AOS-W 6.4.4.10

Alcatel·Lucent
Enterprise

Release Notes

Open Source Code

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

Contents

Contents 3

Revision History 5

Release Overview 6

Important Points to Remember 6

Supported Browsers 8

Contacting Support 8

New Features 10

Regulatory Updates 11

Resolved Issues 12

Known Issues 25

Upgrade Procedure 32

Upgrade Caveats 32

GRE Tunnel-Type Requirements 33

Important Points to Remember and Best Practices 33

Memory Requirements 34

Backing up Critical Data 35

Upgrading in a Multiswitch Network 36

Installing the FIPS Version of AOS-W 6.4.4.10 36
Upgrading to AOS-W 6.4.4.10 37
Downgrading 41
Before You Call Technical Support 43
Acronyms and Abbreviations 44

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 6.4.4.10 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 11 lists the regulatory updates introduced in this release.
- Resolved Issues on page 12 describes the issues resolved in this release.
- Known Issues on page 25 describes the known and outstanding issues identified in this release.
- Upgrade Procedure on page 32 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://service.esd.alcatel-lucent.com
Email	esd.support@alcatel-lucent.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 6.4.4.10.

Security Update

Revocation of AOS-W Default Certificate Issued by GeoTrust

The switch-issued server certificate replaces the AOS-W default certificate issued by **GeoTrust Public CA** for WebUI authentication, Captive Portal, 802.1X termination, and Single Sign-On (SSO) because the default certificate is now revoked.

For more information on the **GeoTrust Public CA** certificate revocation, refer to the advisory.

Using the switch-issued server certificate has the following caveats:

- When MacBook or iOS devices connect to Captive Portal, the CNA (Captive Network Assistant) popup does not appear. So, you must open a browser to get redirected to a Captive Portal page.
- When the Captive Portal custom welcome page is configured in Mac Safari 8.1, the certificate warning pops up as soon as the welcome page appears.
- WISPr authentication fails on the switch.
- Authentication Survivability fails on Windows clients using EAP-TLS authentication.
- 802.1X PEAP authentication fails on Windows 7 clients. So, you must disable the **Validate Server Certificate** option on the Windows 7 clients.

It is recommended to use custom certificates to avoid these caveats.

Switch-Platform

Copy Files from FTP to Flash

You can download an AOS-W image file onto a switch from a TFTP, FTP, or SCP server. Starting from AOS-W 6.4.4.10, the switch CLI has an option to copy files from FTP to flash.

```
copy ftp: <ftphost> <user> <filename> {flash: <destfilename> | system: partition [0|1]}
```

Chapter 3
Regulatory Updates

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

For a complete list of countries 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 6.4.4.10:

- DRT-1.0_56643

This chapter describes the issues resolved in AOS-W 6.4.4.10.

Table 4: *Resolved Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
104094	**Symptom:** The **STM** process did not free memory after deleting or changing an SSID. The fix ensures that the **STM** process frees memory after deleting or changing an SSID. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.9.	Other	All platforms	AOS-W 6.4.4.9	AOS-W 6.4.4.10
113765 141672	**Symptom:** When a user issued a command to delete SNMP trap hosts, the entries were not deleted on the switch. This issue is resolved by adding a check to ensure that the same user is not referenced to different targets. **Scenario:** This issue occurred when the same user was configured for different targets and the entire list was deleted. When one host was deleted, the CLI deleted the user parameters. Subsequent delete commands did not locate the user and the SNMP trap hosts were not deleted. This issue was observed in switches running AOS-W 6.4.3.0.	SNMP	All platforms	AOS-W 6.4.3.0	AOS-W 6.4.4.10
124971 143929 144813 144831	**Symptom:** A switch showed the wrong memory usage thresholds for the **STM** process. This issue is resolved by calculating and showing the correct memory usage thresholds. **Scenario:** This issue occurred because the switch calculated the wrong memory usage thresholds. This issue was observed in switches running AOS-W 6.4.4.0.	Station Management	All platforms	AOS-W 6.4.4.0	AOS-W 6.4.4.10

Table 4: *Resolved Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
126440 127145 140733 144633	**Symptom:** Clients lost connectivity and were unable to send/receive traffic when debug log was enabled. This issue is resolved by removing the reason name mapping in the debug logs for the error codes received from the 802.11K beacon reports. **Scenario:** This issue occurred because the background code value that was mapped to the corresponding string for 802.11K beacon report was out of range. This issue was observed in switches running AOS-W 6.3.x or AOS-W 6.4.x.	Station Management	All platforms	AOS-W 6.3.1.14	AOS-W 6.4.4.10
126616 145721	**Symptom:** Wired users were assigned to wrong VLAN 4095. This issue is resolved by checking for rap-backup before performing MAC authentication or 802.1X authentication. **Scenario:** This issue occurred when a tunnel mode wired AP with MAC authentication was configured. If rap-backup was enabled and a remote AP disconnected from a switch, the wired AP was converted into bridge mode with VLAN 4095. This issue was observed in remote access points running AOS-W 6.3.1.9.	AP Datapath	All remote access points	AOS-W 6.3.1.9	AOS-W 6.4.4.10
126905	**Symptom:** Only 99 user derivation rules were retained after a switch was rebooted although 100 or more user derivation rules were configured. The fix ensures that all user derivation rules are retained after a switch is rebooted. **Scenario:** This issue was observed when the **show aaa derivation-rules user** command was executed after a switch was rebooted. This issue was not limited to any specific switch model or AOS-W version.	Base OS Security	All platforms	AOS-W 6.4.2.8	AOS-W 6.4.4.10
129692 138741	**Symptom:** APs rebooted when the master switch failed. The fix ensures that High Availability (HA) is functional when access points reboot to the Backup Local Management Switch (BLMS). **Scenario:** APs were unable to establish a standby tunnel with the LMS if the LMS was not reachable when the access points attempted to connect for the first time. This issue was observed in OAW-4550 switches running AOS-W 6.4.2.10 in a master-standby-master topology.	AP-Platform	OAW-4550 switches	AOS-W 6.4.2.10	AOS-W 6.4.4.10

Table 4: *Resolved Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
134394 146970	**Symptom:** The configuration of an AP was lost and the AP rebooted repeatedly. This issue is resolved by adding an entry in the sector **FAT** to record the backup environment configuration. **Scenario:** This issue occurred because of a missing boot environment configuration. This issue was observed in OAW-AP105 access points running AOS-W 6.4.3.3.	AP-Platform	OAW-AP105 access points	AOS-W 6.4.3.3	AOS-W 6.4.4.10
134677	**Symptom:** When a user deleted an Access Control List (ACL) with attributes similar to the **Time Ranges** ACL, the ACL listed under the **Time Ranges** tab in the WebUI was also deleted. This issue is resolved by restricting the generation of the delete command for ACLs that have attributes similar to the **Time Ranges** ACLs. **Scenario:** This issue occurred only when an ACL was deleted using the WebUI. This issue was observed in switches running AOS-W 6.4.2.5.	WebUI	All platforms	AOS-W 6.4.2.5	AOS-W 6.4.4.10
134719	**Symptom:** An AP sent frequent TX power decrease messages to a switch because the switch did not process the power change request message. This issue is resolved by skipping the firewall configuration updates from the AP which might cause a delay in processing the power change request. **Scenario:** This issue was observed when the power or channel setting in the ARM profile of a switch was changed. This issue was limited to bridge mode access points or remote access points but not limited to any AOS-W version.	ARM	All platforms	AOS-W 6.4.4.9	AOS-W 6.4.4.10
134824 139171 142938 147661 147662	**Symptom:** A switch crashed unexpectedly and while rebooting, it got into additional exceptions. The log file listed the reason for the event as **Kernel panic**. The fix ensures that the switch reboots and the debug details are stored so the original cause of reboot can be identified. **Scenario:** 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 6.4.4.10

Table 4: *Resolved Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
135029 137672	**Symptom:** The **Monitoring > NETWORK > All Access Points** page in the WebUI showed an incorrect user count. The fix ensures that the WebUI shows the correct user count. **Scenario:** A mismatch in the user count was observed between the **Monitoring** and **Dashboard** pages of the WebUI. Thismismatch was not seen in the CLI. This issue was observed in switches running AOS-W 6.4.2.12, AOS-W 6.4.3.x, or AOS-W 6.4.4.x.	WebUI	All platforms	AOS-W 6.4.2.12	AOS-W 6.4.4.10
135284 137416	**Symptom:** The **Signal to Noise Ratio** (SNR) and **RSSI** columns in the output of the **show ap monitor ap-list** command showed **0**. This issue is resolved by showing the correct SNR and RSSI values in the output of the **show ap monitor ap-list** command. **Scenario:** This issue was observed in OAW-AP220 Series access points running AOS-W 6.4.4.0.	Air Management-IDS	OAW-AP220 Series access points	AOS-W 6.4.4.0	AOS-W 6.4.4.10
135450	**Symptom:** Rate selection used a higher MCS without checking if the transmission frame was a retransmission frame. This issue is resolved by not using higher MCS for a retransmission frame. **Scenario:** This issue was observed when rate selection used higher MCS for a retransmission frame. This issue was observed in access points running ArubaOS 6.4.4.9.	AP-Wireless	All platforms	AOS-W 6.4.4.9	AOS-W 6.4.4.10
135841	**Symptom:** A discrepancy in the month was observed when a user viewed the clock through the WebUI and the CLI. This issue is resolved by not allowing the addition of a month while retrieving data from the **show clock** command. **Scenario:** When a user navigated to **Monitoring > Controller > Uplink > Uplink Management** and **Monitoring > Controller > Universal Serial Bus > USB Devices** pages, the date displayed in the clock was a month ahead of what was displayed when the **show clock** command was executed in the CLI. This issue was observed in OAW-40xx Series switches running AOS-W 6.4.3.6.	WebUI	OAW-40xx Series switches	AOS-W 6.4.4.0	AOS-W 6.4.4.10

Table 4: *Resolved Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
136884 148573	**Symptom:** An AP sent data to the **STA** process in Power Save (PS) mode. This issue is resolved by not sending ACK frames during channel change. **Scenario:** This issue occurred when the hardware sent ACK frames during channel change and the firmware did not receive the ACK frames. 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 6.4.4.10
137031	**Symptom:** A client was unable to associate to the 2.4 GHz radio of an AP intermittently. This issue is resolved by resetting the striping IP when an AP fails over to a backup LMS or preempts back to the main LMS. **Scenario:** This issue occurred when LACP striping IP was configured on the backup LMS but not on the primary LMS. When an AP failed over to the backup LMS or preempted back to the primary LMS, it retained the striping IP provided by the backup LMS. The AP continued to send traffic on the 2.4 GHz radio to the backup LMS. The local switch dropped this traffic because the virtual AP profiles were not registered. This issue was observed in OAW-AP225 access points running AOS-W 6.4.3.4.	AP-Platform	OAW-AP225 access points	AOS-W 6.4.3.4	AOS-W 6.4.4.10
137339 145475	**Symptom:** Port-channel links were not visible in the NMS tool (OV server). This issue is resolved by adding port-channel interface details. **Scenario:** This issue occurred when a switch did not return the port-channel interfaces. This issue was observed in switches running AOS-W 6.4.3.4.	SNMP	All platforms	AOS-W 6.4.3.4	AOS-W 6.4.4.10
137565 142892	**Symptom:** An AP crashed unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue occurred when AP uplink VLAN was configured and large UDP packets were sent from clients. This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.6.	AP Datapath	OAW-AP325 access points	AOS-W 6.4.4.6	AOS-W 6.4.4.10

Table 4: *Resolved Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
137809 144262 145804 145814	**Symptom:** Some client devices (vendor-specific) did not get their respective DHCP IP address on WPA2-PSK-AES or 802.1x-EAP SSID. This issue was not observed in devices with Open or WPA2-PSK-TKIP SSID. The fix ensures that clients get their respective DHCP IP address. **Scenario:** The issue was triggered when reprovisioning an AP from a group with HT-enabled rf-profile to that with HT-disabled rf-profile. This issue was observed in OAW-AP200 Series, OAW-AP205H, OAW-AP210 Series, OAW-AP220 Series, OAW-AP228, and OAW-AP270 Series access points running AOS-W 6.3.1.7.	AP-Platform	OAW-AP200 Series, OAW-AP205H, OAW-AP210 Series, OAW-AP220 Series, OAW-AP228, and OAW-AP270 Series access points	AOS-W 6.3.1.7	AOS-W 6.4.4.10
138093	**Symptom:** The **STM** process in a switch crashed multiple times. The fix ensures that the **STM** process does not crash. **Scenario:** The backup LMS failed to handle a large number of AP fallbacks. The switch ran out of memory and failed to restart the **STM** process. This issue was observed in switches running AOS-W 6.4.2.x or AOS-W 6.5.x.	Station Management	All platforms	AOS-W 6.4.2.8	AOS-W 6.4.4.10
138271	**Symptom:** For High Throughput (HT) and Very High Throughput (VHT) 80 MHz channels, a switch sent the AMON messages with incorrect radio information to the AirWave server. The fix ensures that the switch checks the channel type and populates the AMON messages with the correct radio information. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.x or AOS-W 6.4.4.x.	Station Management	All platforms	AOS-W 6.4.4.4	AOS-W 6.4.4.10
138320	**Symptom:** A wired user role did not change when a client moved from one VLAN to another. This issue is resolved by prioritizing the initial role over the derived role. **Scenario:** This issue occurred when a wired client was passing traffic through a switch connected to a switch over an untrusted port. This issue was observed in switches running AOS-W 6.4.3.2.	Roles/VLAN Derivation	All platforms	AOS-W 6.4.3.2	AOS-W 6.4.4.10

Table 4: *Resolved Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
138637	**Symptom:** Frames with VLAN 0 on PROFINET protocol were dropped and not retransmitted. This issue is resolved by adding checks in the firewall to allow frames with VLAN 0. **Scenario:** This issue was observed in OAW-AP205 access points running AOS-W 6.4.3.4.	AP-Wireless	OAW-AP205 access points	AOS-W 6.4.3.4	AOS-W 6.4.4.10
138868 139336	**Symptom:** A switch classified and blocked the transmission of images sent from the WhatsApp application. The fix ensures that images sent from the WhatsApp application are transmitted. **Scenario:** This issue occurred because the latest version of WhatsApp application was not classified in the switch. This issue was observed in OAW-40xx Series or OAW-4x50 Series switches running AOS-W 6.4.3.7.	Switch-Datapath	OAW-40xx Series and OAW-4x50 Series switches	AOS-W 6.4.3.7	AOS-W 6.4.4.10
139174	**Symptom:** An AP did not populate the 64-bit Rx/Tx rate fields when sending an SNMP message for a client. The fix ensures that the AP sends the 64-bit Rx/Tx rate fields as part of the SNMP message. **Scenario:** This issue was observed in OAW-AP320 Series access points running AOS-W 6.4.4.x.	Station Management	OAW-AP320 Series access points	AOS-W 6.4.4.3	AOS-W 6.4.4.10
139189 147270 147641	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Fatal exception**. This issue is resolved by limiting the number of broadcasts and simultaneously reserving some memory for the broadcasts in the queue. **Scenario:** This issue occurred when multiple virtual APs were used in bridge mode. This issue was observed in OAW-AP225 access points running AOS-W 6.5.0.0.	AP-Platform	OAW-AP225 access points	AOS-W 6.5.0.0	AOS-W 6.4.4.10
139340	**Symptom:** A client that was connected to a wireless bridge did not get an IP address from a DHCP server. This issue is resolved by adding an indirect MAC entry for all clients behind a wireless bridge and sending DHCP packets over all tunnels in a VLAN if broadcast-filter-arp is disabled. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.7.	Switch-Datapath	All platforms	AOS-W 6.4.3.7	AOS-W 6.4.4.10

Table 4: *Resolved Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
139799	**Symptom:** The AirGroup CPPM server table was not populated if FQDN was configured instead of an IP address in RADIUS authentication server profile. This issue is resolved by adding checks to ensure that the AirGroup CPPM server is populated. **Scenario:** This issue occurred because of a memory leak. This issue was observed in switches running AOS-W 6.4.3.4.	Base OS Security	All platforms	AOS-W 6.4.3.4	AOS-W 6.4.4.10
140007	**Symptom:** IPv6 Virtual Router Redundancy Protocol (VRRP) was not functional on an untrusted VLAN or port. This issue is resolved by adding support for IPv6 VRRP on an untrusted VLAN or port. **Scenario:** This issue occurred when VRRP advertisement without IPsec was sent over an untrusted VLAN or port. This issue was observed in OAW-4750 switches running AOS-W 6.4.4.5.	Base OS Security	OAW-4750 switches	AOS-W 6.4.4.5	AOS-W 6.4.4.10
140171 146291	**Symptom:** A switch set the path cost of a mesh portal AP to 3 when the AP was connected to a 1 Gbps port. The fix ensures that the path cost is 0 when an AP connects to a 1 Gbps port. **Scenario:** This issue was observed in OAW-AP200 Series or OAW-AP210 Series access points running AOS-W 6.4.4.8.	Mesh	OAW-AP200 Series and OAW-AP210 Series access points	AOS-W 6.4.4.8	AOS-W 6.4.4.10
140327 144285 144288 144438 147584	**Symptom:** The memory usage of the **Authentication** process in a switch increased gradually. The fix ensures that the **Authentication** process does not leak memory **Scenario:** This issue occurred because of a slow memory leak. This issue was observed in switches running AOS-W 6.4.2.x or AOS-W 6.4.3.x.	Base OS Security	All platforms	AOS-W 6.4.3.3	AOS-W 6.4.4.10
140337 145917	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **FW assert**. The fix ensures that the AP works as expected. **Scenario:** This issue occurred because the Tx buffers were stuck in an AP. This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.7.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.7	AOS-W 6.4.4.10

Table 4: *Resolved Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
140731	**Symptom:** DHCP enforcement in the AAA profile failed in a switch for some clients connecting with static IP addresses. The fix ensures that the traffic from all clients with static IP address is blocked when DHCP enforcement is enabled in the AAA profile. **Scenario:** This issue occurred when MAC-OS clients with static IP address connected to a switch on which the DHCP enforcement was enabled in the AAA profile. This issue was observed in switches running AOS-W 6.4.3.x.	Switch-Datapath	All platforms	AOS-W 6.4.3.7	AOS-W 6.4.4.10
141221	**Symptom:** The **STM** process crashed in a switch. The fix ensures that the switch does not run out of memory and works as expected. **Scenario:** This issue occurred because a switch ran out of memory. This issue was observed in master switches running AOS-W 6.3.1.16 in a master-local topology.	Configuration	All platforms	AOS-W 6.3.1.16	AOS-W 6.4.4.10
141429 148041 148364 148551 149212	**Symptom:** An AP crashed unexpectedly. The log file listed the reason for the event as **Out of memory**. This issue is resolved by reducing the large transmit queue limit. **Scenario:** This issue was observed in OAW-AP205 access points running AOS-W 6.4.4.7.	AP-Platform	OAW-AP205 access points	AOS-W 6.4.4.7	AOS-W 6.4.4.10
142157	**Symptom:** The 5 GHz radio of an AP running in spectrum mode stopped responding. The fix ensures that the 5 GHz radio of an AP works as expected. **Scenario:** This issue was observed in access points running AOS-W 6.4.4.9.	Spectrum	All platforms	AOS-W 6.4.4.9	AOS-W 6.4.4.10
142257	**Symptom:** The **wlanAPName** trap failed to list all access points irrespective of their statuses. This fix ensures that the **wlanAPName** trap lists all access points. **Scenario:** This issue occurred when an SNMP walk action was performed on the **wlanAPName** trap. This issue was observed in switches running AOS-W 6.4.3.5.	SNMP	All platforms	AOS-W 6.4.3.5	AOS-W 6.4.4.10

Table 4: *Resolved Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
142856	**Symptom:** The bandwidth contract was not updated after a role change. This issue is resolved by updating the bandwidth contract when an L2 role is updated. **Scenario:** This issue occurred when the L2 role was changed for a user but the bandwidth contract was not updated if the user did not have an L3 role configured. This issue was observed in switches running AOS-W 6.4.3.7.	Base OS Security	All platforms	AOS-W 6.4.3.7	AOS-W 6.4.4.10
143119	**Symptom:** A browser session took more time than usual to terminate while accessing a switch on pot 8082. This issue is resolved by ignoring browser session on port 8082. **Scenario:** This issue occurred when an HTTP/HTTPS session was being created with switch IP address or any other accessible IP address on the switch on port 8082. An internal logic in the switch caused a loop and the session took long time to terminate. This issue was observed in switches running AOS-W 6.4.3.4.	WebUI	All platforms	AOS-W 6.4.3.4	AOS-W 6.4.4.10
143444	**Symptom:** A switch dropped PROFINET PN_DCP packets. This issue is resolved by allowing VLAN 0 priority tagged packets. **Scenario:** This issue occurred because a switch dropped all VLAN 0 priority tagged packets. This issue was observed in switches running AOS-W 6.4.3.7.	Switch-Datapath	All platforms	AOS-W 6.4.3.7	AOS-W 6.4.4.10
143931	**Symptom:** A custom captive portal background image was not displayed in the preview page of a VRRP standby switch. When the VRRP standby switch became the master switch, captive portal users saw a black page instead of a custom background image. This issue is resolved by: • Disabling **database synchronize captive-portal-custom** • Creating a new captive portal profile and uploading the background image and custom captive portal page on both master and standby switches **Scenario:** This issue was observed in switches running AOS-W 6.4.4.4 in a master-standby topology.	Database	All platforms	AOS-W 6.4.4.4	AOS-W 6.4.4.10

Table 4: *Resolved Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
144570 148449	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**. This issue is resolved by directly accessing the saved context data when crypto context is cleared. **Scenario:** This issue occurred when IPsec tunnels were closed and the queued crypto context was cleared. This issue was observed in OAW-AP200 Series, OAW-AP210 Series, or OAW-AP220 Series access points running AOS-W 6.4.4.8.	AP-Platform	OAW-AP200 Series, OAW-AP210 Series, and OAW-AP220 Series access points	AOS-W 6.4.4.8	AOS-W 6.4.4.10
144700	**Symptom:** The **Datapath** process in a switch crashed and the switch rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout**. This issue is resolved by dropping the packets that come over the mobility tunnel from Home Agent to Foreign Agent (FA) if they cause a bridge miss. **Scenario:** This issue occurred when packets coming over the mobility tunnel from HA to FA caused a bridge miss. This issue was observed in OAW-4704 switches running AOS-W 6.4.3.6.	Switch-Datapath	OAW-4704 switches	AOS-W 6.4.3.6	AOS-W 6.4.4.10
144703	**Symptom:** The **LLDPD** process in a switch dropped the LLDP packets from a client. The fix ensures that the **LLDPD** process does not drop the LLDP packets. **Scenario:** This issue occurred when spanning tree was enabled on the eth2 (POE enabled) port of a remote AP. This issue was observed in remote access points running AOS-W 6.4.3.9.	Remote Access Point	All platforms	AOS-W 6.4.3.9	AOS-W 6.4.4.10
144843	**Symptom:** Policy Based Routing (PBR) did not work in a switch when the nexthop-list exceeded 24 characters. This issue is resolved by increasing the nexthop-list policy name size to 128 characters. **Scenario:** This issue occurred when the nexthop-list policy name exceeded 24 characters. This issue was observed in switches running AOS-W 6.4.4.6.	Policy Based Routing	All platforms	AOS-W 6.4.4.6	AOS-W 6.4.4.10
145619 148357	**Symptom:** An AP showed close to zero downstream traffic when the UDP frame size was 739 bytes or more. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP204 or OAW-AP205 access points running AOS-W 6.4.4.9.	AP-Platform	OAW-AP204 and OAW-AP205 access points	AOS-W 6.4.4.9	AOS-W 6.4.4.10

Table 4: *Resolved Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
145634	**Symptom:** An AP crashed unexpectedly. The log file listed the reason for the event as **kernel panic**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP215 access points running AOS-W 6.4.4.8.	AP-Platform	OAW-AP215 access points	AOS-W 6.4.4.8	AOS-W 6.4.4.10
145755	**Symptom:** A wired port initiated UDP 4500 went outside a branch office switch although an IP route existed. This issue is resolved by allowing inner tunnel when the destination of the inner tunnel is not the master switch. **Scenario:** This issue occurred because an IPsec tunnel inside a master-local IPsec tunnel was not supported. This issue was observed in branch office switches running AOS-W 6.4.4.9.	Branch Switch	All platforms	AOS-W 6.4.4.9	AOS-W 6.4.4.10
146209	**Symptom:** An AP requested more PoE power than the maximum power consumption. This issue is resolved by reducing the requested PoE power from 25.5 W to 23 W. **Scenario:** This issue was observed in OAW-AP228 access points running AOS-W 6.4.4.8.	AP-Platform	OAW-AP228 access points	AOS-W 6.4.4.8	AOS-W 6.4.4.10
146358	**Symptom:** An LACP/VRRP link toggled frequently on a master switch. This issue is resolved by ensuring that the IPv4/IPv6 VRRP packets are received and processed as expected. **Scenario:** This issue was observed in master switches running AOS-W 6.4.3.7 in a master-local topology.	Switch-Platform	All platforms	AOS-W 6.4.3.7	AOS-W 6.4.4.10
146455	**Symptom:** The BLE device in access points were in the non-operational bank (bank A) as reported by CLI output. The fix ensures that an AP periodically checks the condition to ensure that BLE device is operating out of the correct bank (bank B). The fix ensures that an AP scans nearby beacons. **Scenario:** This issue was observed in OAW-AP205H, OAW-AP210 Series, OAW-AP220 Series, or OAW-AP320 Series access points running AOS-W 6.4.3.x or AOS-W 6.4.4.x.	Bluetooth Low Energy	OAW-AP205H, OAW-AP210 Series, OAW-AP220 Series, or OAW-AP320 Series access points	AOS-W 6.4.4.8	AOS-W 6.4.4.10

Table 4: *Resolved Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
146564	**Symptom:** The LLDP negotiation was not correct in an AP. This issue is resolved by adding a delay while shutting down an Ethernet port of an AP if input power is detected. If the LLDP message suggests that power is good, the AP can use both Ethernet ports when input power is detected. **Scenario:** This issue occurred when the eth1 port of an AP was connected before its eth0 port was connected to a POE+ switch. This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.8.	AP-Platform	OAW-AP325 access points	AOS-W 6.4.4.8	AOS-W 6.4.4.10
146911	**Symptom:** Clients using VIA were unable to connect to a switch after the **ISAKMPD** process crashed in the switch. This issue is resolved by changing the IKE context storing and handling. **Scenario:** This issue was observed in switches running AOS-W 6.3.1.14.	IPsec	All platforms	AOS-W 6.3.1.14	AOS-W 6.4.4.10
147157	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **AP-105 Reboot caused by kernel page fault at virtual address 00000ad4, epc == c08a2c88, ra == c088fc18**. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP105 access points running AOS-W 6.4.3.3.	AP-Wireless	OAW-AP105 access points	AOS-W 6.4.3.3	AOS-W 6.4.4.10
147382	**Symptom:** A remote AP with 313U USB MODEM did not come up on cellular link. The fix ensures that the remote AP comes up using 313U MODEM as uplink. **Scenario:** This issue was observed in OAW-RAP3WN remote access points using 313U USB MODEM for uplink and running AOS-W 6.4.4.9.	Remote Access Point	OAW-RAP3WN remote access points	AOS-W 6.4.4.9	AOS-W 6.4.4.10

This chapter describes the known and outstanding issues identified in AOS-W 6.4.4.10.

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 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version
98884 99817 101260	**Symptom:** An application crashes unexpectedly. **Scenario:** 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.	Switch-Datapath	All platforms	AOS-W 6.2.1.5
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
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
124275	**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

Table 5: *Known Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version
124767 124841	**Symptom:** When a Session Initiation Protocol (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
126385	**Symptom:** Clients do not connect to an SSID although the AP is connected to a switch. **Scenario:** This issue occurs when access points work in active-backup mode with VAP in bridge mode. This issue is observed in access points running AOS-W 6.4.2.12. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.2.12
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
127848	**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
131857	**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. AOS-W 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

Table 5: *Known Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version
132714	**Symptom:** When a user tries to add a static Address Resolution Protocol (ARP) entry, a controller 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. **Workaround:** None.	Switch-Platform	All platforms	AOS-W 6.4.3.4
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
140049	**Symptom:** An AP takes longer 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
140057 142265 145485	**Symptom:** An AP is unable to establish a Generic Route Encapsulation (GRE) tunnel with a switch. **Scenario:** This issue occurs when an AP does not broadcast the SSID but remote BSS-table is able to see the BSSID/SSID. This issue is observed when the **STM** process receives a VLAN delete message and deletes all VAPs with the same VLAN in the station VLAN and the switch closes the VAP without notifying the AP. This issue is observed in switches running AOS-W 6.4.2.14. **Workaround:** None.	Station Management	All platforms	AOS-W 6.4.2.14
140206	**Symptom:** A user cannot delete a NTP server while configuring a clock on the switch. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.4. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.3.4

Table 5: *Known Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version
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
141686	**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.	Logging	All platforms	AOS-W 6.4.4.6
142678	**Symptom:** Adding a Network Time Protocol (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 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version
143181	**Symptom:** A switch contacts an Activate server. **Scenario:** This issue is observed in OAW-4x50 Series switches running AOS-W 6.4.4.5. **Workaround:** None.	Branch Switch	OAW-4x50 Series switches	AOS-W 6.4.4.5
143827	**Symptom:** The **Datapath** process in a switch crashes and the switch reboots unexpectedly. The log file lists the reason for the event as **Datapath timeout**. **Scenario:** This issue occurs when a switch processes invalid tunnel entries. This issue is not limited to any specific switch model or AOS-W version. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.3.6

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

144913	**Symptom:** A switch denies a session to a long URL. **Scenario:** This issue occurs when using Web Content Classification (WEBCC) in a switch running on AOS-W 6.4.4.8. **Workaround:** None.	Deep Packet Inspection	All platforms	AOS-W 6.4.4.8
145314	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT**. **Scenario:** This issue occurs when a client requests association with invalid Number of Spatial Stream (NSS), higher than the supported number of spatial streams. 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
145373	**Symptom:** An AP reports a high and incorrect 5 GHz noise. **Scenario:** This issue is observed in a very high throughput traffic environment. This issue is observed in OAW-AP225 access points running AOS-W 6.4.4.8. **Workaround:** None.	AP-Platform	OAW-AP225 access points	AOS-W 6.4.4.8

Table 5: *Known Issues in 6.4.4.10*

Bug ID	Description	Component	Platform	Reported Version
145486 146896 148292	**Symptom:** The configuration on a master switch is not synchronized with a local switch. **Scenario:** Although centralized licensing is enabled and synchronized and licenses are available, access points display the **IL** flag. This issue is observed in OAW-4750 switches running AOS-W 6.4.3.7. **Workaround:** None.	Master-Local	OAW-4750 switches	AOS-W 6.4.3.7
146653	**Symptom:** An AP crashes and reboots unexpectedly. The log file lists the reason for the event as **Kernel panic at 0x009C07BC**. **Scenario:** This issue is observed in OAW-AP325 access points running AOS-W 6.4.4.8. **Workaround:** None.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.8
148995	**Symptom:** A syslog server shows multiple kernel messages in the **<busybox or modprobe> used greatest stack depth: x byte left** format. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.9. **Workaround:** These messages do not impact the network, ignore these messages.	AP-Platform	All platforms	AOS-W 6.4.4.9

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 on page 32
- GRE Tunnel-Type Requirements on page 33
- Important Points to Remember and Best Practices on page 33
- Memory Requirements on page 34
- Backing up Critical Data on page 35
- Upgrading in a Multiswitch Network on page 36
- Installing the FIPS Version of AOS-W 6.4.4.10 on page 36
- Upgrading to AOS-W 6.4.4.10 on page 37
- Downgrading on page 41
- Before You Call Technical Support on page 43

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-4504 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 36.)

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 35 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 35 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 35 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 35.

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 6.4.4.10

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 6.4.4.10

The following sections provide the procedures for upgrading the switch to AOS-W 6.4.4.10 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 34.

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 6.4.4.10.

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 6.4.4.10 on page 37 to install the interim version of AOS-W, and then repeat steps 1 through 11 of the procedure to download and install AOS-W 6.4.4.10.

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 6.4.4.10 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 35 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. The OAW-RAP5/OAW-RAP5WN reboots to complete the provisioning image upgrade.

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 34.

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 6.4.4.10 on page 37.

Follow steps 2 through 7 of the procedure described in Upgrading to AOS-W 6.4.4.10 on page 37 to install the interim version of AOS-W, and then repeat steps 1 through 7 of the procedure to download and install AOS-W 6.4.4.10.

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 6.4.4.10 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 Seriesswitches.

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 35 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 6.4.4.10 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 6.4.4.10 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 35.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W 6.4.4.10 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 6.4.4.10 flash backup from the file stored on the switch. Do not restore the AOS-W 6.4.4.10 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 6.4.4.10, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W 6.4.4.10, 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 6.4.4.10 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 Level 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 Intrusuin 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
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

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
TPC	Transmit Power Control

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
VBN	Virtual Branch Networking

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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