AOS-W 6.4.4.11

Alcatel·Lucent
Enterprise

Release Notes

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

AOS-W 6.4.4.11 is a software patch release that includes new features and enhancements introduced in this release and fixes to issues identified in previous releases.

Use the following links to navigate to the corresponding 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 24 describes the known and outstanding issues identified in this release.
- Upgrade Procedure on page 33 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

This chapter describes the new features and/or enhancements introduced in AOS-W 6.4.4.11.

AP-Platform

PoE Optimization Support on OAW-AP205H

Starting from AOS-W 6.4.4.11, PoE optimization is supported on the OAW-AP205H access points. On enabling this feature:

- The AP draws 13.0 W power.
- USB port is disabled if the **AP USB Power override** parameter is not enabled.
- Power Sourcing Equipment (PSE) is disabled.

Enable the PoE optimization on OAW-AP205H AP from the WebUI or CLI.

In the WebUI

To enable PoE optimization on OAW-AP205H AP using the WebUI:

1. Navigate to **Configuration > WIRELESS > AP Configuration**.
2. In the **AP Group** tab, click the **default** AP group.
   This procedure uses the *default* AP group.
3. In the **Profiles** section, expand **AP** and click **Provisioning**.
4. In the **Profile Details** section, select the **default** profile from the **Provisioning profile** drop-down list.
   This procedure uses the *default* provisioning profile.
5. In the **AP POE Power optimization** drop-down list, select **enabled**.
6. Click **Apply** and **Save Configuration**.

In the CLI

To enable PoE optimization on OAW-AP205H AP using the CLI:

```
(host) (config) #ap provisioning-profile default
(host) (Provisioning profile "default") #ap-poe-power-optimization enabled
(host) (Provisioning profile "default") #write memory
```

Switch-Datapath

Bridge Age Out Mechanism

Starting from AOS-W 6.4.4.11, the bridge entry will not age out as long as the wireless client/device is associated with an AP. To ensure this, a new flag is introduced which is set to 'W', wifi. This flag indicates that the bridge entry cannot age out when the flag is set to 'w'. The bridge entry will get deleted only when the wireless client or station is deleted.

```
(host) #show datapath bridge
Datapath Bridge Table Entries
-----------------------------
Flags: P - Permanent, D - Deny, R - Roamed Client, M - Mobile,
X - Xsec, A - Auth, T - Trusted, W - Wifi

MAC                VLAN  Assigned VLAN  Destination  Flags    Age
-----------------  ----  -------------  -----------  -------  ----
00:1A:1E:00:1A:E8  1     1              0/0/0                 0
00:1A:1E:00:D3:E0  40    40             local        P        0
01:80:C2:00:00:0E  4095  4095           local        P        0
01:80:C2:00:00:02  4095  4095           local        P        0
00:0B:86:16:6A:A0  1     1              0/0/0                 0
3C:77:E6:7C:44:09  40    40             tunnel 12    W        0
```

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 6.4.4.11:

- DRT-1.0_57440

This chapter describes the issues resolved in AOS-W 6.4.4.11.

Table 4: *Resolved Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
126385	**Symptom:** Clients did not connect to an SSID although an AP was connected to a switch. This issue is resolved by dropping the packets if the AP is not currently active. **Scenario:** This issue occurred when APs worked in active-backup mode with VAP in bridge mode. This issue was observed in APs running AOS-W 6.4.2.12.	AP-Platform	All platforms	AOS-W 6.4.2.12	AOS-W 6.4.4.11
137617 143207 148674 150451 150737	**Symptom:** A user was unable to access the WebUI. This issue is resolved by releasing the **HTTPD** resources using a query timeout. **Scenario:** This issue was observed when the **HTTP** process was busy. This issue was observed in switches running AOS-W 6.4.3.5.	WebUI	All platforms	AOS-W 6.4.3.5	AOS-W 6.4.4.11
140206	**Symptom:** The WebUI showed the **ERROR: Cannot delete the NTP Server** error. The fix ensures that the WebUI interprets the CLI configuration correctly. **Scenario:** This issue occurred while configuring the clock using wizard. This issue was observed when NTP server was not configured in the switch. Although the output of the **show ntp servers brief** command showed **No Upstream NTP servers configured**, the WebUI failed to interpret the CLI configuration correctly. This issue was observed in switches running AOS-W 6.4.3.4 or later versions.	WebUI	All platforms	AOS-W 6.4.3.4	AOS-W 6.4.4.11

Table 4: *Resolved Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
141567 147002 150219 150220 150221 150875 151246	**Symptom:** A user was unable to blacklist a wireless client by using the WebUI. The fix ensures that a client can be blacklisted using the WebUI. **Scenario:** This issue was observed in switches running AOS-W 6.4.x versions.	WebUI	All platforms	AOS-W 6.4.2.17	AOS-W 6.4.4.11
141942 149651 149926	**Symptom:** Some APs rebooted unexpectedly. This issue is resolved by adding a check for missed timer interrupts to avoid false internal watchdog timer. **Scenario:** This issue occurred because of missed timer interrupts caused by false internal watchdog timer. This issue was observed in OAW-AP320 Series access points running AOS-W 6.4.4.10.	WebUI	All platforms	AOS-W 6.4.4.10	AOS-W 6.4.4.11
142265 145485 150171	**Symptom:** An AP was unable to establish a Generic Route Encapsulation (GRE) tunnel with a switch. This issue is resolved by deauthenticating the client and cleaning the VLAN ID array. **Scenario:** This issue occurred when the AP was not broadcasting the SSID but remote BSS-table was able to see the BSSID/SSID. This issue was observed when the **STM** process received a VLAN delete message, and deleted all VAPs with the same VLAN in the station VLAN array, which resulted in the switch bringing down the VAP without notifying the AP.	Station Management	All platforms	AOS-W 6.4.2.14	AOS-W 6.4.4.11
142449	**Symptom:** The IPv6 static route settings disappeared after a switch reloaded. This issue is resolved by adding a check for the interface number match and removing the check when the IPv6 address is checked against the next hop address for equality. **Scenario:** This issue occurred when the IPv6 route with a link local as the next hop was not added to the kernel after shut and no shut of a VLAN interface. This issue was observed in switches running AOS-W 6.4.4.7 or later versions.	IPv6	All platforms	AOS-W 6.4.4.7	AOS-W 6.4.4.11

Table 4: *Resolved Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
143181	**Symptom:** A OAW-4x50 Series switch contacted an Activate server continuously. This issue is resolved by adding the **activate periodic-sync {enable|disable}** parameter in the CLI to control the communication with an Activate server. **Scenario:** This issue was observed in OAW-4x50 Series switches running AOS-W 6.4.4.x or later versions.	Branch Office Switch	OAW-4x50 Series switches	AOS-W 6.4.3.7	AOS-W 6.4.4.11
143342	**Symptom:** On configuring a custom IPv6 link-local address, a switch failed to show the running configuration. This issue is resolved by setting a flag for the custom IPv6 link-local address. **Scenario:** This issue was observed when the neighbor discovery and router advertisement settings were enabled. This issue was observed in switches running AOS-W 6.4.4.6.	IPv6	All platforms	AOS-W 6.4.4.6	AOS-W 6.4.4.11
143684	**Symptom:** When a user ran a search for AP name in the WebUI, the result displayed more APs than the preset number of results per page. This issue is resolved by fixing the AP provisioning page pagination when filtering by IP or AP-name. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.8.	WebUI	All platforms	AOS-W 6.4.4.8	AOS-W 6.4.4.11
143827	**Symptom:** A OAW-4030 master switch rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (Intent:cause:register 56:86:50:60)**. This issue is resolved by dropping the packets that contain invalid tunnel entries. **Scenario:** This issue occurred when a switch processed invalid tunnel entries. This issue was not limited to any specific switch model or AOS-W version.	Switch-Datapath	All platforms	AOS-W 6.4.3.6	AOS-W 6.4.4.11
143836	**Symptom:** When an Instant AP was deployed as a campus AP, it failed to come up on a switch using a 4G uplink. The fix ensures that the AP boots successfully on the switch using a 4G uplink. **Scenario:** This issue was observed when the AP uplink router MTU was changed to less than the length of the packet sent by the AP. This issue was observed in 100 Series access points running AOS-W 6.4.2.12 or later versions.	AP-Platform	100 Series access points	AOS-W 6.4.2.12	AOS-W 6.4.4.11

Table 4: *Resolved Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
144185	**Symptom:** APs crashed and rebooted unexpectedly across local switches. The log file listed the reason for the event as **Kernel Panic at "asap_firewall_netif_rx"**. The fix ensures that the APs do not crash and work as expected. **Scenario:** This issue occurred because of an invalid VAP pointer. This issue was observed in APs connected to switches running AOS-W 6.4.3.x versions.	AP-Wireless	All platforms	AOS-W 6.4.3.4	AOS-W 6.4.4.11
144752 146289 146692 146857 150333	**Symptom:** Wired users were incorrectly placed in **default-iap-role** in a switch. The log file listed the reason for the event as **IAP L2 User**. The fix ensures that wired users are placed in the correct user role. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.x.	Role/VLAN Derivation	All platforms	AOS-W 6.4.4.8	AOS-W 6.4.4.11
144913 146000	**Symptom:** The Software Development Kit (SDK) did not support long URL classification as part of Web Content Classification (WebCC). This issue is resolved by updating the SDK to the latest build. **Scenario:** This issue was observed in switches running AOS-W 6.4.x and AOS-W 6.5.x.	WebCC	All platforms	AOS-W 6.4.4.0	AOS-W 6.4.4.11
145142 153043	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **rebooted due to FW ASSERT in _ rcRateFind (ratectrl_11ac.c:1683)**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.8.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.8	AOS-W 6.4.4.11

Table 4: *Resolved Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
145314	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT**. This issue is resolved by rejecting the client association request with a higher Number of Spatial Stream (NSS) value. **Scenario:** This issue occurred when the NSS value in the client association request was higher than the supported NSS value. This issue was observed OAW-AP320 Series access points running AOS-W 6.4.x.	AP-Platform	OAW-AP320 Series access points	AOS-W 6.4.4.8	AOS-W 6.4.4.11
145346 150273 150761	**Symptom:** An AP stopped responding and rebooted. The log files listed the reason for the event as **Badness at kernel/workqueue.c:495**. Improvements in the WLAN driver of the AP resolved this issue. **Scenario:** This issue was observed when the AP was configured as a spectrum monitor mode in 802.11G band and air monitor mode in 802.11A band. This issue was observed in OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, and OAW-AP270 Series access points running AOS-W 6.4.4.9.	AP-Wireless	OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, and OAW-AP270 Series access points	AOS-W 6.4.4.9	AOS-W 6.4.4.11
145373	**Symptom:** High noise floor was observed in an AP. This issue is resolved by upgrading the vendor driver. **Scenario:** This issue occurred because of an increase in traffic load on the APs. This issue was observed in OAW-AP225 access points running AOS-W 6.4.4.8.	AP-Platform	OAW-AP225 access points	AOS-W 6.4.4.8	AOS-W 6.4.4.11
145486 146896 148292	**Symptom:** The configuration on a master switch was not synchronized with a local switch. This issue is resolved by synchronizing the configuration on the master switch with the local switch. **Scenario:** Although centralized licensing was enabled and synchronized and licenses were available, the APs displayed the **IL** (I-Inactive, L-Unlicensed) flag. This issue was observed in OAW-4750 switches running AOS-W 6.4.3.7.	Master-Local	OAW-4750 switches	AOS-W 6.4.3.7	AOS-W 6.4.4.11

Table 4: *Resolved Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
145658	**Symptom:** A switch crashed when the size of **/tmp/.fpcli_cfg_diff** and **/tmp/.fpcli_cfg_diff_enc** temporary files increased. The issue is resolved by adding a size limit of 1 MB for these files and when the limit crosses 1 MB, the **show configuration diff** command will display a warning. **Scenario:** This issue occurred when IP routes were added and removed continuously using a script and the **#write mem** command was not executed. This issue was observed in switches running AOS-W 6.3.1.18.	Switch-Platform	All platforms	AOS-W 6.3.1.18	AOS-W 6.4.4.11
145852	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT**. This issue is resolved by checking and dropping incoming packets where: • The source address is either multicast or the address is null. • The source address corresponds with the VAP BSSID node. **Scenario:** This issue was observed when the firmware file displayed an incoming authentication frame where the source address was equivalent to broadcast. This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.8.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.8	AOS-W 6.4.4.11
146653	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic at 0x009C07BC**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.8.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.8	AOS-W 6.4.4.11
146685	**Symptom:** Clients experienced low throughput for specific SSIDs. This issue is resolved by adding an unallocated token to the traffic management shared pool. **Scenario:** This issue occurred when three VAPs were enabled with no clients and AOS-W recycled the bandwidth allocation tokens and added them in the traffic management shared pool. However, when the three VAPs were disabled, the shared pool was empty and the tokens were lost. This issue was observed in switches running AOS-W 6.4.2.6.	AP-Wireless	All platforms	AOS-W 6.4.2.6	AOS-W 6.4.4.11

Table 4: *Resolved Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
147195	**Symptom:** The value of **NAS-Port-Type** RADIUS attribute was set to **19 (Wireless-User-Type)** when a RAP was authenticated by an external server. This issue is resolved by setting the value of the **NAS-Port-Type** RADIUS attribute to **15 (Wired-User-Type)**. **Scenario:** This issue was observed in switches running AOS-W 6.3.1.16.	RADIUS	All platforms	AOS-W 6.3.1.16	AOS-W 6.4.4.11
147214	**Symptom:** The log file in a switch showed the **An internal system error has occurred at file sapd_msg.c function sapd_papi_snd_cb line 1484 error Message to 127.0.0.1:RF Client failed: err Connection timed out msgcode 1003 arg 0x649324** error. This issue is resolved by not sending the log configuration file to the AP. **Scenario:** This issue occurred because the AP did not support log configuration file. This issue was observed in OAW-AP125 access points running AOS-W 6.4.4.9.	AP-Wireless	OAW-AP125 access points	AOS-W 6.4.4.9	AOS-W 6.4.4.11
147749 148987	**Symptom:** Clients observed performance and connectivity issue in the wireless network. The fix ensures that the clients stay connected without any performance degradation. **Scenario:** This issue occurred when a switch received corrupted packets. This issue was observed in switches running AOS-W 6.4.3.x or later versions.	Station Management	All platforms	AOS-W 6.4.3.6	AOS-W 6.4.4.11
147959 148668	**Symptom:** The configuration on a local switch was truncated and the AP groups were lost after master-local synchronization. The fix ensures that the issue with the truncation of configuration on the local switch is resolved. **Scenario:** This issue was observed in OAW-4650 switches running AOS-W 6.4.3.10.	Master-Local	OAW-4650 switches	AOS-W 6.4.3.10	AOS-W 6.4.4.11

Table 4: *Resolved Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
148103	**Symptom:** One-way audio was observed in Vocera communication badges. The fix ensures that the **R** (Roamed client) flag is added to the session if it belongs to a roamed user. **Scenario:** This issue occurred when: • The clients performed an L3 roaming. • The roamed client made a call to a client associated to the switch as a local client. For the roamed client, the switch acted as a foreign agent. This issue was observed in switches running AOS-W 6.4.2.x or later versions.	UCC	All platforms	AOS-W 6.4.2.13	AOS-W 6.4.4.11
148113	**Symptom:** A client failed to get an IP address when it roamed between APs. The fix ensures that a client gets an IP address when it roams between APs. **Scenario:** This issue was observed when: • L3 mobility was enabled globally. • Mobile-IP was disabled on a VAP. This issue was observed in switches running AOS-W 6.4.2.8.	Mobility	All platforms	AOS-W 6.4.2.8	AOS-W 6.4.4.11
148371	**Symptom:** OV3600 showed null data for **AP Operational Status**, **Duplex**, **Input Capacity**, and **Output Capacity** parameters. This issue is resolved by checking and counting the redundancy state of an AP. If the redundancy state of an AP is UP, STANDBY_UP, STANDBY_READY, or STANDBY, they are counted as up. **Scenario:** This issue occurred because an AP did not send the port status update to a switch when high availability was enabled with CPsec. This issue was observed in OAW-AP205H access points running AOS-W 6.4.4.8.	AP-Platform	OAW-AP205H access points	AOS-W 6.4.4.8	AOS-W 6.4.4.11
148630	**Symptom:** There was a miscalculation in the DHCP time-stamp difference, which was a part of the AMON message. The fix ensures optimization in the calculation of the DHCP difference stamp to improve the precision of the DHCP difference values sent as part of the DHCP AMON message. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.10.	Clarity-Live	All platforms	AOS-W 6.4.4.10	AOS-W 6.4.4.11

Table 4: *Resolved Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
148671	**Symptom:** Some APs discovered the master switch through Automatic Data Processing (ADP) although DHCP options was configured to 43/60. The fix ensures that the APs discover the master switch through DHCP. **Scenario:** This issue was observed when an AP received an IPv6 address and the master switch was discovered using ADP. When the AP received an IPv4 address and discovered another master switch through DHCP, the AP was unable to recover the master switch through ADP. This issue was observed in switches running AOS-W 6.4.3.7.	AP-Platform	All platforms	AOS-W 6.4.3.7	AOS-W 6.4.4.11
148995	**Symptom:** A syslog server showed multiple kernel messages in the **<busybox or modprobe> used greatest stack depth: x byte left** format. This issue is resolved by disabling the debug kernel messages. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.9.	AP-Platform	All platforms	AOS-W 6.4.4.9	AOS-W 6.4.4.11
149307 149555	**Symptom:** An AP showed incorrect High Availability (HA) information and clients lost connectivity. The fix ensures that during HA failover, the **AP management** process has the same state with kernel module. **Scenario:** This issue occurred during HA failover when an AP did not receive a failover response from the standby switch. This resulted in the **AP management** process to be in a different state than the kernel module. This issue was observed in access points running AOS-W 6.4.4.8.	AP-Platform	All platforms	AOS-W 6.4.4.8	AOS-W 6.4.4.11
149744	**Symptom:** Captive Portal showed the internal server error page. This issue is resolved by checking if referer URL is null. **Scenario:** This issue occurred when the user login to Captive Portal failed. During HTTPS redirect, HTTP post was configured on ClearPass Policy Manager and the client did not send the referer URL in the HTTP post. This issue was not limited to any specific switch model and was observed in AOS-W 6.4.4.8.	Captive Portal	All platforms	AOS-W 6.4.4.8	AOS-W 6.4.4.11

Table 4: *Resolved Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
149941	**Symptom:** An AP had to be rebooted manually to connect with a master switch. This issue is resolved by allowing the AP to connect to the master switch automatically. **Scenario:** This issue occurred when the traffic between an AP and a master switch was blocked for some time and the AP terminated the connection with the standby switch. This issue was observed in switches running AOS-W 6.4.4.9 in a master-standby topology.	AP-Platform	All platforms	AOS-W 6.4.4.9	AOS-W 6.4.4.11
150488	**Symptom:** An AP did not allow more than 49 devices to associate with it. The fix allows more than 49 devices to associate with the AP. **Scenario:** This issue occurred when WPA-PSK-AES encryption was used with bridge mode. This issue was observed in OAW-AP204, OAW-AP205, OAW-AP214, OAW-AP215, OAW-AP224, OAW-AP225, or OAW-AP275 access points running AOS-W 6.4.4.9.	AP-Wireless	OAW-AP204, OAW-AP205, OAW-AP214, OAW-AP215, OAW-AP224, OAW-AP225, and OAW-AP275 access points	AOS-W 6.4.4.9	AOS-W 6.4.4.11
150578	**Symptom:** An AP did not forward RTP frames to its uplink randomly. The fix ensures that the AP forwards the RTP frames to its uplink as expected. **Scenario:** This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.9.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.9	AOS-W 6.4.4.11
150838 152014 152015	**Symptom:** A Galaxy Player YP-GS1 client running Android 2.3.6 passed authentication but did not show up in the user table. The fix ensures that YP-GS1 clients show up in the user table. **Scenario:** This issue occurred when High Throughput (HT) was enabled in an AP. This issue was observed in access points running AOS-W 6.4.4.10.	AP-Wireless	All platforms	AOS-W 6.4.4.10	AOS-W 6.4.4.11

Table 4: *Resolved Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
151674	**Symptom:** Multiple RADAR detections were observed on all DFS channels of an AP. This issue is resolved by fixing one or more of the following: • Adding RSSI pulse variation rejection for ETSI domain • Increasing threshold to 50% for ETSI type 3 and type 4 • Increasing precision from +/- 24 usec to +/- 4 usec **Scenario:** This issue was observed in OAW-AP324 and OAW-AP325 access points running AOS-W 6.4.4.6.	AP-Wireless	OAW-AP324 and OAW-AP325 access points	AOS-W 6.4.4.6	AOS-W 6.4.4.11
152499	**Symptom:** Some APs did not establish VPN session with a switch. This issue is resolved by deleting the older security associations except the budding security association. **Scenario:** This issue occurred when an AP reconnected to a switch but its source port changed during the reconnection. The inner IP was not cleared as part of security association cleanup and all security associations, including the budding security association, were cleared. This issue was observed in access points running AOS-W 6.4.4.9.	IPsec	All platforms	AOS-W 6.4.4.9	AOS-W 6.4.4.11
152908	**Symptom:** Multiple processes crashed in a switch unexpectedly. The log file listed the reason for the event as **Nanny rebooted machine - fpapps process died (Intent:cause:register 34:86:50:2)**. This issue is resolved by deleting the security associations that are not marked as **ready** or when negotiations fail. **Scenario:** This issue occurred when a budding security association was freed but the allocated memory was not deleted. This issue was observed in switches running AOS-W 6.4.4.9.	Switch-Platform	All platforms	AOS-W 6.4.4.9	AOS-W 6.4.4.11

This chapter describes the known and outstanding issues identified in AOS-W 6.4.4.11.

Support for OAW-AP320 Series Access Points

The following features are not supported in OAW-AP320 Series access points:

- Enterprise Mesh
- Turbo QAM
- Modem Support
- Radio Frequency Test (RFT)

If there is any specific bug that is not documented in this chapter, contact Alcatel-Lucent Technical Support with your case number.

Table 5: *Known Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version
104874 139962 149550 150743	**Symptom:** Stale entries are not always removed from the **STM** process or the driver in an AP. **Scenario:** This issue is observed in access points running AOS-W 6.4.3.0. **Workaround:** None.	Station Management	All platforms	AOS-W 6.4.3.0
106465 144676	**Symptom:** An AP crashes unexpectedly. **Scenario:** This issue is observed in OAW-AP205 and OAW-AP225 access points running AOS-W 6.4.4.10 **Workaround:** None.	AP-Platform	OAW-AP205 and OAW-AP225 access points	AOS-W 6.4.4.10
115260 128209	**Symptom:** When a user tries to physically reboot a switch, it fails to reboot with the **Not enough space on flash** error. **Scenario:** This issue occurs when backup flash operation is performed regularly. When user is unable to reach a switch over SSH or WebUI, the user tries to physically reboot the switch. After power cycling, the switch gets stuck at restoring database (indicated by LED). After getting console access, the user sees the **Not enough space on flash** error. This issue is observed in switches running AOS-W 6.4.2.x. **Workaround:** Contact Alcatel-Lucent Technical Support to remove the corrupted database and recover the switch.	Switch-Platform	All platforms	AOS-W 6.4.2.12
122479	**Symptom:** The log file of a switch shows the **|lldp| GSM PORT_INFO Lookup failed at Function: lldp_recv for port 17 result 43** interface-related error. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.8. **Workaround:** None.	LLDP	All platforms	AOS-W 6.4.2.8
123458	**Symptom:** An AP fails to send Link Layer Discovery Protocol-Media Endpoint Discovery (LLDPMED) Type-Length-Value (TLV) information after receiving an LLDP packet from a Cisco VoIP phone. **Scenario:** This issue occurs when devices that support LLDP-MED are connected to the downlink Ethernet port of an AP. This issue is observed in access points running AOS-W 6.4.3.3. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.3.3

Table 5: *Known Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version
124275 151661	**Symptom:** All clients obtain IP addresses from the same VLAN even though a RADIUS server Vendor-Specific Attribute (VSA) specifies a VLAN pool with multiple VLANs. **Scenario:** This issue occurs when a RADIUS server VSA overrides the VAP VLAN 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. **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:** When a SIP call is made using the ClearSea application, a Call Detail Record (CDR) is not generated. The call detail is not visible on the Unified Communication and Collaboration (UCC) dashboard and the media traffic is not prioritized. **Scenario:** The issue is observed only when the SIP signaling message is large, is delivered in multiple Transmission Control Protocol (TCP) segments, and the TCP segments are received out of order. This issue is observed in switches running AOS-W 6.4.2.4. **Workaround:** None.	Unified Communication and Collaboration	All platforms	AOS-W 6.4.2.4
126244 133950 136632 136957 141924 151877	**Symptom:** The status of an AP does not match between a master switch and a local switch. **Scenario:** This issue occurs when an AP moves from one IPv4 interface to another IPv4 interface or a IPv6 interface on the same switch. This issue is observed in access points running AOS-W 6.4.2.5. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.2.5
126727 139011	**Symptom:** The MaxEIRP value does not match between a mesh point and a mesh portal. **Scenario:** This issue is observed when a mesh point and a mesh portal are connected to OAW-AP274 access points running AOS-W 6.4.3.2. **Workaround:** None.	Mesh	OAW-AP274 access points	AOS-W 6.4.3.2
127660	**Symptom:** The WebUI does not have an option to configure a Network Access Server (NAS) IP address in the **Configuration > BRANCH > Smart Config** page. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.1. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.4.1

Table 5: *Known Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version
127848 151629	**Symptom:** A remote AP fails to re-establish its Point-to-Point Protocol over Ethernet (PPPoE) connection to the backup Local Management Switch (LMS) IP address when the primary LMS IP address is not available. **Scenario:** This issue is observed in OAW-AP205 or OAW-AP274 access points running AOS-W 6.4.4.0. **Workaround:** None.	Remote Access Point	OAW-AP205 and OAW-AP274 access points	AOS-W 6.4.4.0
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. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.3.1
130981	**Symptom:** A switch reboots unexpectedly. The log file lists the reason for the event as **datapath timeout**. **Scenario:** This issue occurs when the copy command has the \\ (backslash) character at the end of the destination folder name. For example: copy flash: crash.tar ftp: 10.1.1.1. test-user \ArubaOS\\ crash.tar ArubaOS misinterprets the \\ (backslash) character causing a memory fault. This issue is observed in switches running AOS-W 6.4.4.0. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.4.0
131857	**Symptom:** The Type of Service (TOS) value of 0 does not take effect when it is set in the user role. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.3. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.3.3
132714	**Symptom:** When a user tries to add a static ARP entry, a switch shows 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. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.3.4

Table 5: *Known Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version
137196	**Symptom:** A switch fails to respond and reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout**. **Scenario:** This issue occurs when Virtual Internet Access (VIA) is used with Secure Socket Layer (SSL) fallback. This issue is not limited to any specific switch model or AOS-W version. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.0.3
138438	**Symptom:** A user cannot enable DHCP client on a VLAN using the WebUI. **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
138462	**Symptom:** The **SNMPD** process in a switch is in **PROCESS_NOT_RESPONDING_CRITICAL** state. **Scenario:** This issue is observed in local switches running AOS-W 6.4.2.12 in a master-standby-local topology. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.2.12
139981	**Symptom:** A user cannot see page 5 in the internal database although the user can see pages 1 through 4. **Scenario:** This issue occurs because of a corrupt entry in the user database. This issue is observed in switches running AOS-W 6.4.2.14. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.2.14
140049	**Symptom:** An AP takes more time than usual to boot. **Scenario:** This issue occurs when CPsec is enabled in 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
140805	**Symptom:** Configuring multiple DHCP options in the DHCP pool using the **Configuration > Branch > Smart config > Routing > DHCP options** page in the WebUI fails. **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 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version
141686 131777 138008	**Symptom:** A branch switch does not communicate with a master switch. **Scenario:** This issue occurs when the **ip nat outside** option is enabled on the uplink of the branch switch and 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
141822 143282	**Symptom:** The **Authentication** process in a switch crashes unexpectedly. **Scenario:** This issue occurs when the following changes are made to the AAA profile: • 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 version. **Workaround:** None.	RADIUS	All AP platforms	AOS-W 6.4.2.12
142397	**Symptom:** IPv4 syslog messages are interpreted incorrectly because of an invalid timestamp format. **Scenario:** This issue occurs because the timestamp in the syslog message for IPv4 address includes the year at the end, which is not according to the standards. This issue is not limited to any specific switch model or AOS-W version. **Workaround:** None.	RADIUS	All platforms	AOS-W 6.4.4.6
142678	**Symptom:** Adding a NTP server to a switch causes all the remote access points to reconnect without notification. **Scenario:** This issue occurs when the NTP server tries to correct the time difference in a switch. This issue is not limited to any specific switch model or AOS-W 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 on eth1 port. **Scenario:** This issue is observed in OAW-AP103H access points running AOS-W 6.4.4.6. **Workaround:** None.	AP Datapath	OAW-AP103H access points	AOS-W 6.4.4.6

Table 5: *Known Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version
143566	**Symptom:** A switch shows the **Module authentication is busy. Please try later** error message when the **show reference user-role game-guest** command is executed. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.16 in a master-local topology. **Workaround:** None.	Configuration	All platforms	AOS-W 6.4.2.16
144039 150966	**Symptom:** The **Datapath** process in a switch crashes unexpectedly. **Scenario:** This issue occurs when a reputation-based deny ACL rule is configured and random URLs falling in the specific reputation range are sent to a switch. This issue is observed in switches running AOS-W 6.4.4.6. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.4.6

144768
145436
	Symptom: An AP reboots when a Hotspot 2 client sends a request for a parameter defined in the **STM** process.
	Scenario: This issue is observed in OAW-AP135 access points running AOS-W 6.4.2.17.
	Workaround: Execute the following command to disable Hotspot 2.0 support in the AOS-W firmware:
	`(host) (config) #wlan hotspot hs2-profile myhs2`
	`(host) (Hotspot 2.0 Profile "myhs2") #no advertisement-profile`
		Hotspot	OAW-AP135 access points	AOS-W 6.4.2.17

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. This issue occurs because a packet that the application receives is corrupt and validation is not done on the application. This issue is observed in switches running AOS-W 6.2.1.5. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.4.6
145867	**Symptom:** An AP does not boot. The log file lists the reason for the event as **Kernel panic - not syncing: Fatal exception**. **Scenario:** This issue is observed in OAW-AP275 APs running AOS-W 6.4.3.9. **Workaround:** None.	AP-Wireless	OAW-AP275 access points	AOS-W 6.4.3.9

Table 5: *Known Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version
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. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.3.9-FIPS
147300	**Symptom:** A switch fails to respond and reboots unexpectedly. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.6. **Workaround:** None.	Station Management	All platforms	AOS-W 6.4.3.6
148249 148251 148252 148263	**Symptom:** A switch is not accessible after it is rebooted by unplugging the power cable multiple times. **Scenario:** This issue occurs when a switch is hard rebooted multiple times immediately after saving the configuration. This issue is limited to OWA-4005switches. **Workaround:** Reset the switch to factory default configuration.	Switch-Platform	OWA-4005switches	AOS-W 6.4.3.9
148416 149211	**Symptom:** The **STM** process in a switch crashes unexpectedly. **Scenario:** This issue is observed in OAW-4550 switches running AOS-W 6.4.3.4. **Workaround:** None.	Station Management	OAW-4550switches	AOS-W 6.4.3.4
149131	**Symptom:** A switch sends only primary port information through AMAP of the LACP link. **Scenario:** This issue occurs when the port-channel interfaces and AMAP are enabled and the packets are sent on the port-channel interfaces rather than individual interfaces. This issue is not limited to any specific switch model or AOS-W version. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.3.10

149372	**Symptom:** Clients fail to connect to some APs randomly until the APs are rebooted.
	Scenario: This issue occurs after a channel change is triggered on the APs because of RADAR detection. This issue is observed on APs running AOS-W 6.4.4.6 or later versions.
	Workaround: Disable the channel switch announcement on the AP using the following CLI commands:
	`(host) (config) #rf dot11a-radio-profile default`
	`(host) (802.11a radio profile "default") #no csa`
		AP-Wireless	All AP platforms	AOS-W 6.4.4.6

Table 5: *Known Issues in 6.4.4.11*

Bug ID	Description	Component	Platform	Reported Version
150337	**Symptom:** A Vocera B3000N communication badge fails to connect to the wireless network. **Scenario:** This issue is observed when the communication badge associates with an 802.11ac Wave 2 AP. This issue is observed in OAW-AP320 Series access points running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.4.4.9
150693	**Symptom:** The datapath route-cache entry is not cleared when an L3 GRE tunnel is closed. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.9. **Workaround:** None.	OSPF	All platforms	AOS-W 6.4.3.9
151105 151106	**Symptom:** Some APs do not communicate with a Meridian server. **Scenario:** This issue is observed in OAW-AP215 access points running AOS-W 6.4.4.8. **Workaround:** None.	Bluetooth Low Energy	OAW-AP215 access points	AOS-W 6.4.4.8
151431	**Symptom:** The **Proxy-State** attribute is missing in **Disconnect-ACK** or **COA-ACK** message sent from a switch in response to the corresponding **Disconnect-Request** or **COA-Request** message received with **Proxy-State** attribute. This behavior does not comply with RFC 3576/5176. **Scenario:** This issue is observed in switches running AOS-W 6.4.2.6. **Workaround:** None.	RADIUS	All platforms	AOS-W 6.4.2.6
151483	**Symptom:** The output of the **show ap debug aid-table bssid <bssid>** command shows null MAC addresses and the output of the **show ap debug client-table** command shows many stale entries with long association times. **Scenario:** This issue is observed in OAW-AP325 access points running AOS-W 6.4.4.8. **Workaround:** None.	AP-Platform	OAW-AP325 access points	AOS-W 6.4.4.8
151605 152410	**Symptom:** A client does not send or receive traffic. **Scenario:** This issue occurs when a client sends IP packets before DHCP and the ACL in the datapath user and user table do not match. This issue is observed in switches running AOS-W 6.4.4.6. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.4.6

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 WebUIs 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) and OAW-4504XM switches 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 37.)

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 36 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 36 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 36 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 36.

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 6.4.4.11

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 6.4.4.11

The following sections provide the procedures for upgrading the switch to AOS-W 6.4.4.11 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 35.

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 6.4.4.11.

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 6.4.4.11 on page 38 to install the interim version of AOS-W, and then repeat steps 1 through 11 of the procedure to download and install AOS-W 6.4.4.11.

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

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

4. Log in to the AOS-W WebUI from the PC or workstation.
5. Navigate to the **Maintenance > 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 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 36 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 35.

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 6.4.4.11 on page 38.

Follow steps 2 through 7 of the procedure described in Upgrading to AOS-W 6.4.4.11 on page 38 to install the interim version of AOS-W, and then repeat steps 1 through 7 of the procedure to download and install AOS-W 6.4.4.11.

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 6.4.4.11 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 36 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 6.4.4.11 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 6.4.4.11 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 36.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W 6.4.4.11 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 6.4.4.11 flash backup from the file stored on the switch. Do not restore the AOS-W 6.4.4.11 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 6.4.4.11, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W 6.4.4.11, 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 6.4.4.11 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
ALE	Analytics and Location Engine

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
BPDU	Bridge Protocol Data Unit
BRAS	Broadband Remote Access Server

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
CoA	Change of Authorization
CoS	Class of Service
CPE	Customer Premises Equipment

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
DCF	Distributed Coordination Function
DDMO	Distributed Dynamic Multicast Optimization
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
DST	Daylight Saving Time
DTE	Data Terminal Equipment
DTIM	Delivery Traffic Indication Message
DTLS	Datagram Transport Layer Security
DU	Data Unit

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
EIGRP	Enhanced Interior Gateway Routing Protocol
EIRP	Effective Isotropic Radiated Power
EMM	Enterprise Mobility Management
ESI	External Services Interface
ESS	Extended Service Set

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
Gbps	Gigabits per second
GHz	Gigahertz
GIS	Generic Interface Specification
GMT	Greenwich Mean Time
GPP	Guest Provisioning Page
GPS	Global Positioning System

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
LED	Light Emitting Diode
LEEF	Long 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
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

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SDU	Service Data Unit
SD-WAN	Software-Defined Wide Area Network
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
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

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SoH	Statement of Health
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
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

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
TPC	Transmit Power Control
TPM	Trusted Platform Module
TSF	Timing Synchronization Function
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

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
VBN	Virtual Branch Networking
VBR	Virtual Beacon Report
VHT	Very High Throughput
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

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
WINS	Windows Internet Naming Service
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