCC statistics from managed devices using the **clear web-cc md stats** command.

WebUI

Source Address Field Introduced Under DHCP settings

Starting from AOS-W 8.2.1.0, **Source Address** field is introduced under **DHCP Helpers** in the **Configuration** > **Interfaces** > **VLANs** > **IPv6** tab. This field is used to configure **DHCP Helpers** with specific IPv6 address of an interface VLAN that has multiple IPv6 addresses.

EAP-TLS Provisioning Parameter

Starting from AOS-W 8.2.1.0, the **EAP-TLS** option is added to the **Uplink authentication** parameter listed under **Configuration** > **Access Points** page of the WebUI.

Support for WLAN Forwarding Mode Options

Starting from AOS-W 8.2.1.0, new options, **Split-Tunnel** and **Bridge**, are added to the **Forwarding mode** drop-down list in the **WLANs > General** page.

This chapter describes the hardware platforms supported in AOS-W 8.2.1.0.

Switch Platforms

The following table displays the Switch platforms that are supported in AOS-W 8.2.1.0.

Table 4: *Supported Switch Platforms in AOS-W 8.2.1.0*

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

AP Platforms

The following table displays the AP platforms that are supported in AOS-W 8.2.1.0.

Table 5: *Supported AP Platforms in AOS-W 8.2.1.0*

AP Family	AP Model
OAW-AP90 Series	OAW-AP92, OAW-AP93
—	OAW-AP93H
—	OAW-AP103, OAW-AP103H

Table 5: *Supported AP Platforms in AOS-W 8.2.1.0*

AP Family	AP Model
OAW-AP100 Series	OAW-AP104, OAW-AP105
OAW-AP110 Series	OAW-AP114, OAW-AP115
OAW-AP130 Series	OAW-AP134, OAW-AP135
OAW-AP 170 Series	OAW-AP175AC, OAW-AP175AC-F1, OAW-AP175DC, OAW-AP175DC-F1, OAW-AP175P, OAW-AP175P-F1
OAW-AP200 Series	OAW-AP204, OAW-AP205
—	OAW-AP203H
—	OAW-AP205H
—	OAW-AP207
203R Series	OAW-AP203R, OAW-AP203RP
OAW-AP210 Series	OAW-AP214, OAW-AP215
OAW-AP 220 Series	OAW-AP224, OAW-AP225
—	OAW-AP228
OAW-AP270 Series	OAW-AP274, OAW-AP275, OAW-AP277
300 Series	OAW-AP304, OAW-AP305
—	OAW-AP303H

Table 5: *Supported AP Platforms in AOS-W 8.2.1.0*

AP Family	AP Model
OAW-AP310 Series	OAW-AP314, OAW-AP315
OAW-AP320 Series	OAW-APAP-324, OAW-AP325
OAW-AP330 Series	OAW-AP334, OAW-AP335
360 Series	OAW-AP365, OAW-AP367
—	OAW-RAP155, OAW-RAP155P
OAW-RAP100 Series	OAW-RAP108, OAW-RAP109
—	OAW-RAP3WN, OAW-RAP3WNP

Chapter 4
Regulatory Updates

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

For a complete list of countries and the regulatory domains in which the APs are certified for operation, refer to the Downloadable Regulatory Table or the DRT Release Notes at service.esd.alcatel-lucent.com.

The following default DRT file version is part of AOS-W 8.2.1.0:

- DRT-1.0_63516

This chapter describes the issues resolved in AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
103312	**Symptom:** A WebUI using certificate authentication returned an invalid value for a session cookie. This issue is resolved by setting an empty value for the session cookie when it is created. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	Web Server	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
126176	**Symptom:** LLDP requests from multiple clients triggered unnecessary wired authentication requests that failed. The fix ensures that unnecessary wired authentication requests are blocked. **Scenario:** This issue occurred when wired authentication was linked with MAC authentication. This issue was observed in managed devices running AOS-W 8.0.0.0.	LLDP	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
133304	**Symptom:** A user was unable to assign a static IP to a Remote AP using the WebUI. The fix ensures that the user can assign a static IP to a Remote AP. **Scenario:** This issue was observed in a Mobility Master running AOS-W 8.0.0.0 or later versions.	WebUI	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
134824 139171 142938 147661 147662 153682 154385 160315 161477	**Symptom:** A managed device crashed unexpectedly and while rebooting, it experienced additional exceptions. The log file listed the reason for the event as **kernel panic**. The fix ensures that when the managed device reboots, the debug details are stored so that the original cause of reboot can be identified. **Scenario:** This issue was observed in managed devices running AOS-W 8.0.0.0.	Switch-Platform	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
140695	**Symptom:** A newly added AP operated incorrectly on maximum EIRP value. The fix ensures that the AP uses the average of the EIRP values configured on the AP and that of the hardware. **Scenario:** This issue occurred during the initial bootup or factory reset of an AP. This issue was observed in APs running AOS-W 8.0.0.0 or later versions.	AirMatch	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
140779	**Symptom:** SNMP enterprise-specific traps did not contain the enterprise trap OID. The fix ensures that the traps contain the enterprise trap OID. **Scenario:** This issue was observed in a Mobility Master running AOS-W 8.2.0.0.	SNMP	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
143057	**Symptom:** The values displayed for the following parameters in the output of the corresponding **show** commands were inaccurate: ■ The **Channel Busy** value of **show ap debug radio-stats** ■ The **Utilization(%)** value of **show ap spectrum channel-metrics** Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP205H, OAW-AP210 Series, OAW-AP 220 Series, and OAW-AP277 access points running AOS-W 8.2.0.0 or later versions.	AP-Wireless	OAW-AP205H, OAW-AP210 Series, OAW-AP 220 Series, and OAW-AP277 access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0
151817	**Symptom:** After migration, the entries of the APs that were in DOWN status in the AOS-W 6.x.x.x setup were missing from the global AP database of AOS-W 8.x.x.x setup. The fix ensures that the global AP database is updated correctly. **Scenario:** This issue was observed in a Mobility Master running AOS-W 8.0.1.0 or later versions	Migration	All platforms	AOS-W 8.0.1.0	AOS-W 8.2.1.0
154899	**Symptom:** The **BLE Relay** process in a managed device crashed unexpectedly. The fix ensures that the **BLE Relay** process does not crash and the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.1.0.0 or later versions.	BLE	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
156484 171487 172129	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Unable to handle kernel paging request for data at address 0x00000000**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP200 Series access points running AOS-W 8.0.0.0.	AP-Platform	OAW-AP200 Series access points	AOS-W 8.0.0.0	AOS-W 8.2.1.0
158459	**Symptom:** An SNMP query in a managed device returned an incorrect value for the associated user count in an AP. The fix ensures that the SNMP query returns the correct value. **Scenario:** This issue was observed in APs running AOS-W 8.0.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
158719 158720	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (Intent:cause:register 56:86:50:2)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when an AP with two physical ports was connected to a switch, which led to a CPU stack overflow. This issue was observed in OAW-40xx Series and OAW-4x50 Series Switches running AOS-W 8.0.0.0 or later versions.	Switch -Datapath	OAW-40xx Series and OAW-4x50 Series Switches	AOS-W 8.0.0.0	AOS-W 8.2.1.0
160725 171492	**Symptom:** An AP crashed and rebooted unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when the TPM certificate was corrupted. This issue was observed in OAW-AP305 access points running AOS-W 8.2.0.0 or later versions.	AP-Platform	OAW-AP305 access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0
160793	**Symptom:** A client was unable to pass traffic and a VRRP failover occurred. The fix ensures that the client is able to pass traffic. **Scenario:** This issue occurred when the LACP striping IP was configured as the VRRP IP. This issue was observed in OAW-AP 220 Series and OAW-AP320 Series access points running AOS-W 8.0.0.0 or later versions.	AP Datapath	OAW-AP 220 Series and OAW-AP320 Series access points	AOS-W 8.0.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
160854	**Symptom:** Some voice clients failed to pass traffic because they did not receive an ARP response. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when CAC and aggregation were enabled on voice clients. This issue was observed in managed devices running AOS-W 8.0.0.0.	AP-Wireless	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
161825	**Symptom:** An IF MIB showed the same values for all interfaces. The fix ensures that the correct value for each interface is displayed. **Scenario:** This issue was observed in a Mobility Master running AOS-W 8.2.0.0 or later versions.	SNMP	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
162011	**Symptom:** VLAN interface was displayed as DOWN although the interface operstate was UP. The fix ensures that the VLAN interface state is displayed correctly. **Scenario:** This issue occurred due to a log error. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	Mesh	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
162021 167981	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Assertion failed! (pdev->ar_rx_ops->attn_msdu_done(rx_desc)):htt_rx_debug**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in access points running AOS-W 8.2.0.0.	AP-Wireless	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
162605	**Symptom:** A wireless client appeared to be active on two different APs at the same time because one of the APs failed to age out the client entry from its user table. The fix ensures that the AP ages out the client entry from its user table. **Scenario:** This issue occurred when the wireless client roamed from one AP to another AP that terminated on a different managed device. This issue was observed in OAW-AP200 Series access points running AOS-W 8.1.0.0 or later versions.	AP-Wireless	OAW-AP200 Series access points	AOS-W 8.1.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
162870	**Symptom:** Clients experienced a slow connection when an AP used a 4G modem for uplink. The fix ensures that clients get the optimal connection speed. **Scenario:** This issue was observed in OAW-AP203R, OAW-AP203RP, OAW-AP205, and OAW-AP205H access points running AOS-W 8.2.0.0 or later versions.	AP-Platform	OAW-AP203R, OAW-AP203RP, OAW-AP205, and OAW-AP205H access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0
162977 167907	**Symptom:** Incorrect roles were applied to the client after authentication. The fix ensures that the correct roles are applied. **Scenario:** This issue was observed in bridge users connected to APs. This issue was observed in APs running AOS-W 8.0.0.0 or later versions.	AP Datapath	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
163066	**Symptom:** A managed device rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	Switch-Datapath	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
163117	**Symptom:** When a factory-reset managed device joined a Mobility Master, it overwrote the 'trusted' attribute of Ethernet interfaces on the Mobility Master configuration. This issue is resolved by ensuring that only the port that gets the DHCP information during ZTP is overwritten with the 'trusted' attribute. **Scenario:** This issue occurred because, during ZTP, all ports were overwritten with the 'trusted' attribute in the setup file. This issue was not limited to any specific platform or AOS-W version.	Configuration	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0
163547 170184	**Symptom:** The console log of an AP displayed the **nul_get_max_amsdu_size(2126): WARN: AMSDU size is not explicitly configured** warning message. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in APs running AOS-W 8.1.0.0.	AP-Wireless	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
164073	**Symptom:** The SNMP trap messages incorrectly indicated that a client's location had changed. But the voice client was associated to an AP and did not make any call or roam. This issue is resolved by ensuring that an unconditional SNMP trap notification is sent only when a client entry is created for the first time; also, subsequent notifications are sent only when the client's location has changed. **Scenario:** This issue occurred when the voice client was registered to multiple SIP servers and sent SIP register messages. This issue was not limited to any specific platform and was observed in managed devices running AOS-W 8.0.0.0.	UCC	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
164338	**Symptom:** When an outdoor AP is powered up using an AF powered switch, the AP moved to APM mode. The fix ensures that the AP does not move to APM mode. **Scenario:** This issue occurred because the logic in the AP tried to shut down both radios if the power source was AF. A channel validation check was triggered assuming the radios were up and running and moved the AP to APM mode. This issue was observed in OAW-AP275 access points connected to managed devices running AOS-W 8.1.0.0.	ARM	OAW-AP275 access points	AOS-W 8.1.0.0	AOS-W 8.2.1.0
164388	**Symptom:** When IPM was enabled, the system LED displayed an amber light although no power restriction was applied. Improvements to the wireless driver resolved the issue. **Scenario:** This issue occurred because the IPM disabled an option that periodically checks the system power supply status. This issue was observed in access points running AOS-W 8.1.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0
164545 171736 174858	**Symptom:** The WebUI displayed an alert message, **WebCC licenses exceeded**, although no WebCC license was installed. The fix ensures that the alert message is displayed only when the WebCC feature is enabled. **Scenario:** This issue occurred when the WebCC feature was enabled and the number of AP licenses exceeded the WebCC limit. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	Licensing	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
164659	**Symptom:** The output of the **show ap debug dot11r efficiency** command displayed 0% as the value in the **Hit (%)** and **Miss (%)** columns. The fix ensures that the CLI output displays the correct values. **Scenario:** This issue occurred in managed devices operating in tunnel mode. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	Station Management	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
164986 167374	**Symptom**: The logs were flooded with multiple kernel print messages. The fix ensures that the managed device logs are not flooded with these messages. **Scenario:** The issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	AP Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
165900 171831	**Symptom:** For wired users, an ARP entry was not displayed on a managed device. The fix ensures that the ARP entry is displayed. **Scenario:** This issue occurred because the **inter-tunnel-flooding** parameter was disabled when the **interface tunnel** command was executed on the managed device. This issue was observed in managed devices running AOS-W 8.1.0.1 or later versions.	Switch-Datapath	All platforms	AOS-W 8.1.0.1	AOS-W 8.2.1.0
166154	**Symptom:** A user observed inconsistent GRE headers in DNS packets sent by Apple devices. The fix ensures that the flags are not set in the GRE header. **Scenario:** This issue was observed in a Mobility Master where the GRE tunnels were statically configured and keepalive was disabled. This issue was observed in a Mobility Master running AOS-W 8.2.0.0 or later versions.	Switch-Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
166183 169183	**Symptom:** An AP did not boot. When the AP was manually rebooted, it displayed the **bcm96xxx-wdt ff800428.watchdog: Watchdog timer stopped** message in the console log. The fix ensures that the AP boots correctly. **Scenario:** This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
166293	**Symptom:** Wired clients using bridge forwarding mode were unable to pass MAC authentication. The fix ensures that clients successfully pass MAC authentication. **Scenario:** This issue occurred when the clients were connected to IPv6 APs. This issue was not limited to any specific AP platform or AOS-W release version.	Authentication	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
166366	**Symptom:** Users were unable to delete multiple IPM entries in the **Configuration > System > Profiles > All Profiles > AP system** page of the WebUI. The fix allows users to delete multiple IPM entries simultaneously. **Scenario:** This issue occurred when users attempted to delete multiple IPM entries simultaneously. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	WebUI	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
166426 167050 170409	**Symptom:** A Mobility Master rebooted unexpectedly. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:60)**. The fix ensures that the Mobility Master works as expected. **Scenario:** This issue was observed in a Mobility Master running AOS-W 8.2.0.0.	Switch-Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
166596	**Symptom:** Clients connected to an AP were continuously in sleep mode. As a result, clients lost data connectivity for a few seconds before recovering automatically. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the AP lost synchronization with clients in the power save state. This issue was observed in OAW-AP215 access points running AOS-W 8.1.0.0 or later versions.	AP-Wireless	OAW-AP215 access points	AOS-W 8.1.0.0	AOS-W 8.2.1.0
166678	**Symptom:** A Remote AP authenticated a wired client without any credential check. This issue is resolved by deleting all Remote AP users with the same MAC address if they are wired clients and their ports are changed. **Scenario:** This issue occurred when a wired client that used a spoofed MAC address of an authenticated client was connected to a Remote AP. This issue was observed in Remote APs running AOS-W 8.1.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
166838	**Symptom:** The output of the **show ap debug radio-stats** command displayed incorrect values for Tx Data Bytes. The fix ensures that the output of the **show ap debug radio-stats** command displays the correct values for Tx Data Bytes. **Scenario:** This issue was observed in OAW-AP305 access points running AOS-W 8.1.0.0 or later versions.	AP-Wireless	OAW-AP305 access points	AOS-W 8.1.0.0	AOS-W 8.2.1.0
166865 169423	**Symptom:** The output of the **show ap debug radio-stats** command displayed incorrect values for Tx and Rx data bytes. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in 802.11ac or 802.11n clients that were connected to OAW-AP207 access points running AOS-W 8.2.0.0 or later versions.	AP-Wireless	OAW-AP207 access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0
166945	**Symptom:** An AP crashed unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Fatal exception**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP200 Series access points running AOS-W 8.2.0.0 or later versions.	AP-Wireless	OAW-AP200 Series access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0
166963 167520 167719 171713	**Symptom:** An AP rebooted unexpectedly due to an external watchdog reset. Also, the AP rebootstrapped due to a broken heartbeat tunnel. The fix ensures that the AP works as expected. **Scenario:** The issue was observed in OAW-AP207 access points running AOS-W 8.0.0.0 or later versions.	AP Datapath	OAW-AP207 access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0
167056	**Symptom:** The **Remote Intf** parameter in the output of the **show lldp neighbor** and **show ap lldp neighbors** commands displayed the port description TLV. The issue is resolved at both the AP side and managed device side in the following ways: ■ **AP fix**: Providing both port ID and port descriptions separately. ■ **Managed device fix**: Displaying only port number even when the port description is configured. **Scenario:** This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	LLDP	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
167089	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:2c)**. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.1.0.0 or later versions.	Switch-Datapath	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0
167111	**Symptom:** Some clients were unable to pass traffic although they received the IP address from the correct VLAN. This issue is resolved by making multiple control plane attempts to configure the ACL on the data plane. **Scenario:** This issue occurred when the netdestination configurations were updated. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
167454 168103	**Symptom:** The following GSM Section publish errors were observed in the log files: **uthmgr[3709]: <522310> <3709> <ERRS> |authmgr| auth_gsm_publish_ip_user_section: gsm_section_update failed for ip 15.111.201.84 mac 34:36:3b:d3:05:1a result error_htbl_key_not_found size 288**. The issue is resolved by removing the unnecessary GSM channel publish events. **Scenario:** This issue occurred when RADIUS accounting was enabled for the users. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
167467 174516	**Symptom:** A VRRP process crashed. Enhancements to the wireless driver fixed this issue. **Scenario:** This issue occurred when VRRP configurations were deleted and re-created using a script. This issue was observed in managed devices running AOS-W 8.2.0.0.	VRRP	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
167479 167829	**Symptom:** Managed devices rebooted unexpectedly without generating a core dump file. The fix ensures that the core dump is collected as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	Switch-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
167679	**Symptom:** A Mobility Master tried to reach the wrong IP address of an Airwave server. This issue is resolved by correcting the endianess of the IP address. **Scenario:** This issue occurred because of wrong endianess. This issue was observed in a Mobility Master running AOS-W 8.1.0.2.	SNMP	All platforms	AOS-W 8.1.0.2	AOS-W 8.2.1.0
167747 171565 172711	**Symptom:** An AP crashed and rebooted unexpectedly due to a firmware assert. The log file listed the reason for the event as **Unable to handle kernel NULL pointer dereference at virtual address**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when the debug logging and the core dump generation were halted. This issue was observed in OAW-AP325 access points running AOS-W 8.0.0.0.	AP-Wireless	OAW-AP325 access points	AOS-W 8.0.0.0	AOS-W 8.2.1.0
167825 167826 171609	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:0:2c)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when OAW-AP205 access point was added on to the managed device. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	Switch-Datapath	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
167919	**Symptom:** A scanner declined the action frames sent by APs. This resulted in poor wireless performance. Enhancements to the wireless driver resolved the issue. **Scenario:** This issue was observed in OAW-AP205, OAW-AP210 Series, OAW-AP 220 Series, and OAW-AP270 Series access points running AOS-W 8.2.0.0 or later versions.	AP-Wireless	OAW-AP205, OAW-AP210 Series, OAW-AP 220 Series, and OAW-AP270 Series access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0
168039	**Symptom:** Users were unable to connect to VIA. The fix ensures that the users connect to VIA. **Scenario:** This issue occurred when an incorrect value for **NAS-Port-Type** was sent for VIA web authentication. This issue was observed in managed devices running AOS-W 8.1.0.0 or later versions.	RADIUS	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
168060 173578 173582	**Symptom:** The **authentication** process in a managed device crashed multiple times. The fix ensures that the **authentication** process does not crash. **Scenario:** This issue occurred when per-user bandwidth contract was enabled. This issue was observed on managed devices running AOS-W 8.1.0.2 or later versions.	Base OS Security	All platforms	AOS-W 8.1.0.2	AOS-W 8.2.1.0
168157 170007 173928 174042	**Symptom:** The output of the **show ap mesh active** command displayed the following: ■ A mesh portal working in 2.4 GHz mode ■ The mesh point EIRP and maximum EIRP values as 0 But the **flex-radio** mode in the **ap system-profile** was configured as **2.4GHz-and-5GHz**. The fix ensures that the mesh portal works in the configured mode and the output of the command displays the correct EIRP and maximum EIRP values. **Scenario:** This issue was observed in access points running AOS-W 8.0.0.0.	Mesh	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
168170	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP315 and OAW-AP325 access points running AOS-W 8.2.0.0 or later versions.	AP-Wireless	OAW-AP315 and OAW-AP325 access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0
168279 172750	**Symptom:** The configured bandwidth contracts were not applied for some clients. The fix ensures that clients do not exceed the contract speed. **Scenario:** This issue occurred when user role derivation was delayed after a MAC authentication. This issue was observed in managed devices running AOS-W 8.0.0.0	Base OS Security	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
168492 175310	**Symptom**: A Mobility Master displayed the error, **mDNS proxy runtime error at ag_send_packet_unicast 1105 Packet send failed error**. The fix ensures that the mDNS proxy runtime error is not seen on the Mobility Master. **Scenario**: This issue was observed in a Mobility Master running AOS-W 8.2.0.0 or later versions.	AirGroup	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
168499 168711	**Symptom:** APs in AM-mode intermittently switched back to the AP-mode. The fix ensures that the APs do not randomly switch from their configured mode. **Scenario:** This issue occurred due to a mismatch between the current operating bandwidth and the configured bandwidth on the AP when scanning a 40 MHz radio channel. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	ARM	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
168551 169669	**Symptom:** An AP crashed unexpectedly. The log file listed the reason for the event as **<0>[274540.243478] NMI watchdog: BUG: soft lockup - CPU#0 stuck for 22s! [sapd:1676]**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred during a cluster failover. This issue was observed in access points running AOS-W 8.2.0.0 or later versions.	AP Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
168692	**Symptom:** A client connected to a Mobility Master Hardware Appliance was unable to obtain a DHCP IP address after the initial setup wizard was launched. The issue is resolved by enabling the DHCP service in the Mobility Master Hardware Appliance. **Scenario:** This issue occurred because the DHCP service was disabled in the Mobility Master Hardware Appliance. This issue was observed in a Mobility Master Hardware Appliance running AOS-W 8.1.0.0 or later versions.	DHCP	Mobility Master Hardware Appliance	AOS-W 8.1.0.0	AOS-W 8.2.1.0
168697	**Symptom:** The WebUI did not display the correct count of the APs that operated in AM mode. The fix ensures that the WebUI displays the correct count of the APs in AM mode. **Scenario:** This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	Monitoring	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
168795	**Symptom:** A WebCC URL cloud lookup failed on a managed device. The log file listed the reason for the event as **<ERRS> |web_cc| web_cc_callback: URL lookup failed**. The fix ensures that the WebCC URL cloud lookup is successful. **Scenario:** This issue occurred when WebCC was enabled. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	WebCC	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
168798 175902	**Symptom:** An **authentication** process crashed in a managed device. The fix ensures that the **authentication** process does not crash. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.1 in a cluster topology.	Base OS Security	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0
168888	**Symptom:** False radar events were detected on an AP. The fix ensures that false radar events are not detected. **Scenario:** This issue occurred when DFS was enabled on the AP. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AP-Wireless	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
168909	**Symptom:** The noise floor value in a DFS channel was higher than that expected. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when ARM scanning was enabled. This issue was observed in OAW-AP315 and OAW-AP335 access points running AOS-W 8.2.0.0 or later versions.	AP-Wireless	OAW-AP315 and OAW-AP335 access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0
168984 170072 173647 174375 174998	**Symptom:** A managed device failed to update the syslog server. The issue is resolved by enhancing the logging mechanism. **Scenario:** This issue occurred because the syslog file size increased due to excess and incorrect logging from the managed device. This issue was observed in managed devices running AOS-W 8.2.0.2 or later versions.	Switch-Platform	All platforms	AOS-W 8.2.0.2	AOS-W 8.2.1.0
169012	**Symptom:** Multizone was not enabled on an AP. The fix ensures that although the AP has not acquired the RFP license, the MultiZone remains enabled. **Scenario:** This issue occurred when RFP was enabled after assigning MultiZone profile to an AP group. This issue was observed in a cluster running AOS-W 8.2.0.0.	AP Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169091	**Symptom:** The **configuration** process failed in the startup wizard. The issue is resolved by sending the value selected by the user instead of the default value for Port mode and Port. **Scenario:** This issue was observed when a non-default port was used for the Mobility Master to communicate with the managed device. This issue was not limited to any specific managed device model or AOS-W version.	WebUI	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
169105	**Symptom:** The WebUI startup wizard displayed an error - **answer 'PST' is not valid.** The fix ensures that the user's timezone is selected if a timezone is not specified. **Scenario:** This issue occurred when a timezone was not specified. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	WebUI	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
169111	**Symptom**: In the startup wizard of a managed device, some of the configuration options were not displayed when the value for the **Connection to mobility master** parameter was modified. The fix ensures that all the configuration parameters are displayed. **Scenario**: This issue was observed in a Mobility Master running AOS-W 8.2.0.0 or later versions.	WebUI	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
169131 170473 171299 171823 175747	**Symptom:** The AppRF feature failed to block the traffic. The fix ensures that the AppRF feature works as expected. **Scenario:** This issue occurred when DPI classification and WebCC were enabled. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	Switch-Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
169184	**Symptom:** The managed devices continuously dropped the IPv6 traffic. The fix ensures that the traffic is uninterrupted. **Scenario:** This issue occurred when managed devices without a PEFNG license received packets from H323 VoIP clients. This issue was observed in managed devices running AOS-W 8.1.0.0.	Switch-Datapath	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169288	**Symptom:** An incorrect error message, **An internal system error has occurred at file aeroscout.c function rtls_send_message line 190 error sendto failed - e-101 l-74 ip-192.168.20.100 port-27425**, was displayed in the log files. The fix ensures that the correct error message is displayed. **Scenario:** This issue occurred when RTLS server was configured in the AP system profile. This issue was observed in APs running AOS-W 8.0.0.0 or later versions.	Air Management - IDS	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
169329	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **AP rebooted caused by internal watchdog reset**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP275, OAW-AP277, OAW-AP325, and OAW-AP335 access points running AOS-W 8.1.0.3 or later versions.	AP-Wireless	OAW-AP275, OAW-AP277, OAW-AP325, and OAW-AP335 access points	AOS-W 8.1.0.3	AOS-W 8.2.1.0
169416	**Symptom:** A client disconnected from an AP and did not reconnect. The status of the AP was displayed as **Unprovisioned, no such group in the data zone**. This issue is resolved by disabling the virtual AP of the zone which does not have the AP group. **Scenario:** This issue occurred when MultiZone was assigned to an AP group. This issue was observed in a cluster setup running AOS-W 8.2.0.0.	AP Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
169444	**Symptom:** BLE features such as beacon management and asset tracking did not function on a Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance. Enhancements to ble-relay resolved this issue. **Scenario:** This issue occurred because the **ble** process was not active in a Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance. This issue was observed in non-hardware Switches running AOS-W 8.2.0.0 or earlier versions.	BLE	Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance	AOS-W 8.2.0.0	AOS-W 8.2.1.0
169474	**Symptom:** Some wireless clients were unable to obtain IP address after roaming to a new AP. The fix ensures that the 802.11r clients obtain the IP address. **Scenario:** This issue occurred when an 802.11r client in tunnel-mode roamed to a new AP with VLAN derivation. This issue was not limited to any specific AP model or AOS-W release version.	AP-Wireless	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169494	**Symptom**: Clients were unable to connect to APs. The log file listed the reason for the event as **AP is resource constrained**. The fix ensures that the APs send an ageout interval to the **STM** process when the authentication is unsuccessful. **Scenario**: This issue occurred because the **STM** process was not notified after an unsuccessful authentication, which resulted in stale STA entries. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AP-Wireless	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
169526	**Symptom:** Database synchronization failed between a primary and a secondary Mobility Master. The fix ensures that database synchronization is successful. **Scenario:** This issue occurred when L2 synchronization and L3 synchronization were executed simultaneously. This issue was observed in a Mobility Master running AOS-W 8.2.0.0.	Database	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
169535	**Symptom:** A client was unable to view the custom captive portal page in a standby managed device. The fix ensures that the client can view the custom captive portal page in a standby managed device. **Scenario:** This issue occurred when a user added a new standby managed device which did not have the custom Captive Portal page. This issue was observed in managed devices running AOS-W 8.1.0.0 or later versions.	Database	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0
169622	**Symptom:** A syslog server reported the **aruba_change_channel 512 channel 6 mode 3 not found** error for some APs. This issue is resolved by reporting the **channel-not-found** error only when the AP is not in monitoring mode. **Scenario:** This issue was observed in OAW-AP314 and OAW-AP315 access points running AOS-W 8.2.0.0.	AP-Wireless	OAW-AP314 and OAW-AP315 access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0
169626	**Symptom:** An unwanted attribute (FIlter-ID) was sent to the RADIUS server in the interim accounting packets by a managed device. The fix ensures that RADIUS accounting interim update does not contain Filter-Id attribute for an IPv6 client. **Scenario:** This issue occurred when RADIUS interim accounting was enabled on the managed device. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	RADIUS	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
169631	**Symptom:** The WebUI of the Mobility Master displayed an incorrect count of APs and clients. The issue is resolved by reducing the ageout time of clients from 6 minutes to 3 minutes. **Scenario:** This issue was observed in Mobility Master and managed devices running AOS-W 8.1.0.0 or later versions.	WebUI	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0
169661	**Symptom:** The Site-to-Site crypto map failed to match the traffic selectors when the **ANY** subparameter was added to the **src-net** command. The fix ensures that the Site-to-Site crypto map matches the any-any traffic selectors. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.0 versions.	IPsec	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
169726	**Symptom:** An SNMP query to retrieve the total number of clients associated with a managed device returned an inflated count. This issue is resolved by ensuring that only the count of active clients associated with the managed device is retrieved. **Scenario:** The issue occurred when dormant clients were also considered while retrieving the total number of clients. Hence, the SNMP query results did not tally with the value obtained through CLI or WebUI. This was observed in managed devices running AOS-W 8.0.0.0 or later versions.	SNMP	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0
169973	**Symptom:** Some IAP clients incorrectly derived the logon role on a Mobility Master and failed to pass traffic. The fix ensures that the OAW-IAP users derive the correct role. **Scenario:** This issue occurred when a heavy load was encountered in an IAP tunnel. This issue was observed in managed devices running AOS-W 8.1.0.0 or later versions.	Switch-Datapath	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0
170002	**Symptom:** An AP crashed and rebooted unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue occurred due to a race condition in the WLAN firmware. This issue was observed in 300 Series access points running AOS-W 8.2.0.0 or later versions.	AP-Wireless	300 Series access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
170056	**Symptom:** WebUI-based image upgrade for some image files using the **Local File** option failed. The fix ensures that the WebUI-based image upgrade is successful. **Scenario:** This issue occurred when the image upgrade was attempted using Chrome or Safari, but not while using Firefox. This issue was not limited to any specific platform or AOS-W version.	Upgrade	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
170085	**Symptom:** The **Transmit EIRP** values configured in the 802.11a and 802.11g radio profiles were lost and reset to the default value (15 dBm) after a managed device reload. The fix ensures that the configured **Transmit EIRP** values are retained. **Scenario:** This issue occurred only when the **Transmit EIRP** value was set to either 51 dBM or 127 dBm in the radio profile. This issue was observed in APs running AOS-W 8.2.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
170116	**Symptom: Slog_flash** process crashed multiple times and generated the core files frequently. The fix ensures that the crash does not occur. **Scenario:** This issue occurred when a USB with no storage space was inserted into a OAW-40xx Series Switch. This issue was observed in OAW-40xx Series Switches running AOS-W 8.1.0.2 or later versions.	Cluster-Manager	OAW-40xx Series Switch	AOS-W 8.1.0.2	AOS-W 8.2.1.0
170136	**Symptom**: An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **softlockup: hung tasks**. The fix ensures that the AP does not crash and reboot unexpectedly. **Scenario**: This issue was observed in OAW-AP310 Series and OAW-AP320 Series access points running AOS-W 8.2.0.0 or later versions.	AP Datapath	OAW-AP310 Series and OAW-AP320 Series access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0
170203 170832	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **Fatal exception in interrupt @ ol_rx_flush_handler+0x40/0x118 [umac] / ol_rx_indication_handler**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP305 access points running AOS-W 8.2.0.0 or later versions.	AP-Wireless	OAW-AP305 access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0
170275	**Symptom:** A logout window popped up incorrectly after a successful captive portal authentication although the **logout-popup-window** parameter was disabled in the captive portal profile. **Scenario:** This issue was observed in a Mobility Master running AOS-W 8.2.0.0 or later versions.	Captive Portal	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
170389	**Symptom:** When an AP rebooted, there was an increase in the number of kernel messages, with severity as critical. The fix ensures that the severity level of the kernel messages is reduced. **Scenario:** This issue was observed in APs running AOS-W 8.1.0.4 or later versions.	AP-Platform	All platforms	AOS-W 8.1.0.4	AOS-W 8.2.1.0
170425	**Symptom:** Clients were requested to increase the maximum interim accounting interval, because the default timer value increased the workload of a managed device and captive portal. The issue was resolved by increasing the upper limit of timeout value to 60 minutes. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
170522	**Symptom:** APs rebooted unexpectedly at various locations due to a random memory corruption. The fix ensures that the APs do not crash. **Scenario:** This issue was observed in access points running AOS-W 8.0.0.0 or later versions. **Duplicates:** 167229, 167548, 167831, 167864, 168537, 168658, 168972, 168973, 169050, 169078, 169199, 169563, 169712, 170137, 170202, 170252, 170431, 170786, 170823, 170824, 170834, 170914, 170948, 171189, 171231, 171499, 171697, 171919, 171935, 172894, 172897, 172958, 172961, 173211, 173333, 173497, 173777, 173786, 173942, 173970, 174021, 174120, 174124, 174171, 174296, 174642, 174710, 174720, 175226, and 175415.	AP-Wireless	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
170569	**Symptom:** Stale ARP entries were observed in the route cache table of cluster nodes. The fix ensures that stale entries are deleted appropriately. **Scenario:** This issue was observed in a cluster setup running AOS-W 8.0.0.0 or later versions.	Switch-Datapath	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
170659	**Symptom:** Sometimes, the bulk user download process failed on a cluster. The log file listed the reason for the event as, **<ERRS> |authmgr| System encountered an internal communication error. Error occurred when message is being sent from source application authmgr destination application sibyte_raw at file message.c function send_message_sibyte line 8284**. The fix ensures that the bulk user download process downloads only six users at a time to avoid this error. **Scenario:** This issue occurred when there were more than 6 user entries in a bulk user download message. This issue was observed in a cluster setup running AOS-W 8.2.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
170693 171762	**Symptom:** The following error messages were observed in managed devices in a cluster setup: **<ERRS> |authmgr| Datapath-UserAction (IPv4/L2) failed, No error handling**. The fix ensures that the error messages are not displayed unnecessarily. **Scenario:** This issue was observed in a cluster setup running AOS-W 8.2.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
170747	**Symptom:** The **arci-cli-helper** process was intermittently seen to be taking higher than usual CPU cycles. This issue is resolved by ensuring that the socket descriptor is closed when no data is received. **Scenario:** This issue occurred when existing TCP sessions to **arci-cli-helper** were not gracefully shut down due to which the socket descriptors were not cleared. This issue was observed in managed devices running AOS-W 8.2.0.0.	Monitoring	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
170813	**Symptom:** Some clients failed to associate with an 802.1X SSID after an AP failed over to the LMS from the backup LMS. This issue is resolved by clearing the stale configuration entries in the AP driver log after a failover. **Scenario:** This issue occurred when 802.11r configuration was enabled on the backup LMS but not on the LMS. This issue was not limited to any specific managed device model or AOS-W release version.	AP-Platform	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
170816	**Symptom:** A certificate-based OAW-RAP failed to come up. The fix ensures that the following events take place: ■ The OAW-RAP attempts authentication against all authentication servers that are part of an authentication server group. ■ The OAW-RAP attempts authentication starting from the first authentication server in the authentication server group if authentication fails. **Scenario:** This issue occurred when a OAW-RAP failed to authenticate against all authentication servers that were part of an authentication server group. Although authentication failed, the OAW-RAP stored the name of the last authentication server and attempted other authentication requests against the same server. This issue was observed in Remote APs running AOS-W 8.2.0.0 or later versions.	Certificate Manager	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
170872 172034 172573	**Symptom:** A Mobility Master crashed due to a memory corruption in the **AirGroup** process. The fix ensures that the memory corruption does not occur. **Scenario:** This issue occurred when a high volume of SSDP packets were received from the same MAC address but with different IP addresses. This issue was observed in Mobility Master running AOS-W 8.1.0.3 or later versions.	AirGroup	All platforms	AOS-W 8.1.0.3	AOS-W 8.2.1.0
170903 174289	**Symptom**: APs failed to broadcast SSIDs after a managed device was upgraded. The fix ensures that the AP broadcasts the SSIDs after a managed device is upgraded. **Scenario**: This issue occurred because the SSIDs were lost whenever a broken mesh link was re-established. This issue was observed in OAW-AP274 and OAW-AP275 access points running AOS-W 8.2.0.0 or later versions.	Mesh	OAW-AP274 and OAW-AP275 access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0
170916	**Symptom:** The DNS server IP address was reserved as master candidates. In addition, it was displayed as HA standby even though HA is disabled. The fix ensures that the resolved IP addresses are taken as master candidate and HA standby is displayed only when HA is enabled and standby IP configuration is synchronized with the managed device. **Scenario:** This issue was observed in access points running AOS-W 8.2.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
170931	**Symptom:** A standby managed device displayed incorrect EIRP and MaxEIRP values for some APs. The fix ensures that the managed device displays the correct EIRP and MaxEIRP values for all the APs. **Scenario:** This issue occurred when an AP detected more than 32 neighboring radios. This issue was observed in managed devices running AOS-W 8.2.0.1.	AP-Platform	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0
170936 172424	**Symptom:** A user with AP provisioning role was unable to provision APs through the WebUI. The fix ensures that the user can provision APs through the WebUI. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	WebUI	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
171001 171121	**Symptom:** Some stale ARP entries for clients on L2 VLAN did not age out and were found in the datapath route cache. This issue is resolved by ensuring that ARP entries are not added during OFC- or OFA-initiated ARP exchanges. **Scenario:** This issue occurred when the datapath route cache ARP entries and the kernel ARP entries were not synchronized. This issue was not limited to any specific platform or AOS-W version.	Switch-Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
171093	**Symptom:** An AP crashed and rebooted unexpectedly. The log file for the event listed the reason as **Critical process /aruba/bin/sapd [pid 30240] DIED**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when an adhoc network advertising a valid SSID was detected by the AP under the following configuration conditions: ■ The WMS was disabled. ■ The **detect-valid-ssid-misuse** and **protect-ssid** parameters were enabled in the **ids unauthorized-device-profile**. This issue was observed in OAW-AP325 access points running AOS-W 8.0.0.0 or later versions.	Air Management - IDS	OAW-AP325 access points	AOS-W 8.0.0.0	AOS-W 8.2.1.0
171099	**Symptom:** The standby User Anchored Controllers (S-UAC) in a cluster setup failed to track the correct VLAN usage count for dormant clients. The fix ensures that the VLAN usage counters are updated correctly. **Scenario:** This issue occurred when redundancy was enabled. This issue was observed in a cluster setup running AOS-W 8.2.0.0 or later versions.	Station Management	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171230	**Symptom:** Clients experienced intermittent packet loss. This issue is resolved by setting a limit on the number of retries when the client is unresponsive. **Scenario:** This issue occurred when some clients did not send a deauthentication or disassociation request to an AP and became unresponsive. The AP attempted to communicate with the unresponsive clients and created an RTS and BAR storm in the network. Hence, other clients in the network experienced intermittent packet loss. This issue was observed in OAW-AP205, OAW-AP215, and OAW-AP225 access points running AOS-W 8.2.0.0 or later versions.	AP-Wireless	OAW-AP205, OAW-AP215, and OAW-AP225 access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0
171233	**Symptom:** A Site-to-Site VPN failed to come up. The fix ensures that the datapath route-cache entry is deleted when the corresponding security association related to a 32-bit destination network mask is deleted and the Site-to-Site VPN comes up as expected. **Scenario:** This issue occurred when the IKE/IPsec security association related to a 32-bit destination network mask was broken but the corresponding datapath route-cache entry persisted. This issue was observed in managed devices running AOS-W 8.1.0.0.	IPsec	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0
171241	**Symptom:** Users were not allowed to enter IPsec key length that exceeded 7-8 characters. This issue is resolved by making internal code changes that allows 6-64 characters. **Scenario:** This issue occurred when a user tried to configure an IPv4 or IPv6 address of a managed device for PSK authentication. This issue was observed in a managed device running AOS-W 8.2.0.1.	WebUI	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0
171316	**Symptom:** An error, **dot1x_gsm_set_pmkcache(): GSM: Failed to publish PMK-cache object. Error:error_no_free_slots** was frequently displayed on a managed device when PMK cache GSM channel was full. The fix ensures that the error message is not displayed on the managed device. **Scenario:** This issue was observed in a cluster setup running AOS-W 8.2.0.1.	Base OS Security	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171324	**Symptom:** Some authentication servers disappeared from the server group that was configured on a managed device. The fix ensures that re-ordering the servers or server rules in a server group does not delete the authentication servers. **Scenario:** This issue occurred when authentication servers or server rules in a server group were re-ordered from the Mobility Master WebUI. This issue was observed in managed devices running AOS-W 8.2.0.1.	Configuration	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0
171347 173138	**Symptom:** In the WebUI, the APs operating in AM mode were not counted in the **Configurations > AP Group** page of the managed device although the status of these APs were displayed as UP in the **Dashboard > Access Points** page of the Mobility Master. The fix ensures that the APs are counted in the **Configurations > AP Group** page. **Scenario:** This issue occurred when APs changed to AM mode. This issue was observed in managed devices running AOS-W 8.2.0.1 or later versions.	Monitoring	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0
171382 174540	**Symptom:** The signal strength of the 2.4g radio in an AP reduced to a low value unexpectedly. The fix ensures that the AP retains the correct radio signal strength. **Scenario:** This issue was observed in OAW-AP207 access points running AOS-W 8.1.0.4.	AP-Platform	OAW-AP207 access points	AOS-W 8.1.0.4	AOS-W 8.2.1.0
171392	**Symptom:** Configuration involving netdestinations and ACLs using netdestinations caused a datapath module crash on a managed device. The fix ensures that the process does not crash. **Scenario:** This issue occurred due to the debug statements that were printed when the ACLs were applied on the traffic. This issue was observed in managed devices running AOS-W 8.2.0.1.	Switch-Datapath	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0
171398	**Symptom:** The captive portal page did not display the correct background and also the image was missing. The fix ensures the captive portal page displays the correct background and the image. **Scenario:** This issue occurred when the captive portal profile name exceeded the maximum limit. This issue was observed in a managed device running AOS-W 8.2.0.0 or later versions.	Captive Portal	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171411 175624	**Symptom:** An unexpected STM runtime error was displayed in the logs. The fix ensures that the error log is printed only when there is a valid error code. **Scenario:** This issue occurred when the ARM statistics health update was in progress. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	Station Management	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0
171433 173001	**Symptom:** The **show running config** command output indicated that ADP was enabled on a managed device though it was disabled from the Mobility Master. This issue is resolved by ensuring that the **STM** process is updated correctly after a restart. **Scenario:** This issue occurred either after an **STM** process restart or when a managed device rebooted. This issue was observed in a Mobility Master running AOS-W 8.0.1.0 or later versions.	Station Management	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0
171498	**Symptom:** An AP crashed unexpectedly. The log file listed the reason for the event as **AP process crash (core file: core.rapper.18-64-72-cf-e6-62.AP-334.62115)**. The fix ensures that the AP drops the unwanted IKE request packets to avoid the crash. **Scenario:** This issue occurred when the AP was flooded with VPN requests. This issue was observed in OAW-AP334 and OAW-AP335 access points running AOS-W 8.2.0.1.	AP-Platform	OAW-AP334 and OAW-AP335 access points	AOS-W 8.2.0.1	AOS-W 8.2.1.0
171502	**Symptom:** The **ip helper-address** command failed when executed on non-device nodes from a Mobility Master. The fix ensures that the **ip helper-address** command can be executed from non-device nodes. **Scenario:** This issue occurred because the command could be executed only on device nodes. This issue was observed in a Mobility Master running AOS-W 8.2.0.1 or later versions.	DHCP	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0
171580 172626	**Symptom:** When a user upgraded from AOS-W 8.2.0.0. to AOS-W 8.2.0.1, an AP entry appeared twice in the aggregation node level. The fix ensures that there is only entry in the aggregation node level**.** **Scenario:** This issue occurred because the **Mon-serv** manager updated an existing AP as well as created it once again in the monitoring database. This issue was observed in a cluster setup with APs terminating on them, but is not restricted to any specific AOS-W version.	Monitoring	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171582	**Symptom:** The allowed VLAN list on a port channel interface was missing from a managed device after upgrading the image and executing the **ccm-debug full-config-sync** command for a full configuration synchronization. The fix ensures that the allowed VLAN list on the port channel is displayed after upgrading the image. **Scenario:** This issue occurred when a managed device was upgraded from AOS-W 8.1.0.1 to AOS-W 8.1.0.4. The issue was observed in managed devices running AOS-W 8.1.0.4.	Configuration	All platforms	AOS-W 8.1.0.4	AOS-W 8.2.1.0
171587	**Symptom:** A managed device falsely detected a FATA-jack attack and raised an IDS event for clients that used 802.11r and initiated a re-association request. This issue is resolved by checking for authentication algorithm values greater than 3. **Scenario:** This issue was observed when 802.11r (Fast BSS Roaming) was enabled and supported clients roamed using WPA authentication algorithm 2. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	Air Management - IDS	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
171614 172310 174525 175401	**Symptom:** The **datapath** process on a managed device crashed. The log file listed the reason for the event as **Reboot Cause: Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. The fix ensures that the **datapath** process does not crash due to invalid memory access. **Scenario:** This issue occurred due to an invalid memory access. This issue was observed in managed devices running AOS-W 8.1.0.4.	Switch-Datapath	All platforms	AOS-W 8.1.0.4	AOS-W 8.2.1.0
171680	**Symptom:** A Mobility Master lost the masterip configuration for devices after upgrading. Due to this, the managed device became the Master from standby. The fix ensures that the device synchronization is successful. **Scenario:** This issue was observed in a cluster setup running AOS-W 8.1.0.4.	Configuration	All platforms	AOS-W 8.1.0.4	AOS-W 8.2.1.0
171705	**Symptom:** The RADIUS authentication failed after upgrading a Mobility Master to AOS-W 8.2.0.1 when managed devices are in a cluster. The fix ensures that the RADIUS authentication is successful. **Scenario:** This issue occurred when configuring **aaa** authentication servers for managed devices. This issue was observed in a cluster setup running AOS-W 8.2.0.1.	RADIUS	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171733	**Symptom:** The output of the **kernel coredump** command displayed an error when executed on a Mobility Master. This issue is resolved by increasing the crash kernel memory. **Scenario:** This issue occurred when the configuration was sent to the managed devices using the **kernel coredump** command. This issue was observed in managed devices running AOS-W 8.2.0.1.	Switch-Datapath	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0
171819	**Symptom:** Clients connecting to an AP failed to load the captive portal page. The fix ensures that the captive portal page loads successfully. **Scenario:** This issue occurred when the AP was configured as a Remote AP in split-tunnel forwarding mode. This issue was observed in OAW-AP200 Series, 300 Series, OAW-AP310 Series and OAW-AP320 Series access points running AOS-W 8.2.0.1.	AP Datapath	OAW-AP200 Series, 300 Series, OAW-AP310 Series and OAW-AP320 Series access points	AOS-W 8.2.0.1	AOS-W 8.2.1.0
171931	**Symptom:** Some APs reported a high packet rate value for the uplink traffic in the AMON message. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred because of inconsistent handling of NULL frames in the Rx data statistics. This issue was observed in 300 Series, OAW-AP303H, OAW-AP310 Series, OAW-AP320 Series, OAW-AP330 Series, and 360 Series access points running AOS-W 8.2.0.1 or later versions.	AP-Wireless	300 Series, OAW-AP303H, OAW-AP310 Series, OAW-AP320 Series, OAW-AP330 Series, and 360 Series access points	AOS-W 8.2.0.1	AOS-W 8.2.1.0
171976	**Symptom**: The output of the **show ap debug radio-stats** command did not display accurate counter values. The fix ensures that accurate values are displayed. **Scenario**: This issue occurred when 802.11ac and 802.11n clients were connected to APs. This issue was observed in OAW-AP207 access points running AOS-W 8.2.0.0 or later versions.	AP-Wireless	OAW-AP207 access points	AOS-W 8.2.0.0	AOS-W 8.2.1.0
172095	**Symptom:** Sometimes, the crash directory was missing from OAW-4x50 Series Switch. This issue is resolved by moving all crash files to a fixed location. **Scenario:** This issue occurred when a process in a OAW-4x50 Series Switch crashed. This issue was observed in OAW-4x50 Series Switches running AOS-W 8.0.0.0 or later versions.	Switch-Platform	OAW-4x50 Series Switches	AOS-W 8.2.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
172243 175921	**Symptom:** Although LLDP-MED configuration was enabled on all ports of an AP, it was disabled for ports E1 through E3. The fix ensures that LLDP-MED is enabled for ports E1 through E3. **Scenario:** This issue was observed in OAW-AP303H access points running AOS-W 8.2.0.1 or later versions.	AP-Platform	OAW-AP303H access points	AOS-W 8.2.0.1	AOS-W 8.2.1.0
172279 175985	**Symptom:** Clients were unable to pass captive portal authentication. The fix ensures that the clients are able to pass captive portal authentication. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.2 or later versions.	Captive Portal	All platforms	AOS-W 8.2.0.2	AOS-W 8.2.1.0
172388	**Symptom:** A managed device failed to download certificates from the Mobility Master. The fix ensures that the certificates are imported to the managed device. **Scenario:** This issue occurred due to a mismatch in the object type defined in XML and profile manager. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	Certificate Manager	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
172462 173388	**Symptom**: The **Managed Network > Dashboard > Access Points** page in the WebUI displayed the status of an AP as UP although the AP was DOWN. The fix ensures that the WebUI does not display UP for the APs that are DOWN. **Scenario**: This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	WebUI	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
172468	**Symptom:** A client failed authentication against a RADIUS server. Enhancements made to the **authentication** process resolved this issue. **Scenario:** This issue occurred when the **authentication** process in a managed device could not assign a sequence-number to a RADIUS request. As a result, the managed device did not sent RADIUS requests to the RADIUS server. This issue was observed in managed devices running AOS-W 8.1.0.0.	RADIUS	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0
172506	**Symptom:** A managed device discarded the first TCP SYN packet when a client connected to an FTP server. The fix ensures that the managed device does not discard the first TCP SYN packet. **Scenario:** This issue occurred in a managed device with DPI enabled. This issue was observed in managed devices running AOS-W 8.2.0.0.	Switch-Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
172610 173537 174713 176560	**Symptom:** AP was not seen on a backup LMS, when both the active and standby LMS were rebooted and the backup LMS was restored with HA enabled. The fix ensures that the AP comes up on both the primary and backup LMS after a reboot. **Scenario:** This issue was observed when both the active and standby LMS were disconnected. This issue is not restricted to any Switch model or AOS-W version.	AP-Platform	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0
172638 174128	**Symptom:** A managed device rebooted multiple times. The log file listed the reason for the event as **Datapath timeout**. The fix ensures that the reboot does not occur. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.1 or later versions.	Switch-Datapath	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0
172647 172786	**Symptom:** A user was unable to move an existing configuration node to a new node. The fix ensures that the user is able to move a configuration node. **Scenario:** This issue occurred when the encrypted password was sent for validation. This issue was observed in managed devices running AOS-W 8.2.0.1 or later versions.	Configuration	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0
172703	**Symptom:** A Remote AP attempted to obtain an IPv6 address even though it had already obtained an IPv4 address. Hence the Remote AP failed to boot. The fix ensures that the Remote AP boots when it obtains either an IPv4 address or an IPv6 address. **Scenario**: This issue occurred in Remote APs with dual-stacked FQDN containing both IPv4 and IPv6 addresses. This issue was observed in Remote APs running AOS-W 8.2.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
172709 175404 176375	**Symptom:** The **Dashboard** > **Access Points** page on a Mobility Master failed to display the radio statistics for an AP. The fix ensures that the AP and radio statistics are displayed correctly. **Scenario:** This issue occurred because the status of the AP was DOWN when the Mobility Master monitoring database processed the radio statistics. This issue was observed in a Mobility Master running AOS-W 8.2.0.0 or later versions.	Monitoring	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
172740	**Symptom**: The **Dashboard > Controllers** and **Configuration > Controllers** page of the WebUI displayed an incorrect status of managed devices. The fix ensures that the WebUI displays the correct status of the managed devices. **Scenario**: This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	WebUI	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
172758	**Symptom:** The AP image preload operation failed when executed from a managed device. The fix ensures that the AP image preload operation works as expected. **Scenario:** This issue was observed in OAW-4750 Switches running AOS-W 8.1.0.0.	Switch-Platform	OAW-4750 Switches	AOS-W 8.1.0.0	AOS-W 8.2.1.0
172763	**Symptom:** A Mobility Master stopped sending traps to OmniVista 3600 Air Manager when the SNMP V3 Engine ID was configured. The fix ensures that the Mobility Master sends traps to OmniVista 3600 Air Manager. **Scenario**: This issue occurred when the SNMP V3 Engine ID value started with 8. This issue was observed in a Mobility Master running AOS-W 8.2.0.0 or later versions.	SNMP	Mobility Master	AOS-W 8.2.0.0	AOS-W 8.2.1.0
172788	**Symptom:** A query on the following SNMP OIDs each reported an incorrect value of zero: ■ **monAPInfoMonitorTime - 1.3.6.1.4.1.14823.2.2.1.6.7.1.1.1.6** ■ **monAPInfoInactivityTime 1.3.6.1.4.1.14823.2.2.1.6.7.1.1.1.7** The fix ensures that the query displays the correct value. **Scenario:** This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	Air Management-IDS	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
172803	**Symptom:** Clients were unable to connect to an AP. The log file listed the reason for the event as **UAC Down**. The fix ensures that the clients successfully connect to an AP. **Scenario:** This issue occurred when the LMS IP was configured as the VRRP IP with AP load balancing enabled. This issue was observed in a cluster setup running AOS-W 8.1.0.4.	AP Datapath	All platforms	AOS-W 8.1.0.4	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
172877	**Symptom:** A managed device rebooted unexpectedly. The log file listed the reason for the event as **datapath timeout**. The fix ensures that the managed device works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.0.	Switch-Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
172959	**Symptom:** The **Profmgr** process displayed as busy for few minutes on a managed device. The fix ensures that the **Profmgr** process state is displayed correctly. **Scenario:** This issue occurred when the **show config datastore** command was executed on the managed device. This issue was observed in managed devices running AOS-W 8.1.0.4 or later versions.	Configuration	All platforms	AOS-W 8.1.0.4	AOS-W 8.2.1.0
173009	**Symptom:** VIA profile failed to download on a stand-alone Switch after establishing a VPN connection. This issue is resolved by adding correct logic to check the VIA license in the **authentication** process. **Scenario:** This issue was observed in OAW-4005 stand-alone Switches running AOS-W 8.2.0.1 or later versions.	IPsec	OAW-4005 Switches	AOS-W 8.2.0.1	AOS-W 8.2.1.0
173145	**Symptom:** A timer on an AP expired in advance after a cluster failover caused the **SAPD** process to crash. The fix ensures that the **SAPD** process does not crash due to a cluster failover. **Scenario:** This issue occurred when an AP failed over to a backup LMS and then detected the LMS. This issue was observed in APs running AOS-W 8.0.0.0 or later versions.	AP-Platform	All platforms	AOS-W 8.1.0.4	AOS-W 8.2.1.0
173360	**Symptom:** Source NAT application was not effective on the voice traffic. The fix ensures that source NAT is effective for the voice traffic when OpenFlow is enabled. **Scenario:** This issue occurred when OpenFlow was enabled on a Mobility Master. This issue was observed in a Mobility Master running AOS-W 8.0.0.0 or later versions.	SDN-Platform	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
173404	**Symptom:** A managed device was unable to download the configuration from a Mobility Master and displayed the error, **CONTROLLER-IP/V6 NOT SET**. The fix ensures that the managed device is able to download the configuration file seamlessly. **Scenario:** This issue occurred only when Switch-ip is configured for a managed device through a bulkedit CSV file. This issue was observed in a Mobility Master running AOS-W 8.1.0.0 or later versions.	Switch - Platform	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0
173427	**Symptom:** APs displayed up with an ID flag in the AP database. The log file listed the reason for the event as **Error: Duplicate LLDP-MED application type "voice"**. The fix ensures that APs do not come up with an ID flag. **Scenario:** This issue occurred due to two voice applications in the AP LLDP profile. This issue was observed in access points running AOS-W 8.1.0.2.	AP-Platform	All platforms	AOS-W 8.1.0.2	AOS-W 8.2.1.0
173436	**Symptom:** The **mcellsolverstart** process crashed in a Mobility Master unexpectedly. This issue is resolved by updating the DB schema. **Scenario:** This issue occurred as the DB schema in the Mobility Master was outdated. This issue was observed in a Mobility Master running AOS-W 8.2.0.0 or later versions.	AirMatch	All platforms	AOS-W 8.2.0.2	AOS-W 8.2.1.0
173468 173567 173656 173697 173922	**Symptom**: An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic - not syncing: Fatal exception NIP [e2dd2424] set_eth_loopback+0x1484/0x2060 [asap_mod]**. The fix ensures that the AP does not crash and reboot. **Scenario**: This issue was observed in OAW-AP335 access points running AOS-W 8.2.0.2 or later versions.	AP Datapath	OAW-AP335 access points	AOS-W 8.2.0.2	AOS-W 8.2.1.0
173535	**Symptom:** Users were unable to log into a Mobility Master using the WebUI. The issue is resolved by automatically rebooting the Mobility Master when the storage disk is remounted in read-only mode. **Scenario:** This issue occurred because the VM server storage disk was remounted in read-only mode on the Mobility Master Virtual Appliance due to disk timeouts. This issue was observed in Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance running AOS-W 8.0.0.0 or later versions.	Switch-Platform	Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance	AOS-W 8.0.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
173990	**Symptom:** A user was unable to upload a VIA installer package using the **Configuration > Services > VPN > VIA** page of the WebUI. The fix ensures that the VIA installer package upload is successful. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.2.	WebUI	All platforms	AOS-W 8.2.0.2	AOS-W 8.2.1.0
174017	**Symptom:** The **halt** command did not work in a managed device. The fix ensures that the **halt** command works as expected. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.0.	Switch-Platform	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
174193	**Symptom:** The **Configuration** > **Task** > **Provision new Campus APs** page displayed the message **AP Provisioning is currently being managed by Clearpass**. The fix ensures that the message is not displayed. **Scenario:** This issue occurred when the **default-cap** or **default-rap server-group** configuration was changed. This issue was observed in managed devices running AOS-W 8.2.0.1 or later versions.	WebUI	All platforms	AOS-W 8.2.0.1	AOS-W 8.2.1.0
174280	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **TIMED OUT WAITING FOR STOPPED EVENT**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP334 access points running AOS-W 8.2.0.2 or later versions.	AP-Wireless	OAW-AP334 access points	AOS-W 8.2.0.2	AOS-W 8.2.1.0
174375	**Symptom:** A managed device failed to update the syslog server. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when a managed device created incorrect log entries and the log file size increased. This issue was observed in managed devices running AOS-W 8.1.0.0 or later versions.	Switch-Platform	All platforms	AOS-W 8.1.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
174534	**Symptom**: HPE switches using the factory or TPM certificates were unable to establish an IPsec connection with a managed device. The fix ensures that the HPE switches can establish an IPsec connection with a managed device. **Scenario**: This issue occurred because the Certificate Policies extension OID of the HPE switch did not match with the preferred OIDs on the managed device. 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-W 8.2.1.0
174611	**Symptom:** The IPM priority was displayed incorrectly in the WebUI of a Mobility Master. The fix ensures that the IPM priority is displayed correctly in the WebUI. **Scenario:** This issue was observed in a Mobility Master running AOS-W 8.2.0.2.	Configuration	All platforms	AOS-W 8.2.0.2	AOS-W 8.2.1.0
174744	**Symptom:** The server certificate was not deleted when the web-server profile was deleted. The fix ensures that the server certificate is deleted. **Scenario:** This issue was observed in managed devices running AOS-W 8.2.0.2.	Certificate Manager	All platforms	AOS-W 8.2.0.2	AOS-W 8.2.1.0
174746	**Symptom:** Clients failed to receive RAs when the IPv6 proxy RA was enabled on a managed device. The issue is resolved by prioritizing the RA traffic appropriately. **Scenario:** This issue occurred because the IPv6 router solicitation packets were discarded when the managed device was overloaded with untrusted multicast traffic. This issue was observed in managed devices running AOS-W 8.2.0.0 or later versions.	IPv6	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
174756 174088	**Symptom:** Some Windows clients did not connect to an AP with VHT capabilities. The fix ensures that the clients connect to the AP that has VHT capabilities. **Scenario:** This issue occurred when a virtual AP was created in legacy mode without HT/VHT. This issue was observed in access points running AOS-W 8.0.0.0 or later versions.	AP-Wireless	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
174823 175163	**Symptom:** The **authentication** process crashed unexpectedly. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the **aaa test-server verbose** command was executed. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	Base OS Security	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
174864 175413 175448 175549	**Symptom:** A managed device crashed and rebooted unexpectedly. The log file listed the reason for the event as **datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:4)**. The fix ensures that the managed device works as expected. **Scenario:** This issue occurred when DPI was enabled. This issue was observed in managed devices running AOS-W 8.2.0.0.	Switch-Datapath	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
174943	**Symptom:** The **tx rate** value was displayed incorrectly when the **show ap debug radiostats** command was executed. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in 300 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points running AOS-W 8.2.0.1 or later versions.	AP-Wireless	300 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series	AOS-W 8.2.0.1	AOS-W 8.2.1.0
174979	**Symptom:** The size of the **ale.log** file size increased on a Mobility Master. This issue is resolved by updating only the consolidated data to the **ale.log** once a day. **Scenario:** This issue occurred due to frequent processing of AMON messages unnecessarily. This issue was observed in a Mobility Master running AOS-W 8.2.0.0 or later versions.	NBAPI	All platforms	AOS-W 8.2.0.2	AOS-W 8.2.1.0
175060	**Symptom:** The **Dashboard > Performance** page of a Mobility Master displayed the most significant digit of the total client count. The fix ensures that the **Dashboard > Performance** page displays the correct client count. **Scenario:** This issue was observed in a Mobility Master running AOS-W 8.2.0.0.	WebUI	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
175120	**Symptom:** The output of the **show ip route** command displayed a client's IP route address in reverse order. The fix ensures that the IP route address is displayed in correct order. **Scenario:** This issue occurred due to missing endianness of the IP route address in the Mobility Master Virtual Appliance. This issue was observed in a Mobility Master Virtual Appliance running AOS-W 8.2.0.2 or later versions.	IPsec	Mobility Master Virtual Appliance	AOS-W 8.2.0.2	AOS-W 8.2.1.0
175126 175128	**Symptom:** A Mobility Master incorrectly deleted the certificates uploaded in flash when deleting them from a child node device that had inherited these certificates. The fix ensures that an error is displayed when trying to delete an inherited certificate from a child node. **Scenario:** This issue occurred when there was no reference to the certificate being deleted in the local node. This issue was observed in a Mobility Master running AOS-W 8.2.0.0 or later versions.	Certificate Manager	All platforms	AOS-W 8.2.0.0	AOS-W 8.2.1.0
175240	**Symptom:** The **CTF MAC** field in the output of the **show ap remote debug uac-list** command displayed incorrect values. The fix ensures that the **CTF MAC** field displays the correct values. **Scenario:** This issue was observed in access points running AOS-W 8.2.0.2.	AP Datapath	All platforms	AOS-W 8.2.0.2	AOS-W 8.2.1.0

Table 6: *Resolved Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
175475 175727	**Symptom:** The **mDNS** process in a managed device displayed high memory utilization. This issue is resolved by sending ClearPass Policy Manager requests only for AirGroup users. **Scenario:** This issue occurred when AirGroup was disabled but a ClearPass Policy Manager request was sent for each authenticated user. This lead to a memory leak. This issue was observed in managed devices running AOS-W 8.2.0.2.	AirGroup	All platforms	AOS-W 8.2.0.2	AOS-W 8.2.1.0
175937	**Symptom:** A managed device crashed and rebooted unexpectedly without collecting the crash information. The log file listed the reason for the event as **Kernel Panic (Intent:cause:register 12:86:40:2)**. The fix ensures that the USB does not disconnect while collecting the core dump. **Scenario:** This issue occurred when the USB got disconnected while collecting the core dump. This issue was observed in managed devices running AOS-W 8.0.0.0 or later versions.	Switch-Platform	All platforms	AOS-W 8.0.0.0	AOS-W 8.2.1.0
176183	**Symptom:** The **mDNS** process crashed on a Mobility Master Virtual Appliance. This fix ensures that the **mDNS** process does not crash. **Scenario:** This issue occurred when a high memory address range was assigned to the timer. This issue was observed in a Mobility Master Virtual Appliance running AOS-W 8.2.0.2.	AirGroup	Mobility Master Virtual Appliance	AOS-W 8.2.0.2	AOS-W 8.2.1.0

This chapter describes the issues identified in AOS-W 8.2.1.0.

Table 7: *Known Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version
159921	**Symptom:** The **Dashboard > WAN** page of the Mobility Master WebUI 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
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:** Execute the **bootenv_backup.sh** script to clear the saved record.	AP-Platform	All platforms	AOS-W 8.1.0.0
167288	**Symptom:** A stand-alone Switch does not display the wired client icon, list, and count of users in the WebUI. **Scenario:** This issue is observed in stand-alone Switches running AOS-W 8.2.0.0. **Workaround:** None.	WebUI	All platforms	AOS-W 8.2.0.0
168180	**Symptom:** The **profmgr** process crashes when a single instance default profile is modified by the administrator in 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
168636	**Symptom:** Clients are unable to connect to a Switch from Aruba Central??? using SSH. **Scenario:** This issue is observed in OAW-4005 Switches running AOS-W 8.0.1.0 or later versions. **Workaround:** None.	Aruba Central???	OAW-4005 Switches	AOS-W 8.0.1.0

Table 7: *Known Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version
169827	**Symptom:** Encapsulated ARP packets with inner payload size lesser than 64 bytes are dropped by an Alcatel-Lucent HPE switch. **Scenario:** This issue occurs when the Alcatel-Lucent HPE switch is connected to a wired tunnelled node port of a managed device. This issue is observed in managed devices running AOS-W 8.1.0.4. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 8.1.0.4
170611	**Symptom:** A user is unable to disable TLS 1.0 and TLS 1.1 versions on a FIPS build within SSL protocol. **Scenario:** This issue is observed in managed devices running AOS-W 8.0.0.0 or later versions. **Workaround:** None.	Web Server	All platforms	AOS-W 8.2.0.0
171611	**Symptom:** A crypto map is incorrectly picked during IKE and IPsec negotiation on a managed device if **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. **Workaround:** Execute the **no vpn-peer peer-mac** command on the managed device.	IPsec	All platforms	AOS-W 8.1.0.4
172534	**Symptom:** WEP clients are unable to pass traffic on 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 setup running AOS-W 8.1.0.0 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 8.1.0.0
173083	**Symptom:** When configured as redundant Mobility Master, the label for the Mobility Master is incorrectly displayed as **Mobility Controller** in the WebUI. **Scenario:** This issue is observed in a Mobility Master running AOS-W 8.2.0.1. **Workaround:** None.	WebUI	All platforms	AOS-W 8.2.0.1
173816	**Symptom:** A managed device displays the **500 Internal Server Error** message when a user attempts local file upgrade. **Scenario:** This issue occurs with some image file sizes. This issue is observed in managed devices running AOS-W 8.2.0.1 **Workaround:** Use SCP, FTP, or TFTP to upgrade the managed devices.	Image Upgrade	All platforms	AOS-W 8.2.0.1

Table 7: *Known Issues in AOS-W 8.2.1.0*

Bug ID	Description	Component	Platform	Reported Version

174644
174925
	Symptom: AirGroup loses all the learned server and user details and also fails to learn any new user or server details.
	Scenario: This issue occurs whenever an AirGroup service or profile is modified. This issue is observed in AOS-W 8.2.0.0 or later versions.
	Workaround: Re-enable AirGroup on the node by using the following commands:
	`no airgroupprofile activate`
	`!`
	`airgroupprofile activate airgroupprofile <profile-name > mode <mode>`
	`!`
		AirGroup	All platforms	AOS-W 8.2.0.2

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 a Mobility Master 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
176444	**Symptom:** The startup wizard does not allow adding licenses to a stand-alone Switch. **Scenario:** This issue is observed in stand-alone Switches running AOS-W 8.2.1.0. **Workaround:** None.	Switch - Platform	All platforms	AOS-W 8.2.1.0

176998	**Symptom:** The client traffic is dropped when the **enforce-dhcp** parameter is enabled.
	Scenario: This issue occurs when clients roam from one AP to another AP that terminates on a different managed device and has no context of the client. The client does not initiate DHCP discovery after authentication, but sends traffic which is dropped by the managed device.
	Workaround:
	1. Disable **enforce-dhcp** parameter in the AAA profile using either the WebUI or the CLI:
	WebUI
	In the Managed Network node hierarchy, navigate to **Configuration > Authentication > AAA Profile**.
	Select an AAA Profile and clear the **Enforce DHCP** check box.
	CLI:
	Execute the following commands in the CLI:
	`(host) [mynode] (config) # aaa profile <default>`
	`(host) [mynode] (AAA Profile "<default>") # no enforce-dhcp`
	2. Renew the DHCP lease on the client if the traffic is blocked.
		Base OS Security	All platforms	AOS-W 8.2.1.0

Chapter 7
Upgrade Procedure

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 63 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 63 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 63 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 ArubaOS 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 62.

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 63 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 62.

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 63 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 63.
2. Verify that the control plane security is disabled.
3. Set the Switch to boot with the previously saved pre-AOS-W configuration file.
4. Set the Switch to boot from the system partition that contains the previously running AOS-W image.

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

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

Downgrading Using the WebUI

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

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

Downgrading Using the CLI

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

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

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

   or

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

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

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

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

Before You Call Technical Support

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

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

Appendix A
Glossary of Terms

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

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

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

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

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

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

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

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

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

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

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

802.11e
802.11e is an enhancement to the 802.11a and 802.11b specifications that enhances the 802.11 Media Access Control layer with a coordinated Time Division Multiple Access (TDMA) construct. It adds error-correcting mechanisms for delay-sensitive applications such as voice and video. The 802.11e

specification provides seamless interoperability between business, home, and public environments such as airports and hotels, and offers all subscribers high-speed Internet access with full-motion video, high-fidelity audio, and VoIP.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

EAP-MSCHAP
EAP Microsoft Challenge Handshake Authentication Protocol.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Gbps
Gigabits per second.

GBps
Gigabytes per second.

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

GHz
Gigahertz.

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

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

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

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

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

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

H2QP
Hotspot 2.0 Query Protocol.

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

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

HSPA
High-Speed Packet Access.

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

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

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

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

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

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

IEEE
Institute of Electrical and Electronics Engineers.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Kbps
Kilobits per second.

KBps
Kilobytes per second.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Mbps
Megabits per second

MBps
Megabytes per second

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

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

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

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

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

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

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

MHz
Megahertz

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

RAM
Random Access Memory.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

subnet
Subnet is the logical division of an IP network.

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

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

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

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

TAC
Technical Assistance Center.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

UI
User Interface.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

WWW
World Wide Web.

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

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

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

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

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