AOS-W 6.4.4.19

Alcatel·Lucent Enterprise

Release

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

The AOS-W 6.4.4.19 release notes includes the following topics:

- New Features on page 10 describes the features and enhancements introduced in this release.
- Regulatory Updates on page 12 lists the regulatory updates introduced in this release.
- Resolved Issues on page 13 describes the issues resolved in this release.
- Known Issues on page 19 describes the known and outstanding issues identified in this release.
- Upgrade Procedure on page 36 describes the procedures for upgrading a switch to this release.

Important Points to Remember

This section describes the important points to remember before you upgrade the switch to this release of AOS-W.

AirGroup

Support for Wired Users

Starting from AOS-W 6.4.3.0, AirGroup does not support trusted wired users.

AP Settings Triggering a Radio Restart

If you modify the configuration of an AP, those changes take effect immediately; you do not need to reboot the switch or the AP for the changes to affect the current running configuration. Certain commands, however, automatically force the AP radio to restart.

Table 2: *Profile Settings in AOS-W 6.4.x*

Profile	Settings
802.11a/802.11g Radio Profile	■ Channel ■ Enable Channel Switch Announcement (CSA) ■ CSA Count ■ High throughput enable (radio) ■ Very high throughput enable (radio) ■ TurboQAM enable ■ Maximum distance (outdoor mesh setting) ■ Transmit EIRP ■ Advertise 802.11h Capabilities ■ Beacon Period/Beacon Regulate ■ Advertise 802.11d Capabilities
Virtual AP Profile	■ Virtual AP enable ■ Forward Mode ■ Remote-AP operation
SSID Profile	■ ESSID ■ Encryption ■ Enable Management Frame Protection ■ Require Management Frame Protection ■ Multiple Tx Replay Counters ■ Strict Spectralink Voice Protocol (SVP) ■ Wireless Multimedia (WMM) settings ● Wireless Multimedia (WMM) ● Wireless Multimedia U-APSD (WMM-UAPSD) Powersave ● WMM TSPEC Min Inactivity Interval ● Override DSCP mappings for WMM clients ● DSCP mapping for WMM voice AC ● DSCP mapping for WMM video AC ● DSCP mapping for WMM best-effort AC ● DSCP mapping for WMM background AC

Table 2: *Profile Settings in AOS-W 6.4.x*

Profile	Settings
High-throughput SSID Profile	■ High throughput enable (SSID) ■ 40 MHz channel usage ■ Very High throughput enable (SSID) ■ 80 MHz channel usage (VHT)
802.11r Profile	■ Advertise 802.11r Capability ■ 802.11r Mobility Domain ID ■ 802.11r R1 Key Duration ■ key-assignment (CLI only)
Hotspot 2.0 Profile	■ Advertise Hotspot 2.0 Capability ■ RADIUS Chargeable User Identity (RFC4372) ■ RADIUS Location Data (RFC5580)

Supported Browsers

The following browsers are officially supported for use with the Web User Interface (WebUI) in this release:

- Microsoft Internet Explorer 10.x and 11 on Windows 7 and Windows 8
- Mozilla Firefox 23 or later on Windows Vista, Windows 7, Windows 8, and Mac OS
- Apple Safari 5.1.7 or later on Mac OS

Contacting Support

Table 3: *Contact Information*

Contact Center Online	
Main Site	http://enterprise.alcatel-lucent.com
Support Site	https://support.esd.alcatel-lucent.com
Email	ebg_global_supportcenter@al-enterprise.com
Service & Support Contact Center Telephone	

Contact Center Online	
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 enhancements are introduced in AOS-W 6.4.4.19.

AP-Wireless

Mute AP Radio

Starting from this release, the **rf dot11a-radio-profile** and **rf dot11g-radio-profile** commands include the **am-tx-mute** parameter. Enable the **am-tx-mute** parameter to prevent an AP that operates in the AM or spectrum mode from creating spurious transmissions during AP boot. By default, the **am-tx-mute** is disabled.

Enable the **am-tx-mute** parameter in the **rf dot11a-radio-profile** or **rf dot11g-radio-profile** command only for APs that operate in the AM or spectrum mode.

To enable the am-tx-mute parameter:

```
(host) (config) #rf dot11a-radio-profile default
(host) (config) (rf dot11a-radio-profile "default")#am-tx-mute
```

Remote AP

Enhancements in USB Initialization of 4G/LTE Modem

AOS-W allows you to configure two AP Name (APN) during USB initialization of the 4G/LTE modem. While the first APN initiates the connection to obtain an IP address, the second APN sends and receives data. Use semicolon (;) as a delimiter to create two separate strings for the APN configurations in the following commands under the AP provisioning profile:

```
(host) (config) #ap provisioning-profile <profile-name>
(host) (Provisioning profile "<profile-name>") #usb-init <APN1-string>; <APN2-string>
```

Example

The following sample configuration includes the string values for two APN configurations:

```
(host) (config) #ap provisioning-profile default
(host) (Provisioning profile "default") #usb-init "AT+CGDCONT=1,\"IP\",\"APN1\";1,1,\"APN2\""
```

You must obtain the APN from your ISP and ensure that each APN entry follows the manufacturer's AT command reference.

Firewall Visibility

FW_AGG Sessions Message Enhancement

A new field, **client mac address**, is added to the FW_AGG sessions message table to establish a relationship between the station MAC address and the application details.

GRE

Allow Unknown Unicast Packets

Starting from AOS-W 6.4.4.19, the **bcmc-optimization allow-unknown-unicast** parameter is introduced in the **interface vlan** command. When the **bcmc-optimization allow-unknown-unicast** parameter is enabled, a switch floods unknown unicast packets.

The **bcmc-optimization allow-unknown-unicast** parameter is optional and can be enabled only if the **bcmc-optimization** parameter is enabled.

If both **bcmc-optimization** and **bcmc-optimization allow-unknown-unicast** parameters are disabled, the switch does not flood any broadcast, multicast, or unknown unicast packet.

If only the **bcmc-optimization** parameter is enabled, the switch drops all broadcast, multicast, and unknown unicast packets.

If both **bcmc-optimization** and **bcmc-optimization allow-unknown-unicast** parameters are enabled, the switch drops only broadcast and multicast packets and floods the unknown unicast packets.

Use the following command to allow unknown unicast:

```
(host) (config-subif) #bcmc-optimization allow-unknown-unicast
```

Use the following command to disallow unknown unicast:

```
(host) (config-subif) #no bcmc-optimization allow-unknown-unicast
```

Periodic regulatory changes require modifications to the regulatory channel list supported by an AP. To view a complete list of channels supported by an AP for a specific country domain, access the CLI and execute the **show ap allowed-channels country-code <country-code> ap-type <ap-model>** command.

For a complete list of countries certified with different AP models, refer to the respective DRT release notes at service.esd.alcatel-lucent.com.

The following default Downloadable Regulatory Table (DRT) file version is part of AOS-W 6.4.4.19:

- DRT-1.0_66351

This chapter describes the issues resolved in AOS-W 6.4.4.19.

Table 4: *Resolved Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
154096	**Symptom:** The channel of a virtual AP was inconsistent after a radar event was detected. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when a bridge-always virtual AP which had disconnected from a switch detected a radar event on the channel and selected a new channel. This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.0 or later versions.	AP Regulatory	OAW-AP325 access points	AOS-W 6.5.2.0	AOS-W 6.4.4.19
156732 172812	**Symptom:** SAPD timeout error messages were observed for an AP in the switch logs. The fix ensures that the timeout messages are not logged in a switch. **Scenario:** This issue occurred when the backup LMS was not configured on the AP system profile. This issue is not limited to any specific AP model or AOS-W release version.	AP-Platform	All platforms	AOS-W 6.4.4.12	AOS-W 6.4.4.19
160308 161434	**Symptom:** A switch crashed and rebooted unexpectedly. The log file listed the reason for the event as **Nanny rebooted machine - low on free memory (Intent:cause:register 34:86:0)**. The fix ensures that the switch works as expected. **Scenario:** This issue occurred when a switch was running low on memory. This issue was observed in switches running AOS-W 6.4.4.12 or later versions.	Switch-Datapath	All platforms	AOS-W 6.4.4.12	AOS-W 6.4.4.19

Table 4: *Resolved Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
165535	**Symptom:** A client was unable to connect to an AP. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in APs running AOS-W 6.4.4.0 or later versions with WPA TKIP security.	AP-Wireless	All platforms	AOS-W 6.4.4.0	AOS-W 6.4.4.19
165788	**Symptom:** A user was unable to remove stale entries from a standby switch. The fix allows the user to delete stale entries from the standby switch. **Scenario:** This issue was observed in a standby switch running AOS-W 6.4.4.12 or later versions in a master-standby topology.	Station Management	All platforms	AOS-W 6.4.4.12	AOS-W 6.4.4.19
169131 170473 171299 171823 175747 177806	**Symptom:** AppRF failed to block traffic. The fix ensures that AppRF blocks the desired traffic. **Scenario:** This issue occurred when DPI and WebCC were enabled in a switch. This issue was observed in OAW-4x50 Series switches running AOS-W 6.4.4.15.	Switch-Datapath	OAW-4x50 Series switches	AOS-W 6.4.4.15	AOS-W 6.4.4.19
170249 172066 175830 175931 176688 179004 181990 182752	**Symptom:** A client was unable to connect to an AP. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the CPU utilization of an AP reached 100%. This issue was observed in OAW-AP100 Series access points running AOS-W 6.4.4.14 or later versions.	AP-Wireless	OAW-AP100 Series access points	AOS-W 6.4.4.14	AOS-W 6.4.4.19

Table 4: *Resolved Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
171230	**Symptom:** A client experienced intermittent packet loss. This issue is resolved by limiting the number of retries attempted when a client is unresponsive. **Scenario:** This issue occurred when a client 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 6.4.4.16 or later versions.	AP-Wireless	OAW-AP205, OAW-AP215, and OAW-AP225 access points	AOS-W 6.4.4.16	AOS-W 6.4.4.19
172801 175444 176229	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Kernel panic: Fatal exception**. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP225 access points running AOS-W 6.4.4.16 or later versions.	AP-Wireless	OAW-AP225 access points	AOS-W 6.4.4.16	AOS-W 6.4.4.19
173868	**Symptom:** A different user with the same static IP address failed to send or receive traffic when connected to an SSID. This issue is resolved by resetting the user information associated with the IP address and inheriting it from the client with the new MAC address. **Scenario:** This issue occurred when the **prohibit-ip-spoofing** parameter was disabled in the firewall settings. This issue was observed in switches running AOS-W 6.4.4.0 or later versions.	Base OS Security	All platforms	AOS-W 6.5.3.3	AOS-W 6.4.4.19
174943	**Symptom:** The **Tx rate** value was displayed incorrectly in the **show ap debug radiostats** command output. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue was observed in OAW-AP320 Series access points running AOS-W 6.4.4.0 or later versions.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.5.3.4	AOS-W 6.4.4.19

Table 4: *Resolved Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
175387	**Symptom:** APs blocked ARP requests which had the same IP address as that of local DHCP server of AP. The fix ensures the following: ■ AP datapath does not block the ARP request from the AP with the DHCP VLAN address. ■ If there is a wired or wireless client connected to AP and has the same IP address, the ARP reply is dropped by ARP as an ARP spoof. But, if this IP address does not belong to a client that is connected to AP, the ARP reply is forwarded. **Scenario:** This issue occurred when a route-cache entry was added with the AP local DHCP address and VLAN. But, when an ARP request which was with the same IP address as that of the AP's DHCP server was received by the AP, the AP datapath dropped the ARP request due to a mismatch in VLAN information. This issue was observed in APs running AOS-W 6.4.4.0 or later versions.	AP Datapath	All platforms	AOS-W 6.5.4.4	AOS-W 6.4.4.19
175669	**Symptom:** The **show ap active** command did not show any flag for an AP that was operating in restricted mode because of POE-AF. This issue is resolved by showing the p flag in the **show ap active** command for an AP that operates in restricted mode. **Scenario:** This issue was observed in access points running AOS-W 6.5.1.9.	AP-Platform	All platforms	AOS-W 6.5.1.9	AOS-W 6.4.4.19
176430	**Symptom:** Some APs sent ARP requests for a gateway with an incorrect IP address. The fix ensures that the APs send correct IP addresses for ARP request. **Scenario:** The issue occurred in the following scenarios: ■ When APs disconnected from the switch. ■ When the DHCP server was unreachable. ■ When the gateway was unreachable. This issue was observed in APs running AOS-W 6.4.4.16 or later versions.	AP Datapath	All platforms	AOS-W 6.4.4.16	AOS-W 6.4.4.19

Table 4: *Resolved Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
176607	**Symptom:** A client that was connected to an AP failed to obtain an IP address. The fix ensures that the client obtains an IP address. **Scenario:** This issue occurred due to a memory leak in the APs with onboard or USB-based BLE radios. This issue was observed in OAW-AP210 Series, OAW-AP220 Series, and OAW-AP320 Series access points running AOS-W 6.4.4.0 or later versions.	BLE	OAW-AP210 Series, OAW-AP220 Series, and OAW-AP320 Series access points	AOS-W 6.5.1.9	AOS-W 6.4.4.19
176902	**Symptom:** A switch dropped ARP response from a wired silent client behind an untrusted port. The fix ensures that the switch does not drop ARP response from silent clients behind untrusted ports. **Scenario:** This issue occurred when protect ARP spoofing was enabled and the wired client was connected behind untrusted port. Due to this, a switch deleted the datapath user entries of the client and the client became unreachable. This issue was observed in switches running AOS-W 6.4.4.16.	Switch-Database	All platforms	AOS-W 6.4.4.16	AOS-W 6.4.4.19
178016	**Symptom:** An AP detected false radar signals and changed its radio channel frequently. Enhancements to the wireless driver resolved this issue. **Scenario:** This issue occurred when the false radar type id was 36. This issue was observed in OAW-AP105 access points running AOS-W 6.4.4.0 or later versions.	AP-Wireless	OAW-AP105 access points	AOS-W 6.5.3.4	AOS-W 6.4.4.19

Table 4: *Resolved Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
178119	**Symptom:** A client was unable to connect to the AP. The fix ensures that the client was able to connect to the AP. **Scenario:** This issue occurred when the AP stopped broadcasting the configured SSID. This issue was observed in OAW-AP225 and OAW-AP325 access points running AOS-W 6.4.4.0 or later versions.	AP-Platform	OAW-AP225 and OAW-AP325 access points	AOS-W 6.4.4.12	AOS-W 6.4.4.19
178324	**Symptom:** The 5 GHz channel of an outdoor AP switched to channel 46 which was excluded in the regulatory-domain-profile. This issue is resolved by sending only the outdoor channel EIRP list for an outdoor AP. **Scenario:** This issue occurred when an outdoor AP randomly picked up a channel designated for use by an indoor AP from the exhaustive EIRP list. This issue was observed in outdoor APs running AOS-W 6.4.4.0 or later versions.	AP-Platform	All platforms	AOS-W 6.4.4.0	AOS-W 6.4.4.19
180214	**Symptom:** The status of the AP is displayed as DOWN in the WebUI but displayed as UP when you execute the command, **show ap database long** in the CLI. The fix ensures that the status is displayed correctly in the WebUI and CLI. **Scenario:** This issue was observed in switches running AOS-W 6.5.3.6.	AP-Platform	All platforms	AOS-W 6.5.3.6	AOS-W 6.4.4.19

This chapter describes the known issues and limitations identified in AOS-W 6.4.4.19.

Limitations in AOS-W 6.4.4.19

Following are the limitations observed in AOS-W 6.4.4.19:

AP LACP Limitation

AP LACP is not supported in OAW-AP324 and OAW-AP325 access points, for both Mesh and Remote modes.

Known Issues in AOS-W 6.4.4.19

Following are the known issues observed in AOS-W 6.4.4.19.

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
115215 145811	**Symptom:** The **show ap spectrum channel-metrics ap-name** command output always displays the WiFi utility value as 0%. **Scenario:** This issue occurs when the AP operates on **Spectrum Monitor** mode. This issue is observed in APs running AOS-W 6.4.2.5 or later versions. **Workaround:** None.	Spectrum-Infrastructure	All platforms	AOS-W 6.4.2.5
123458	**Symptom:** A VoIP client receives an IP address from a wrong VLAN. **Scenario:** This issue occurs under the following scenarios: ■ When an AP fails to send LLDP-MED packets after receiving LLDP packets from the VoIP phone. ■ When a client that supports LLDP-MED is connected to the downlink Ethernet port of an AP. This issue is observed in APs running AOS-W 6.4.3.3. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.3.3
124275 151661	**Symptom:** All clients continue to obtain IP addresses from the same VLAN even though a RADIUS server VSA specifies a VLAN pool with multiple VLANs. **Scenario:** This issue occurs when a RADIUS server VSA overrides the virtual AP VLANs with a different VLAN pool that is configured with the even assignment type. This issue is observed in switches running AOS-W 6.4.2.6 or later versions. **Workaround:** Change the VLAN assignment type from **even** to **hash** using the following CLI command: `(host) (config) #vlan-name <name> assignment hash`	Station Management	All platforms	AOS-W 6.4.2.6
124767 124841	**Symptom:** Media traffic is not prioritized and call details are not visible for SIP calls on the UCC dashboard. **Scenario:** This issue occurs when large segmented SIP signaling messages are broken into multiple segments and delivered out of order. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** None.	UCC	All platforms	AOS-W 6.4.2.4

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
127756 166172	**Symptom:** Multiple APs crash and reboot unexpectedly. The log file lists the reason for this event as **Out of memory**. **Scenario:** This issue occurs due to memory leak in the APs running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.4.4.9
128209 115260	**Symptom:** When an administrator tries to hard reboot a switch, it fails to reboot with the error message, **Not enough space on flash**. **Scenario:** This issue occurs due to a database file corruption. This issue is observed in switches running AOS-W 6.4.2.3 or later versions. **Workaround:** Contact Technical Support to remove the corrupted database file.	Switch-Platforms	All platforms	AOS-W 6.4.2.3
128457	**Symptom:** The **wlsxMeshNodeEntryChanged** trap generated by a switch does not have mesh link reset information. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.1 or later versions. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.3.1
130931 180579 180581	**Symptom:** The **Datapath** and **Authentication** processes running on a switch crash after the switch is upgraded. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.5.0.0
130981	**Symptom:** A switch reboots unexpectedly. The log file for the event lists the reason as **datapath timeout**. **Scenario:** This issue occurs when the **copy** command has the **** characters at the end of the destination folder name. For example, AOS-W misinterprets the **** characters in the **copy flash: crash.tar ftp: 10.1.1.1.test-user \ArubaOS\\ crash.tar** command. This issue is observed in switches running AOS-W 6.4.4.0 or later versions. **Workaround:** None.	Switch-Platforms	All platforms	AOS-W 6.4.4.0
131857	**Symptom:** When the ToS value is set to 0 in the user role, the value does not take effect. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.3 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.3.3

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
131777 138008 141686	**Symptom:** A branch switch does not communicate with a master switch. **Scenario:** This issue occurs under the following scenarios: ■ The **NAT Outside** option is enabled in the **Configuration** > **BRANCH** > **Smart Config** > **Networking** page of the WebUI. ■ The IP address of the master switch is different from the public IP address. This issue is observed in branch switches running AOS-W 6.4.4.0. **Workaround:** None.	Branch Switch	All platforms	AOS-W 6.4.4.0
132714	**Symptom:** When an administrator tries to add a static ARP entry, a switch displays the **Cannot add static ARP entry** error message. The log file lists the reason for the event as **Static ARP: too many entries (ipMapArpStaticEntryAdd)**. **Scenario:** This issue occurs because the static ARP counter continues to increment every time there is a change in the link status. This issue is observed in switches running AOS-W 6.4.3.4 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.3.4
132770	**Symptom:** In a centralized licensing system, the following license expiry message is displayed without sufficient information: **Jan 7 08:30:00 :300158: <WARN> |licensemgr| Licenses contributed by the client will expire in 29 days**. **Scenario:** This issue occurs when a client switch that contributes license goes down. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.2.12
137196 159792	**Symptom:** A switch fails to respond and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout**. **Scenario:** This issue occurs when VIA is used with SSL fallback. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.0.3

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
138438	**Symptom:** The **Configuration** > **BRANCH** > **Smart Config** > **Networking** page in the WebUI does not provide an option to set the IP address of the user VLAN to **dhcp-client**. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.6. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.4.6
138776 146701	**Symptom:** The **AP Poe Power Optimization** dropdown under **AP Configuration** > **AP** > **Provisioning** > **default** settings page cannot be configured. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.5 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.4.5
140049	**Symptom:** An AP takes longer than usual to boot. **Scenario:** This issue occurs when CPsec is enabled on a switch. This issue is observed in switches running AOS-W 6.4.3.3-FIPS. **Workaround:** None.	IPsec	All platforms	AOS-W 6.4.3.3-FIPS
140721	**Symptom:** An AP reboots unexpectedly without providing any reboot information. **Scenario:** This issue is observed in OAW-AP103H access points running AOS-W 6.4.4.4 or later versions. **Workaround:** None.	AP-Platform	OAW-AP103H access points	AOS-W 6.4.4.4
140805	**Symptom:** The **Configuration** > **BRANCH** > **Smart config** > **Routing** > **DHCP** options page of the WebUI does not provide an option to configure multiple DHCP options for a DHCP pool. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.6. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.3.6

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
141822 143282	**Symptom:** The process handling authentication requests crash due to a segmentation fault while sending RADIUS-accounting packets. **Scenario:** This issue occurs when you make the following changes to a AAA profile which is used by a client associated to the WLAN: ■ Modify the **RADIUS accounting server-group** assigned in the AAA profile to a different server-group. ■ Enable **multiple-server-accounting** which is originally disabled in the AAA profile. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** None.	RADIUS	All platforms	AOS-W 6.4.2.12
142397	**Symptom:** IPv4 syslog messages are interpreted incorrectly because of an invalid timestamp format. **Scenario:** The timestamp in the syslog message for IPv4 address includes the year at the end, which is not according to the format defined in RFC-3164. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** None.	Logging	All platforms	AOS-W 6.4.4.6
142678	**Symptom:** Adding an NTP server to a switch causes the Remote APs to reconnect without notification and cannot recover many Instant AP VPNs. **Scenario:** This issue occurs when the NTP server tries to correct the time difference in the switch. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** Reboot the switch after configuring the NTP server.	IPsec	All platforms	AOS-W 6.4.2.13
142975	**Symptom:** An AP stops forwarding traffic until it is rebooted. **Scenario:** This issue occurs in one of the following scenarios: ■ When virtual APs in tunnel mode and bridge mode are configured on the same AP. ■ When a tunnel mode virtual AP and a bridge mode wired AP are configured on the same AP. This issue is not limited to any specific AP model or AOS-W release version. **Workaround:** Configure different VLANs for the Virtual AP or Wired AP in tunnel mode and bridge mode.	AP Datapath	All platforms	AOS-W 6.4.4.6

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
143566	**Symptom:** A switch displays the **Module authentication is busy. Please try later** error when the **show reference user-role <role-name>** command is executed. **Scenario:** This issue occurs when more than 212 entries exist for a given role in user derivation-rules or server-group derivation rules. This issue is observed in switches running AOS-W 6.4.2.16 in a master-local deployment. **Workaround:** None.	Configuration	All platforms	AOS-W 6.4.2.16
145803	**Symptom:** A switch does not generate **wlsxNConnectionBackfromLocal** trap although the trap is enabled. **Scenario:** This issue occurs when a local switch is reloaded and the master switch does not generate the **wlsxNConnectionBackfromLocal** trap. This issue is observed in switches running AOS-W 6.4.4.6 or later versions. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.4.6
146924	**Symptom:** The WIPS wizard does not load in a switch. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.9-FIPS version. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.3.9-FIPS
147300	**Symptom:** A switch fails to respond and reboots. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.6 or later versions. **Workaround:** None.	Station Management	All platforms	AOS-W 6.4.3.6
147483 161501 162368 162369 163249 167972 171581	**Symptom:** Multiple radio resets are observed on the **g** radio operating in AP and AM modes. **Scenario:** This issue occurs when scanning is enabled. This issue is observed in APs running AOS-W 6.5.0.0 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.5.0.0
147563	**Symptom:** An AP shuts down unexpectedly and its power LED glows solid red. **Scenario:** This issue is observed in PoE enabled OAW-AP325 access points connected to switches running AOS-W 6.4.4.8 or later versions. **Workaround:** None.	BLE	OAW-AP325 access points	AOS-W 6.4.4.8

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
148416	**Symptom:** The **Station Management (STM)** process crashes due to memory corruption. **Scenario:** This issue occurs when there is an increase in the number of user roles. This results in the role bandwidth message not fitting into one PAPI message. This issue is observed in OAW-4550 switches running AOS-W 6.4.3.4 or later versions. **Workaround:** None.	AP-Platform	OAW-4550 switches	AOS-W 6.4.3.4
148557	**Symptom:** Clients observe a sudden increase in the number of DHCPv6/Multicast messages from the APs. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	AP-Platform	OAW-4650 switches	AOS-W 6.4.4.9
148977 155343	**Symptom:** A branch office switch randomly loses configuration updates from the master switch. **Scenario:** This issue occurs after a new license is sent from the master switch to the branch office switch. Thereafter, license-dependent configuration updates are not sent to the branch office switch. This issue is observed in branch office switches running AOS-W 6.4.4.8 or later versions. **Workaround:** None.	Licensing	All platforms	AOS-W 6.4.4.8
149594	**Symptom:** The **AMON_USER_INFO_MESSAGE** message does not contain the user-agent information, whereas the SNMP user information has the user-agent information. **Scenario:** This issue is observed in a master-local topology when choosing AMON over SNMP in OV3600. This issue is observed in switches running AOS-W 6.4.3.9 or later versions. **Workaround:** Choose SNMP in OV3600.	Base OS Security	All platforms	AOS-W 6.4.3.9
150693	**Symptom:** The datapath route cache entry is not cleared when an L3 GRE tunnel is closed. **Scenario:** This issue occurs after a channel change is triggered on the APs due to radar detection. This issue is observed in switches running AOS-W 6.4.3.9. **Workaround:** None.	OSPF	All platforms	AOS-W 6.4.3.9

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
151995	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Fatal exception**. **Scenario:** This issue occurs due to high CPU and memory utilization. This issue is observed in APs running AOS-W 6.4.4.8. **Workaround:** None.	Wi-Fi Driver	All platforms	AOS-W 6.4.4.8
152627 174134	**Symptom:** Multiple APs crash and reboot unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: Rebooting the AP because of FW ASSERT**. **Scenario:** This issue occurs when the AP switches the spatial stream based on the client capabilities while transmitting or receiving data. This issue is observed in APs running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.4.4.16
153217	**Symptom:** Multiple processes running on a switch terminate unexpectedly. **Scenario:** This issue occurs when an AAA server responds with more than one RADIUS-state attributes in the RADIUS packets. This issue is observed in switches running AOS-W 6.3.x.x, AOS-W 6.4.x.x, or AOS-W 6.5.x.x versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.3.6
153463	**Symptom:** The AP channel utilization graph shows multiple breaks and is incomplete. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.10 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.4.3.10
153824	**Symptom:** A switch fails to pass traffic when static IPsec routing with IP-to-IP IPsec tunnel is enabled. **Scenario:** This issue occurs when the route cache entry is installed with the wrong flag. This issue is observed in switches running AOS-W 6.4.4.10 or later versions. **Workaround:** None.	IPsec	All platforms	AOS-W 6.4.4.10

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
154045	**Symptom:** Some APs keep sending the error message, **mini_httpd [806]: main: 1349: no more children available** to the switch syslog. This effects the control plane operations. **Scenario:** This issue occurs when a Wi-Fi client is disconnected from the AP while generating many HTTPS redirect requests. This issue is observed in APs running AOS-W 6.4.2.6 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.2.6
154189	**Symptom:** Some APs are unable to fail over to the **Backup-LMS** IP address when CPsec is enabled. **Scenario:** This issue is observed in APs running AOS-W 6.4.3.9 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.3.9
154291	**Symptom:** Although the user completes captive portal authentication and the appropriate role is set in the user table, the **web auth disabled** message is displayed when the user tries to login again. **Scenario:** This issue occurs when the user logs in again, and MAC authentication fails. This issue is observed in switches running AOS-W 6.3.1.23. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.3.1.23
154513	**Symptom:** A master switch fails to delete the stale route entries of the branch office switch. When the entry is deleted manually, the switch displays the error, **ERROR: Cannot Delete Static Route**. **Scenario:** This issue occurs when the VLAN IP address of the branch office switch is changed and an updated CSV file (static IP address template) is uploaded on the master switch. This triggers the branch office switch to reboot, but fails to delete the stale route entries. This issue is observed in a master-branch office switch deployment with switches running AOS-W 6.4.4.8 or later versions. **Workaround:** None.	BOC	All platforms	AOS-W 6.4.4.8

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
154625 155709 155894 156383 158536 161789	**Symptom:** The VRRP state changes although heartbeats are not missed. **Scenario:** This issue occurs when a standby switch inadvertently transitions to master state because the master switch delays the processing of VRRP advertisements. This issue is observed in switches running AOS-W 6.5.0.3 in a local-master topology. **Workaround:** Disable debug logs and syslog server. Increase the advertisement interval.	Switch-Platform	All platforms	AOS-W 6.5.0.3
155190	**Symptom:** A switch does not identify certain models of HPE DAC cables of 1 m, 3 m, or 7 m; for example, J9281B, J9285B, or J9536A. **Scenario:** This issue is observed in OAW-4x50 Series switches running AOS-W 6.4.3.9 or later versions. **Workaround:** None.	Switch-Platform	OAW-4x50 Series switches	AOS-W 6.4.3.9
155332	**Symptom:** A mismatch in the number of APs in **Down** status is observed between the **Monitoring** > **Network Summary** page and the **Monitoring** > **All Access Points** page of the WebUI. **Scenario:** This issue occurs when an AP loses connectivity after it is changed from AP mode to AM mode. This issue is observed in switches running AOS-W 6.4.4.11 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.4.11
156127 176815	**Symptom:** The **STM** process running on a switch crashes unexpectedly. **Scenario:** This issue occurs when the switch is running low on memory. This issue is observed in OAW-6000 switches running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	AirGroup	OAW-6000 switches	AOS-W 6.4.4.9
156908	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **Kernel panic - not syncing: softlockup: hung tasks**. **Scenario:** The issue occurs because the frames with sequence number 0 are inserted in the incorrect position. This issue is observed in APs running AOS-W 6.4.3.7 or later versions. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.4.3.7

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
157301 170652 170653	**Symptom:** Some APs reboot unexpectedly. The log file lists the reason for the event as **Rebooting the AP because of FW ASSERT**. **Scenario:** This issue occurs when a backup LMS is configured as a new LMS. This issue is observed in APs running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.4.16
157363	**Symptom:** OAW-AP325 shuts down unexpectedly and its power LED glows solid red. **Scenario:** This issue is observed in POE enabled OAW-AP325 access points connected to a switch running AOS-W 6.4.4.8 or later versions. **Workaround:** None.	AP-Platform	OAW-AP325 access points	AOS-W 6.4.4.8
157662 158708 160524 160615	**Symptom: Datapath** process crashes on a switch that acts as a standby switch. **Scenario:** This issue occurs due to corrupt data packets. This issue is observed in switches running AOS-W 6.5.0.3 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.5.0.3
157752	**Symptom:** Viber application traffic is not denied by AppRF as expected. **Scenario:** This issue occurs when a Viber call is initiated from one of the clients from an external network. This issue is observed in switches running AOS-W 6.4.4.10 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.10
158057	**Symptom:** The log file in a switch displays the **Unexpected fatal Configuration** error messages although there is no functionality impact. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.7 or later versions. **Workaround:** None.	Configuration	All platforms	AOS-W 6.4.3.7

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
158538	**Symptom:** A switch reboots continuously after upgrading from AOS-W 6.3.x.x version to AOS-W 6.4.x.x version. The log file lists the reason for the event as **Nanny rebooted machine - fpapps process died**. **Scenario:** This issue occurs due to an upgrade failure. This issue is observed in switches running AOS-W 6.4.4.12 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.4.12
158550	**Symptom:** A user is unable to add RAP whitelist with special characters in the **full name** field under the **Configuration** > **AP Installation** > **Whitelist** WebUI page. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.7 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.3.7
158576	**Symptom:** The word **Interference** is misspelled in the **Dashboard** mouse-over help for the **Channel Utilization** graph listed under the **Radios** table. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.4.9
158871 159851	**Symptom:** A OAW-4750 switch reboots due to datapath crash. **Scenario:** This issue occurs due to a race condition. This issue is observed in OAW-4750 switches running AOS-W 6.5.0.0 or later versions. **Workaround:** None.	Switch-Datapath	OAW-4750 switches	AOS-W 6.5.0.0
159493 162023	**Symptom:** Multiple switches reboot unexpectedly. The log file lists the reason for the event as **datapath timeout**. **Scenario:** This issue occurs due to corrupt data entries in mobility multicast group table. This issue is observed in switches running AOS-W 6.4.4.12 or later versions. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.5.0.3

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
159791	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot Time and Cause: Reboot caused by kernel panic: Fatal exception in interrupt.** **Scenario:** This issue occurs when the IPsec tunnel is terminated while passing traffic. This issue is observed in OAW-AP215 access points running AOS-W 6.4.3.6 or later versions. **Workaround:** None.	VPN	OAW-AP215 access points	AOS-W 6.4.3.6
159833 165229	**Symptom:** A user cannot enable or disable OSPF on a GRE tunnel interface. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.4 or later versions. **Workaround:** None.	OSPF	All platforms	AOS-W 6.4.3.4
161922	**Symptom:** AirGroup clients are unable to discover servers consistently. **Scenario:** This issue occurs as the switch keeps caching multiple entries of TXT records for wired AirGroup servers. This issue is observed on switches running AOS-W 6.5.1.4. **Workaround:** None.	AirGroup	All platforms	AOS-W 6.5.1.4
162359 166229	**Symptom:** Instant AP clients that terminate on a switch are unable to pass traffic. Hence, clients are not assigned the required Instant AP user role. **Scenario:** This issue occurs when a custom AAA wired profile is applied on the port where the Instant AP is terminated. This issue is observed in OAW-4750 switches running AOS-W 6.4.4.11 or later versions. **Workaround**: Apply the default AAA wired profile on the port.	Remote AP	OAW-4750 switches	AOS-W 6.4.4.11
163123	**Symptom:** The error log file in a switch repeatedly lists the **ERRS |ike| usec 0 ERRS |ike| timeout value is very small Sec 0** message. **Scenario:** This issue occurs when a VPN connection is triggered with EAP-TLS. This issue is observed in switches running AOS-W 6.4.4.10 or later versions. **Workaround:** None.	IPsec	All platforms	AOS-W 6.4.4.10

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
164476 177025	**Symptom:** The **show datapath session dpi** command output indicates that the non-FTP sessions are incorrectly classified as FTP sessions. **Scenario:** This issue occurs when DPI is enabled on switches running AOS-W 6.4.4.14 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.4.14
165669	**Symptom:** A switch reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout (Intent:cause:register 56:86:0:2c)**. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.6 version. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.3.6
167111 176946	**Symptom:** Clients are unable to pass traffic although they receive the IP address from the correct VLAN. **Scenario:** This issue occurs when the netdestination configurations are updated. This issue is observed in switches running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.4.9
168363	**Symptom:** Clients experience packet loss due to high datapath utilization in the CPU. **Scenario:** This issue is observed in OAW-4750 switches running AOS-W 6.4.3.6. **Workaround:** None.	Switch-Datapath	OAW-4750 switches	AOS-W 6.4.3.6
168587	**Symptom:** An AP shows incorrect High Availability (HA) information and clients lose connectivity. **Scenario:** This issue occurs during HA failover when an AP does not receive a failover response from the standby switch. This issue is observed in access points running AOS-W 6.4.4.9 or later versions. **Workaround:** Reboot the AP.	AP-Platform	All platforms	AOS-W 6.4.4.9

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
168634	**Symptom:** A switch crashes and reboots unexpectedly. The log file lists the reason for this event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue occurs after a switch is upgraded. This issue is observed in switches running AOS-W 6.4.4.15. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.15
168795 177092 178670	**Symptom:** A WebCC URL cloud lookup in a switch fails. The log file lists the reason for the event as **<ERRS> |web_cc| web_cc_callback: URL lookup failed**. **Scenario:** This issue occurs when WebCC is enabled on switches running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	WebCC	All platforms	AOS-W 6.4.4.16
168984 170072 173647 174375 174998	**Symptom:** A switch fails to update the syslog server. **Scenario:** This issue occurs because the syslog file becomes huge due to excess and incorrect logging from the switch. This issue is observed in switches running AOS-W 6.4.4.13 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.4.13
169664	**Symptom:** A switch reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout (Intent:cause:register 56:86:50)**. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.16 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.2.16
169749	**Symptom:** Clients are unable to connect to 5 GHz radio on some APs. **Scenario:** This issue occurs because radio 0 does not transmit traffic. This issue is observed in OAW-AP325 access points running AOS-W 6.4.4.13 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.13

Table 5: *Known Issues in AOS-W 6.4.4.19*

Bug ID	Description	Component	Platform	Reported Version
170813	**Symptom:** Clients fail to associate with an 802.1X SSID after an AP fails over to the LMS from the backup LMS. **Scenario:** This issue occurs when 802.11r configuration is enabled on the backup LMS but not on the LMS. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** Ensure that the status of the 802.11r configuration is the same, either enabled or disabled, on both LMS and backup LMS.	AP-Platform	All platforms	AOS-W 6.4.4.16
172019 172464 175355	**Symptom:** A switch has high CPU utilization and APs get disconnected. **Scenario:** This issue occurs when a switch is upgraded. This issue is observed in switches running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	Web Server	All platforms	AOS-W 6.4.4.16
176067	**Symptom:** The authentication of management user public key fails if it exceeds 14 characters. **Scenario:** This issue occurs due to a limit of maximum 96 characters for creating a public key. This issue is observed in switches running AOS-W 6.4.4.16. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.4.16
177420	**Symptom:** The HTTP Strict Transport Security (HSTS) header is missing in HTTP response. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.16. **Workaround:** None.	Web Server	All platforms	AOS-W 6.4.4.16
178182 179612	**Symptom:** A user experiences intermittent Skype call drops. **Scenario:** This issue occurs when an AP stops transmitting packets for a few seconds to track power save status. This issue is observed in access points running AOS-W 6.5.1.9. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.5.1.9
178462 179319 180173 180667 181235	**Symptom:** The **show memory debug** command does not include the **memory available** column. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.16 or later versions. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.4.16

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

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

Topics in this chapter include:

Upgrade Caveats

- AP LLDP profile is not supported on OAW-AP120 Series access points in AOS-W 6.4.x.
- Starting from AOS-W 6.3.1.0, the local file upgrade option in the OAW-4306 Series switch Web UIs have been disabled.
- AOS-W 6.4.x does not allow you to create redundant firewall rules in a single ACL. AOS-W will consider a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
  - source IP/alias
  - destination IP/alias
  - proto-port/service

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

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

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

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

- AOS-W 6.4.x supports only the newer MIPS switches (OAW-4306 Series, OAW-4504XM, OAW-4604, OAW-4704, OAW-M3, OAW-40xx Series, and OAW-4x50 Series). Legacy PPC switches (OAW-4302, OAW-4308, OAW-4324, SC1/SC2) are not supported. Do not upgrade to AOS-W 6.4.x if your deployment contains a mix of MIPS and PPC switches in a master-local setup.
- When upgrading the software in a multiswitch network (one that uses two or more Alcatel-Lucent switches), special care must be taken to upgrade all the switches in the network and to upgrade them in the proper sequence. (See Upgrading in a Multiswitch Network on page 41.)

GRE Tunnel-Type Requirements

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

- AOS-W 6.4.4.0 continues to support L2 GRE tunnel type zero, but it is recommended to use a non-zero tunnel type.
- If both L2 and L3 tunnels are configured between endpoint devices, you must use a non-zero tunnel type for L2 GRE tunnels.

Important Points to Remember and Best Practices

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

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any other changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of your network by answering the following questions:
  - How many APs are assigned to each switch? Verify this information by navigating to the **Monitoring > NETWORK > All Access Points** section of the WebUI, or by executing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the switch (DNS, DHCP Option, Broadcast)?
  - What version of AOS-W is currently on the switch?
  - Are all switches in a master-local cluster running the same version of software?
  - Which services are used on the switches (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software images to the switch. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to this version of AOS-W, assess your software license requirements and load any new or expanded licenses you may require. For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the *AOS-W 6.4.x User Guide*.

Memory Requirements

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

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

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

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

- **Crash Data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing Up Critical Data on page 39 to copy the **crash.tar** file to an external server, and then execute the **tar clean crash** command to delete the file from the switch.
- **Flash Backups:** Use the procedures described in Backing Up Critical Data on page 39 to back up the flash directory to a file named **flash.tar.gz**, and then execute the **tar clean flash** command to delete the file from the switch.
- **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing Up Critical Data on page 39 to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the switch.

Backing Up Critical Data

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

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

Backing up and Restoring Compact Flash in the WebUI

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

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

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

Backing up and Restoring Compact Flash in the CLI

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

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

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

   ```
   (host) # backup flash
   Please wait while we tar relevant files from flash...
   Please wait while we compress the tar file...
   Checking for free space on flash...
   Copying file to flash...
   File flashbackup.tar.gz created successfully on flash.
   ```
3. Execute the **copy** command to transfer the backup flash file to an external server or storage device.

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

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

   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   (host) # copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
   ```
4. Execute the **restore** command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system.

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

Upgrading in a Multiswitch Network

In a multiswitch network (a network with two or more Alcatel-Lucent switches), special care must be taken to upgrade all switches based on the switch type (master or local). Be sure to back up all switches being upgraded, as described in Backing Up Critical Data on page 39.

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

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

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

Installing the FIPS Version of AOS-W 6.4.4.18

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

Instructions on Installing FIPS Software

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

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

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

Upgrading to AOS-W 6.4.4.18

The following sections provide the procedures for upgrading the switch to AOS-W 6.4.4.19 by using the WebUI or CLI.

Install Using 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 38.

NOTE

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

Upgrading From an Older Version of AOS-W

Before you begin, verify the version of AOS-W currently running on your switch. If you are running one of the following versions of AOS-W, you must download and upgrade to an interim version of AOS-W before upgrading to AOS-W 6.4.4.18.

NOTE

When upgrading from an existing AOS-W 6.4.4.x release, it is required to set AMON packet size manually to a desired value. However, the packet size is increased to 32K by default for fresh installations of AOS-W 6.4.4.8.

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

Follow step 2 to step 11 of the procedure described in Upgrading to AOS-W 6.4.4.18 on page 41 to install the interim version of AOS-W, and then repeat steps 1 through 11 of the procedure to download and install AOS-W 6.4.4.18.

Upgrading From a Recent Version of AOS-W

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

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

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

1. Download AOS-W 6.4.4.18 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 on the switch at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the switch will not load a corrupted image.

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

NOTE

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

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

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

    If you chose to automatically reboot the switch in step 8, the reboot process starts automatically within a few seconds (unless you cancel it).
12. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > NETWORK > All WLAN Controllers** page to verify the upgrade.

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

1. Log in to the WebUI to verify all your switches are up after the reboot.
2. Navigate to the **Monitoring > NETWORK > Network Summary** page to determine if your APs are up and ready to accept clients. In addition, verify that the number of access points and clients are what you would expect.
3. Verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use and in different locations when possible.

5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing Up Critical Data on page 39 for information on creating a backup. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses.

Install Using the CLI

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash space available for an upgrade using the CLI. For details, see Memory Requirements on page 38.

Upgrading From an Older Version of AOS-W

Before you begin, verify the version of AOS-W currently running on your switch. For more information, see Upgrading to AOS-W 6.4.4.18 on page 41.

Follow steps 2 through 7 of the procedure described in Upgrading to AOS-W 6.4.4.18 on page 41 to install the interim version of AOS-W, and then repeat steps 1 through 7 of the procedure to download and install AOS-W 6.4.4.18.

Upgrading From a Recent Version of AOS-W

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

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

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

1. Download AOS-W 6.4.4.18 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 nonboot partition.

```
(host)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
```
or
```
(host)# copy tftp: <tftphost> <image filename> system: partition <0|1>
```
or
```
(host)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
```
or
```
(host)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
```

The USB option is available on the OAW-4010, OAW-4030, and OAW-4x50 Series switches.

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 39 for information on creating a backup.

Downgrading

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

If you upgraded from AOS-W 3.3.x to AOS-W 5.0, the upgrade script encrypts the internal database. New entries created in AOS-W 6.4.4.18 are lost after the downgrade (this warning does not apply to upgrades from AOS-W 3.4.x to AOS-W 6.1).

If you downgrade to a pre-6.1 configuration that was not previously saved, some parts of your deployment may not work as they previously did. For example, when downgrading from AOS-W 6.4.4.18 to 5.0.3.2, changes made to WIPS in AOS-W 6.x prevent the new predefined IDS profile assigned to an AP group from being recognized by the older version of AOS-W. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.
These new IDS profiles begin with *ids-transitional* while older IDS profiles do not include *transitional*. If you have encountered this issue, execute the **show profile-errors** and **show ap-group** commands to view the IDS profile associated with the AP group.

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

Before You Begin

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

1. Back up your switch. For details, see Backing Up Critical Data on page 39.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W 6.4.4.18 configuration file.
4. Set the switch to boot from the system partition that contains the previously running AOS-W image.

   When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next switch reload. An error message is displayed if system boot parameters are set for incompatible image and configuration files.
5. After downgrading the software on the switch, perform the following steps:
   - Restore pre-AOS-W 6.4.4.18 flash backup from the file stored on the switch. Do not restore the AOS-W 6.4.4.18 flash backup file.
   - You do not need to reimport the WMS database or RF Plan data. However, if you have added changes to RF Plan in AOS-W 6.4.4.18, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W 6.4.4.18, you need to reinstall the certificates in the downgraded AOS-W version.

Downgrading Using the WebUI

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

1. If the saved preupgrade configuration file is on an external FTP/TFTP server, copy the file to the switch by navigating to the **Maintenance > File > Copy Files** page.
   a. For **Source Selection**, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the preupgrade configuration file.
   b. For **Destination Selection**, enter a file name (other than default.cfg) for Flash File System.

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

Downgrading Using the CLI

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

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

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

   or

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

2. Set the switch to boot with your preupgrade configuration file.

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

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

   In the following example, partition 1, the backup system partition, contains the backup release AOS-W 6.4.4.2. Partition 0, the default boot partition, contains the AOS-W 6.4.4.18 image.

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

Appendix a
Acronyms and Abbreviations

The following table lists the acronyms and abbreviations used in Aruba documents.

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
3G	Third Generation of Wireless Mobile Telecommunications Technology
4G	Fourth Generation of Wireless Mobile Telecommunications Technology
AAA	Authentication, Authorization, and Accounting
ABR	Area Border Router
AC	Access Category
ACC	Advanced Cellular Coexistence
ACE	Access Control Entry
ACI	Adjacent Channel interference
ACL	Access Control List
AD	Active Directory
ADO	Active X Data Objects
ADP	Aruba Discovery Protocol
AES	Advanced Encryption Standard
AIFSN	Arbitrary Inter-frame Space Number

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
ALE	Analytics and Location Engine
ALG	Application Layer Gateway
AM	Air Monitor
AMON	Advanced Monitoring
AMP	AirWave Management Platform
A-MPDU	Aggregate MAC Protocol Data Unit
A-MSDU	Aggregate MAC Service Data Unit
ANQP	Access Network Query Protocol
ANSI	American National Standards Institute
AP	Access Point
API	Application Programming Interface
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
AVF	AntiVirus Firewall
BCMC	Broadcast-Multicast
BGP	Border Gateway protocol
BLE	Bluetooth Low Energy
BMC	Beacon Management Console

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
BPDU	Bridge Protocol Data Unit
BRAS	Broadband Remote Access Server
BRE	Basic Regular Expression
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CA	Certification Authority
CAC	Call Admission Control
CALEA	Communications Assistance for Law Enforcement Act
CAP	Campus AP
CCA	Clear Channel Assessment
CDP	Cisco Discovery Protocol
CDR	Call Detail Records
CEF	Common Event Format
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CLI	Command-Line Interface
CN	Common Name

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
CoA	Change of Authorization
CoS	Class of Service
CPE	Customer Premises Equipment
CPsec	Control Plane Security
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSA	Channel Switch Announcement
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSR	Certificate Signing Request
CSV	Comma Separated Values
CTS	Clear to Send
CW	Contention Window
DAS	Distributed Antenna System
dB	Decibel
dBm	Decibel Milliwatt
DCB	Data Center Bridging
DCE	Data Communication Equipment

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
DCF	Distributed Coordination Function
DDMO	Distributed Dynamic Multicast Optimization
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DFT	Discreet Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMO	Dynamic Multicast optimization
DN	Distinguished Name
DNS	Domain Name System
DOCSIS	Data over Cable Service Interface Specification
DoS	Denial of Service
DPD	Dead Peer Detection
DPI	Deep Packet Inspection
DR	Designated Router
DRT	Downloadable Regulatory Table
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
DST	Daylight Saving Time
DTE	Data Terminal Equipment
DTIM	Delivery Traffic Indication Message
DTLS	Datagram Transport Layer Security
DU	Data Unit
EAP	Extensible Authentication Protocol
EAP-FAST	EAP-Flexible Authentication Secure Tunnel
EAP-GTC	EAP-Generic Token Card
EAP-MD5	EAP-Method Digest 5
EAP-MSCHAP EAP-MSCHAPv2	EAP-Microsoft Challenge Handshake Authentication Protocol
EAPoL	EAP over LAN
EAPoUDP	EAP over UDP
EAP-PEAP	EAP-Protected EAP
EAP-PWD	EAP-Password
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
ECC	Elliptical Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
EIGRP	Enhanced Interior Gateway Routing Protocol
EIRP	Effective Isotropic Radiated Power
EMM	Enterprise Mobility Management
ESI	External Services Interface
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
EULA	End User License Agreement
FCC	Federal Communications Commission
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FIB	Forwarding Information Base
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
FQLN	Fully Qualified Location Name
FRER	Frame Receive Error Rate
FRR	Frame Retry Rate
FSPL	Free Space Path Loss
FTP	File Transfer Protocol
GBps	Gigabytes per second

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
Gbps	Gigabits per second
GHz	Gigahertz
GIS	Generic Interface Specification
GMT	Greenwich Mean Time
GPP	Guest Provisioning Page
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
GVRP	GARP or Generic VLAN Registration Protocol
H2QP	Hotspot 2.0 Query Protocol
HA	High Availability
HMD	High Mobility Device
HSPA	High-Speed Packet Access
HT	High Throughput
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS	Internet Authentication Service
ICMP	Internet Control Message Protocol

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
IdP	Identity Provider
IDS	Intrusion Detection System
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IKE PSK	Internet Key Exchange Pre-shared Key
IoT	Internet of Things
IP	Internet Protocol
IPM	Intelligent Power Monitoring
IPS	Intrusion Prevention System
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
JSON	JavaScript Object Notation
KBps	Kilobytes per second
Kbps	Kilobits per second
L2TP	Layer-2 Tunneling Protocol

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDPC	Low-Density Parity-Check
LEA	Law Enforcement Agency
LEAP	Lightweight Extensible Authentication Protocol
LED	Light Emitting Diode
LEEF	Log Event Extended Format
LI	Lawful Interception
LLDP	Link Layer Discovery Protocol
LLDP-MED	LLDP–Media Endpoint Discovery
LMS	Local Management Switch
LNS	L2TP Network Server
LTE	Long Term Evolution
MAB	MAC Authentication Bypass
MAC	Media Access Control

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
MAM	Mobile Application Management
MBps	Megabytes per second
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MD5	Message Digest 5
MDM	Mobile Device Management
mDNS	Multicast Domain Name System
MFA	Multi-factor Authentication
MHz	Megahertz
MIB	Management Information Base
MIMO	Multiple-Input Multiple-Output
MLD	Multicast Listener Discovery
MPDU	MAC Protocol Data Unit
MPLS	Multiprotocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSS	Maximum Segment Size
MSSID	Mesh Service Set Identifier
MSTP	Multiple Spanning Tree Protocol

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
MTU	Maximum Transmission Unit
MU-MIMO	Multi-User Multiple-Input Multiple-Output
MVRP	Multiple VLAN Registration Protocol
NAC	Network Access Control
NAD	Network Access Device
NAK	Negative Acknowledgment Code
NAP	Network Access Protection
NAS	Network Access Server Network-attached Storage
NAT	Network Address Translation
NetBIOS	Network Basic Input/Output System
NIC	Network Interface Card
Nmap	Network Mapper
NMI	Non-Maskable Interrupt
NMS	Network Management Server
NOE	New Office Environment
NTP	Network Time Protocol
OAuth	Open Authentication
OCSP	Online Certificate Status Protocol

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
OFA	OpenFlow Agent
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier
OKC	Opportunistic Key Caching
OS	Operating System
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
OVA	Open Virtual Appliance
OVF	Open Virtualization Format
PAC	Protected Access Credential
PAP	Password Authentication Protocol
PAPI	Proprietary Access Protocol Interface
PCI	Peripheral Component Interconnect
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PEAP-GTC	Protected Extensible Authentication Protocol-Generic Token Card
PEF	Policy Enforcement Firewall
PFS	Perfect Forward Secrecy
PHB	Per-hop behavior

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
PIM	Protocol-Independent Multicast
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMK	Pairwise Master Key
PoE	Power over Ethernet
POST	Power On Self Test
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PPTP	PPP Tunneling Protocol
PRNG	Pseudo-Random Number Generator
PSK	Pre-Shared Key
PSU	Power Supply Unit
PVST	Per VLAN Spanning Tree
QoS	Quality of Service
RA	Router Advertisement
RADAR	Radio Detection and Ranging

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RAP	Remote AP
RAPIDS	Rogue Access Point and Intrusion Detection System
RARP	Reverse ARP
REGEX	Regular Expression
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio Frequency Identification
RIP	Routing Information Protocol
RRD	Round Robin Database
RSA	Rivest, Shamir, Adleman
RSSI	Received Signal Strength Indicator
RSTP	Rapid Spanning Tree Protocol
RTCP	RTP Control Protocol
RTLS	Real-Time Location Systems
RTP	Real-Time Transport Protocol
RTS	Request to Send

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
RTSP	Real Time Streaming Protocol
RVI	Routed VLAN Interface
RW RoW	Rest of World
SA	Security Association
SAML	Security Assertion Markup Language
SAN	Subject Alternative Name
SCB	Station Control Block
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SDN	Software Defined Networking
SDR	Software-Defined Radio
SDU	Service Data Unit
SD-WAN	Software-Defined Wide Area Network
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SIP	Session Initiation Protocol
SIRT	Security Incident Response Team
SKU	Stock Keeping Unit
SLAAC	Stateless Address Autoconfiguration
SMB	Small and Medium Business
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SNIR	Signal-to-Noise-Plus-Interference Ratio
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SoC	System on a Chip
SoH	Statement of Health
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
STBC	Space-Time Block Coding
STM	Station Management
STP	Spanning Tree Protocol
STRAP	Secure Thin RAP
SU-MIMO	Single-User Multiple-Input Multiple-Output
SVP	SpectraLink Voice Priority
TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFTP	Trivial File Transfer Protocol
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TLV	Type-length-value
ToS	Type of Service
TPC	Transmit Power Control
TPM	Trusted Platform Module
TSF	Timing Synchronization Function

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
TSPEC	Traffic Specification
TTL	Time to Live
TTLS	Tunneled Transport Layer Security
TXOP	Transmission Opportunity
U-APSD	Unscheduled Automatic Power Save Delivery
UCC	Unified Communications and Collaboration
UDID	Unique Device Identifier
UDP	User Datagram Protocol
UI	User Interface
UMTS	Universal Mobile Telecommunication System
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VA	Virtual Appliance
VBN	Virtual Branch Networking
VBR	Virtual Beacon Report
VHT	Very High Throughput

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
VIA	Virtual Intranet Access
VIP	Virtual IP Address
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over IP
VoWLAN	Voice over Wireless Local Area Network
VPN	Virtual Private Network
VRD	Validated Reference Design
VRF	Visual RF
VRRP	Virtual Router Redundancy Protocol
VSA	Vendor-Specific Attributes
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WebUI	Web browser User Interface
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
WIDS	Wireless Intrusion Detection System
WINS	Windows Internet Naming Service

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
WIPS	Wireless Intrusion Prevention System
WISPr	Wireless Internet Service Provider Roaming
WLAN	Wireless Local Area Network
WME	Wireless Multimedia Extensions
WMI	Windows Management Instrumentation
WMM	Wi-Fi Multimedia
WMS	WLAN Management System
WPA	Wi-Fi Protected Access
WSDL	Web Service Description Language
WWW	World Wide Web
WZC	Wireless Zero Configuration
XAuth	Extended Authentication
XML	Extensible Markup Language
XML-RPC	XML Remote Procedure Call
ZTP	Zero Touch Provisioning