AOS-W 6.4.4.13

Alcatel·Lucent

Enterprise

Copyright Information

Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit:

enterprise.alcatel-lucent.com/trademarks

All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. (2017)

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

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 6.4.4.13 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:

- describes the features and enhancements introduced in this release.
- lists the regulatory updates introduced in this release.
- describes the issues resolved in this release.
- describes the known and outstanding issues identified in this release.
- 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 6.4.4.13.

AP-Platform

View License Logging Level

Starting from AOS-W 6.4.4.13, a new sub category, **ap-license** is added to the **logging level** command to view AP license logging messages in AOS-W.

Switch-Datapath

Configure Silent Client Aging

Starting from AOS-W 6.4.4.13, a new parameter, **wirelessbridge-aging** is added to the **firewall wireless-bridge-aging** command to configure silent client aging. Enabling this parameter ages out the wireless bridge entry when a client disassociates from the access point. Disabling this parameter ages out the wireless bridge entry based on the bridge age out timer. By default, this parameter is disabled.

IPsec

Provision to Configure MTU for Virtual Adapter

VIA calculates the optimal MTU value for the virtual adapter based on the physical network interface on the client machine. But in some situations, this optimal value may not be desired. This feature allows the administrator to change the MTU value used by VIA. This feature can be configured using the **VIA Client mtu value** parameter in the VIA connection profile. This parameter is introduced in AOS-W 6.4.4.13.

For more information, refer to the *Aruba VIA 2.3.4 Windows® Edition Release Notes*.

BLE

Alcatel-Lucent USB BLE Device Firmware Upgrade

Starting from AOS-W 6.4.4.13, when the Alcatel-Lucent USB BLE device is plugged into the OAW-AP205H, OAW-AP210 Series, or OAW-AP220 Series access points, AOS-W upgrades the firmware of the BLE device automatically.

BLE Firmware

Starting from AOS-W 6.4.4.13, BLE firmware version 1.2-17 is packaged within AOS-W.

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 6.4.4.13:

- DRT-1.0_59241

This chapter describes the issues resolved in AOS-W 6.4.4.13.

Table 4: *Resolved Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
132038 153115	**Symptom:** An AP failed to terminate on a switch and the console displayed **unregister_netdevice: waiting for tun0 to become free** log. The fix ensures that an AP terminates on a switch correctly. **Scenario:** This issue was observed in OAW-AP320 Series access points running AOS-W 6.4.4.8.	AP Datapath	OAW-AP320 Series access points	AOS-W 6.5.0.0	AOS-W 6.4.4.13
141117	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic**. This issue is resolved by ignoring the multicast MAC address during node allocation. **Scenario:** This issue occurred when an AP accepted a multicast MAC address as a correct authentication request during node allocation. This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.4.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.4	AOS-W 6.4.4.13
141594 144029 147933 148379 148384 149916 151187 156639 160100	**Symptom:** An AP rebooted unexpectedly. The log file listed the reason for the event as **Internal watchdog reset**. Improvements in the wireless driver resolves this issue. **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 6.4.4.13

Table 4: *Resolved Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
141708 156496	**Symptom:** Some APs were stuck in **Inactive - Dirty or no config** state while establishing standby tunnel with a master switch. This issue is resolved by changing the way in which the Remote AP information is stored in a switch. **Scenario:** This issue occurred when the Remote AP information was not stored correctly in a switch. This issue was observed in a master-local topology with switches running AOS-W 6.4.4.11.	Switch-Datapath	All platforms	AOS-W 6.4.4.11	AOS-W 6.4.4.13
143016	**Symptom:** The IPv6 link local address was deleted from the IP VLAN of a switch. The fix ensures that the IPv6 link local address is not deleted when a switch is rebooted. **Scenario:** This issue occurred when a switch was rebooted with user configured link local address for IPv6 VLAN. This issue was observed in switches running AOS-W 6.4.4.6.	IPv6	All platforms	AOS-W 6.4.4.6	AOS-W 6.4.4.13
143354	**Symptom:** The USB APB did not report to the **ble_daemon** process. The fix ensures that the USB APB reports to the **ble_daemon** process. **Scenario:** This issue was observed in access points running AOS-W 6.5.0.0.	Bluetooth Low Energy	All platforms	AOS-W 6.5.0.0	AOS-W 6.4.4.13
144774	**Symptom:** An AP stopped responding and rebooted due to an incorrect radio reset. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, and OAW-AP270 Series access points running AOS-W 6.4.4.8 or later versions.	AP-Platform	OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, and OAW-AP270 Series access points	AOS-W 6.4.4.8	AOS-W 6.4.4.13
145234 151998	**Symptom:** The WebUI displayed an incorrect switch IP address for an AP. The fix ensures that the WebUI displays the correct switch IP address for an AP. **Scenario:** This issue occurred when a master switch was part of HA active-standby configuration and an AP associated with the master switch switched from active to standby state. This issue was observed in a master-local topology with switches running AOS-W 6.4.4.3.	WebUI	All platforms	AOS-W 6.4.4.3	AOS-W 6.4.4.13

Table 4: *Resolved Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
146874	**Symptom:** The voice (VO) and video (VI) aware scanning parameters allowed VO/VI traffic that was passed by an AP to the station (STA) on Downlink (DL) only. AP scan requests were rejected by the host driver so that the VO/VI traffic was not interrupted. But, when the VO/VI traffic was passed by the STA to the AP on Uplink (UP) only, AP scan requests were not rejected. This resulted in the AP missing frames from STA and thereby affected the audio and video quality. The fix ensures that while processing data frames from the STA, the Traffic Identifier (TID) and the Access Category (AC) of the packets are checked, so that AP scan requests are rejected on receiving VO/VI frames from the STAs. **Scenario:** This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.2.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.2	AOS-W 6.4.4.13
148004 155405 157742	**Symptom:** An AP had the following issues: ● The 2.4 GHz BSSID disappeared for a fraction of a second. ● High CPU and memory utilization. ● High ping latency on the physical interface of the AP. The fix ensures that the AP operates as expected. **Scenario:** This issue occurred in the following scenarios: ● When the slow_timer_recovery parameter was enabled in the AP System profile. ● When the system time of the AP and that of the controller were not synchronized. This issue was observed in OAW-AP103H, 100 Series, and RAP 100 Series access points running AOS-W 6.4.3.6 or later versions.	AP-Platform	OAW-AP103H, 100 Series, and RAP 100 Series access points	AOS-W 6.4.3.6	AOS-W 6.4.4.13
151105 151106	**Symptom:** Some APs did not communicate with a Meridian server. The fix ensures that the APs work as expected and communicate with a Meridian server. **Scenario:** This issue was observed in OAW-AP215 access points running AOS-W 6.4.4.8.	Bluetooth Low Energy	OAW-AP125 access points	AOS-W 6.4.4.8	AOS-W 6.4.4.13

Table 4: *Resolved Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
151310 158038	**Symptom:** An AP rebooted unexpectedly due to low memory. The fix ensures that the debugging messages are not flooding the memory. **Scenario:** This issue occurred as a flood of debugging messages interrupted the kernel panic, which resulted in resetting the watchdog. This issue was observed in OAW-AP320 Series access points running AOS-W 6.5.0.2 or later versions.	AP-Platform	OAW-AP320 Series access points	AOS-W 6.5.0.2	AOS-W 6.4.4.13
151565	**Symptom:** A RAP incorrectly sent the local DHCP request packets to a switch. The fix ensures that the local DHCP requests of a Remote AP are not encrypted and are sent to the IPsec tunnel. **Scenario:** This issue occurred when a RAP sent encrypted DHCP request packets with the DHCP server as the destination. This issue was observed in Remote access points running AOS-W 6.3.1.22 or later versions.	Remote AP	All AP platforms	AOS-W 6.3.1.22	AOS-W 6.4.4.13
151916 154524 154714 158996 159283	**Symptom:** The **SAPD** process was terminated on some APs. The fix ensures that the **SAPD** process does not terminate due to unhandled signals. **Scenario:** This issue occurred in access points that did not support CPsec and generated unhandled signals. This issue was observed in access points running AOS-W 6.5.2.0 or later versions.	Bluetooth Low Energy	All platforms	AOS-W 6.5.2.0	AOS-W 6.4.4.13
152038 152041 153771 158202	**Symptom:** Clients were unable to connect to APs that were active on backup LMS. This issue is resolved by deleting the standby tunnel when the HA is cleaned up. **Scenario:** This issue occurred when an AP rebootstrapped or HA was disabled and the standby tunnel was not deleted. This resulted in the AP rebootstrapping to the old standby as active. This issue was observed in OAW-AP325 access points running AOS-W 6.5.0.2 or later versions.	AP-Platform	OAW-AP325 access points	AOS-W 6.5.0.2	AOS-W 6.4.4.13
153011	**Symptom:** An access point crashed unexpectedly. Improvements in the wireless driver resolves this issue. **Scenario:** This issue was observed in OAW-AP125 access points running AOS-W 6.4.4.10.	AP-Wireless	OAW-AP125 access points	AOS-W 6.4.4.10	AOS-W 6.4.4.13

Table 4: *Resolved Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
153018 156024 156025 156026 156027 156028 156032 156033 156034 156035 156038 156039 156042 156045 156046 156049 156146 156150 156215	**Symptom:** An AP crashed unexpectedly. Improvements in the AP memory management resolves this issue. **Scenario:** 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 6.4.4.13
154094	**Symptom:** The **station management** process in a switch crashed unexpectedly. The fix ensures that the **station management** process does not crash and works as expected. **Scenario:** This issue was observed in OAW-4650 switches running ArubaOS 6.5.2.0.	AP-Platform	OAW-4650 switches	AOS-W 6.5.2.0	AOS-W 6.4.4.13
154403 159825	**Symptom:** The **SAPD** process in an access point crashed unexpectedly. The fix ensures that the **SAPD** process does not crash and the AP works as expected. **Scenario:** This issue was observed in OAW-AP225 access points running AOS-W 6.4.4.10.	AP-Platform	OAW-AP225 access points	AOS-W 6.4.4.10	AOS-W 6.4.4.13
154464	**Symptom:** Packet drops were observed in an AP. The fix ensures that the AP does not drop packets. **Scenario:** This issue occurred when the port speed configured for the uplink and downlink ports of an AP was different. This issue was observed in OAW-AP205H access points running AOS-W 6.5.2.0 or earlier versions.	AP-Datapath	OAW-AP205H access points	AOS-W 6.5.2.0	AOS-W 6.4.4.13

Table 4: *Resolved Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
154567 156237	**Symptom:** An AP failed to send a DNS query to resolve the master switch. The fix ensures that the AP sends the DNS query to resolve the master switch. **Scenario:** This issue was observed in OAW-AP320 Series access points running AOS-W 6.4.4.9 in an IPv6 environment.	AP-Platform	OAW-AP320 Series access points	AOS-W 6.4.4.9	AOS-W 6.4.4.13
154596 159261	**Symptom:** 802.1X authentication failed on OAW-AP325 access points for 2.4 GHz bridge mode clients. The fix ensures that the clients are able to pass 802.1X authentication. **Scenario:** This issue occurred when LACP was enabled on APs and the AP was setting the destination IP of G band GRE traffic in bridge mode to striping-ip instead of lms-ip. This issue was observed in OAW-AP325 access points running AOS-W 6.5.0.2 and later versions.	AP-Platform	OAW-AP325 access points	AOS-W 6.5.0.2	AOS-W 6.4.4.13
154909	**Symptom:** The **station management** process in an AP displayed the **sapm_amapi.c function sapm_add_ap_counters_row line 6149 error Failed to get gsm info for AP 203H** error message. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in Remote access points running AOS-W 6.5.2.0.	AP-Platform	All platforms	AOS-W 6.5.2.0	AOS-W 6.4.4.13
155526	**Symptom:** An AP crashed and rebooted frequently. The log file listed the reason for the event as **Reboot caused by kernel panic: NSS FW coredump: bringing system down**. The fix ensures that the AP does not crash or reboot. **Scenario:** This issue occurred when an AP forwarded an unaligned packet payload to the Network Security Services (NSS) firmware. This issue was observed in OAW-AP320 Series access points running AOS-W 6.5.1.2.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.5.1.2	AOS-W 6.4.4.13
155730	**Symptom:** Client search based on the **User Name** field in the **Monitoring > NETWORK > All WLAN Clients** page of the WebUI failed to display correct results. The fix ensures that the client search from the WebUI works as expected. **Scenario:** This issue occurred when the user name of a client contained a special character such as **/**. This issue was observed in switches running AOS-W 6.4.4.10 or later versions.	WebUI	All platforms	AOS-W 6.4.4.10	AOS-W 6.4.4.13

Table 4: *Resolved Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
155750	**Symptom:** The user roles were missing in a local switch. This issue is resolved by adding missing checks in handling master-master redundancy and license changes. **Scenario:** This issue occurred in a master-local or master-standby topology where a master switch had PEF license and the standby switch did not have a PEF license. This issue was observed in all switches running AOS-W 6.4.x or later versions, in master-local or master-standby topology.	Base OS Security	All platforms	AOS-W 6.4.3.7	AOS-W 6.4.4.13
156041 156043 156044	**Symptom:** An AP rebooted unexpectedly. The fix ensures that the AP works as expected. **Scenario:** This issue was observed in OAW-AP124 access points running AOS-W 6.4.4.10.	AP-Platform	OAW-AP124 access points	AOS-W 6.4.4.10	AOS-W 6.4.4.13
156061 158728 159140	**Symptom:** A client was unable to get a DHCP IP address and the datapath bridge counters showed high allocation failures. The fix ensures that a client gets DHCP IP address. **Scenario:** This issue was observed when a user upgraded a switch to AOS-W 6.5.0.4. This issue is observed in OAW-4750 switches running AOS-W 6.5.0.2.	Switch-Datapath	OAW-4750 switches	AOS-W 6.5.0.2	AOS-W 6.4.4.13
156139 156615	**Symptom:** Clients failed to connect to an AP until the AP was rebooted. This issue is resolved by marking the disassociated clients as invalid in the peer table. **Scenario:** This issue occurred when the peer ID of a client was not cleared correctly after the peer was no longer associated to the AP. This issue was observed in OAW-AP325 access points running ArubaOS 6.4.4.8.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.8	AOS-W 6.4.4.13
156233 159442 159527 159817	**Symptom:** AppRF did not block certain traffic although DPI was enabled. The fix ensures that DPI classifies the sessions correctly. **Scenario:** This issue occurred when DPI failed to classify the sessions. This issue was observed in switches running AOS-W 6.5.0.3.	Switch-Datapath	All plarforms	AOS-W 6.5.0.3	AOS-W 6.4.4.13

Table 4: *Resolved Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
156404 158531 158532	**Symptom:** An AP crashed unexpectedly. The log file listed the reason for the event as **KERNEL(ar-28-006@172.16.68.46): page:a800000000b10190 flags:0x0000000000000400 mapping:0000000000000000 mapcount:0 count:0**. Improvements in the AP memory management resolves this issue. **Scenario:** This issue was observed in OAW-AP125 access points running AOS-W 6.4.4.11.	AP-Wireless	OAW-AP125 access points	AOS-W 6.4.4.11	AOS-W 6.4.4.13
156485 158064	**Symptom:** A mesh point failed to re-establish a link to a point-to-point portal after the portal was rebooted. Improvements to the decryption method of the broadcast packets resolves this issue. **Scenario:** This issue occurred when the point-to-point portal was rebooted. This issue was observed in access points running AOS-W 6.5.0.0.	Mesh	All platforms	AOS-W 6.5.0.0	AOS-W 6.4.4.13
156586	**Symptom:** When the VLAN of the server changed, the switch could not handle the DLNA update. This issue is resolved by sending wildcard query on the new VLAN. **Scenario:** This issue occurred when the final VLAN was not the default VLAN of the VAP. This resulted in the switch being unable to learn DLNA from Chromecast. This issue was observed in OAW-4x50 Series switches running AOS-W 6.4.4.10.	AirGroup	OAW-4x50 Series switches	AOS-W 6.4.4.10	AOS-W 6.4.4.13
156951	**Symptom:** The **show running-config** command displayed extra spaces for IPv6-related ACLs, though the administrator had configured the ACLs without any extra spaces. The fix ensures that the extra spaces are removed from the running configuration. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.9 or later versions.	Base OS Security	All platforms	AOS-W 6.4.4.9	AOS-W 6.4.4.13
157044	**Symptom:** A switch disclosed the SSH server version on performing a vulnerability scan. The fix ensures that the switch does not disclose the SSH server version. **Scenario:** This issue was not limited to any specific switch model or AOS-W version.	Base OS Security	All platforms	AOS-W 6.4.2.10	AOS-W 6.4.4.13

Table 4: *Resolved Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
157056	**Symptom:** A local switch did not generate a syslog message for a successful 802.1X authentication of a client. The fix ensures that the syslog message is generated for successful 802.1X client authentications. **Scenario:** This issue was observed in a master-local topology running AOS-W 6.4.4.10 or later versions.	Base OS Security	All platforms	AOS-W 6.4.4.10	AOS-W 6.4.4.13
157379	**Symptom:** The Tx power, major number, and minor number were deleted in an BLE enabled AP. The fix ensures that the Tx power, major number, and minor number are not deleted in an BLE-enabled AP. **Scenario:** This issue was observed when the AOS-W bundled with BLE firmware was upgraded or downgraded in access points running AOS-W 6.5.2.0.	Bluetooth Low Energy	All platforms	AOS-W 6.5.2.0	AOS-W 6.4.4.13
158031	**Symptom:** The **mobileip** process in a switch crashed unexpectedly. This issue is resolved by moving clients to no mobility state if HA allocate fails for a client with static IP. **Scenario:** This issue occurred when clients used static IP addresses and L3 mobility **router mobile** was enabled with a single anchor switch that was not reachable. This issue was observed in OAW-6000 switches running AOS-W 6.4.3.11.	Mobility	OAW-6000 switches	AOS-W 6.4.3.11	AOS-W 6.4.4.13
158229	**Symptom:** A switch showed an error on boot after an upgrade. The log file listed the reason for this event as **WARNING: Configuration upgrade failed**. The fix ensure that the switch upgrade is successful. **Scenario:** This issue was observed when a switch was upgraded from AOS-W 6.3.x to AOS-W 6.4.4.12. This issue was observed in switches running AOS-W 6.4.4.12.	Base OS Security	All platforms	AOS-W 6.4.4.12	AOS-W 6.4.4.13
158250	**Symptom:** The OUI 44:48:C1 was not supported. The fix ensures that all APs support the OUI 44:48:C1. **Scenario:** This issue was observed in access points running AOS-W 6.5.2.0.	AP-Platform	All platforms	AOS-W 6.5.2.0	AOS-W 6.4.4.13

Table 4: *Resolved Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
158410	**Symptom:** Clients connected to a Remote AP in bridge-persistent mode did not pass traffic when the Remote AP lost connectivity with a switch. The fix ensures that the client can pass traffic. **Scenario:** This issue was observed in Remote access points running AOS-W 6.4.2.2.	Remote AP	All platforms	AOS-W 6.4.2.2	AOS-W 6.4.4.13
158546	**Symptom:** An AP rebooted randomly. The log file listed the reason for the event as **Wrong cookie in request**. The fix ensures that the AP ignores the message sent by the non-active switch. **Scenario:** This issue occurred during a HA failover in the following sequence: 1. The **write memory** command was executed in a master switch. 2. The master switch synchronized the changed configuration to the local and standby switches. 3. An AP failed over from a local switch to a standby switch. 4. The AP received a message from the non-active local switch. This issue was observed in a master-local topology with switches running AOS-W 6.4.2.15.	AP-Platform	All platforms	AOS-W 6.4.2.15	AOS-W 6.4.4.13
158551	**Symptom:** The **authentication** process in a switch crashed unexpectedly. Improvements in the switch memory management resolves this issue. **Scenario:** This issue occurred because of memory leaks in the **authentication** process. This issue was observed in switches running AOS-W 6.5.0.3 with radsec enabled.	Base OS Security	All platforms	AOS-W 6.5.0.3	AOS-W 6.4.4.13

Table 4: *Resolved Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
158718 160401	**Symptom:** An AP displayed wrong inventory many times. The fix ensures that the AP displays the correct inventory. **Scenario:** This issue was observed in access points running AOS-W 6.5.2.0.	Bluetooth Low Energy	All platforms	AOS-W 6.5.2.0	AOS-W 6.4.4.13
158829	**Symptom:** OAW-AP320 Series access points crashed and rebooted unexpectedly. The log file listed the reason for the event as **kernel panic: NSS FW coredump: bringing system down**. The fix ensures that the AP does not reboot unexpectedly. **Scenario:** This issue was observed in OAW-AP320 Series access points running AOS-W 6.5.1.3 or later versions.	AP-Wireless	OAW-AP320 Series access points	AOS-W 6.5.1.3	AOS-W 6.4.4.13

This chapter describes the known and outstanding issues identified in AOS-W 6.4.4.13.

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 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version
115260 128209	**Symptom:** When an administrator tries to hard reboot a switch, it fails to reboot with the **Not enough space on flash** error message. **Scenario:** This issue occurs occasionally due to a database file corruption. This issue is observed in switches running AOS-W 6.4.2.3 or later versions. **Workaround:** Contact Technical Support to remove the corrupted database file.	Switch-Platforms	All platforms	AOS-W 6.4.2.3
123458	**Symptom:** A VoIP client receives an IP address from a wrong VLAN. **Scenario:** This issue occurs when an AP fails to send LLDP-MED packets after receiving an LLDP packet from a VoIP phone. This issue is observed when a client that supports LLDPMED is connected to the downlink Ethernet port of an AP. This issue is observed in APs running AOS-W 6.4.3.3. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.3.3
124275 151661	**Symptom:** All clients continue to obtain IP addresses from the same VLAN even though a RADIUS server VSA specifies a VLAN pool with multiple VLANs. **Scenario:** This issue is observed when a RADIUS server VSA overrides the virtual AP VLANs with a different VLAN pool that is configured with the even assignment type. This issue is observed in switches running AOS-W 6.4.2.6 or later versions. **Workaround:** Change the VLAN assignment type from **even** to **hash** using the following CLI command: `(host) (config) #vlan-name <name> assignment hash`	Station-Management	All platforms	AOS-W 6.4.2.6
124767 124841	**Symptom:** Media traffic is not prioritized and call details are not visible for SIP calls on the UCC dashboard. **Scenario:** This issue is observed when large segmented SIP signaling messages are broken in to multiple segments and delivered out of order. This issue is not limited to any specific switch model or AOS-W release version. **Workaround:** None.	Unified Communication and Collaboration	All platforms	AOS-W 6.4.2.4
127094 138590 144730	**Symptom:** The **Dashboard > Access Points > Radios** page of the WebUI displays some of the AP names as **unknown**. **Scenario:** This issue occurs during a HA failover when an AP switches from the master switch to a standby switch. This issue is not limited to any specific AP model or AOS-W version. **Workaround:** None.	AP-Platform	All AP platforms	AOS-W 6.4.2.12

Table 5: *Known Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version
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 **** characters at the end of the destination folder name. For example, ArubaOS misinterprets the **** characters in the **copy flash: crash.tar ftp: 10.1.1.1.test-user \ArubaOS\\ crash.tar** command. This issue is observed in switches running AOS-W 6.4.4.0. **Workaround:** None.	Switch-Platforms	All platforms	AOS-W 6.4.4.0
131857	**Symptom:** When the ToS value is set to 0 in the user role, the value does not take effect. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.3. **Workaround:** None.	Switch-Datapath	All platforms	AOS-W 6.4.3.3
132770	**Symptom:** In a centralised licensing system, the following license expiry message is displayed without sufficient information: **Jan 7 08:30:00 :300158: <WARN> |licensemgr| Licenses contributed by the client will expire in 29 days**. **Scenario:** This issue occurs in a centralised licensing system when a client switch that contributes license goes down. This issue was not limited to any specific switch model or AOS-W version. **Workaround:** None.	AP-Platform	All AP platforms	AOS-W 6.4.2.12
137196	**Symptom:** A switch fails to respond and reboots unexpectedly. The log file lists the reason for the event as **Reboot Cause: Datapath timeout**. **Scenario:** This issue occurs when VIA is used with 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:** The **Configuration > BRANCH > Smart Config > Networking** page in the WebUI does not provide an option to set the IP address of the user VLAN to **dhcp-client**. **Scenario:** This issue is observed in switches running AOS-W 6.4.4.6. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.4.6

Table 5: *Known Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version
140049	**Symptom:** An AP takes longer 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:** The **Configuration > BRANCH > Smart config > Routing > DHCP options** page of the WebUI does not provide an option to configure multiple DHCP options for a DHCP pool. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.6. **Workaround:** None.	WebUI	All platforms	AOS-W 6.4.3.6
141686	**Symptom:** A branch switch does not communicate with a master switch. **Scenario:** This issue occurs under the following scenarios: ● The **NAT Outside** option is enabled in the **Configuration > BRANCH > Smart Config > Networking** page of the WebUI. ● The IP address of the master switch is different from the public IP address. This issue is observed in branch switches running AOS-W 6.4.4.0. **Workaround:** None.	Branch Switch	All platforms	AOS-W 6.4.4.0
141822 143282	**Symptom:** The process handling authentication requests crashes due to a segmentation fault while sending RADIUS-accounting packets. **Scenario:** This issue occurs when you make the following changes to a AAA profile which is used by a client associated to the WLAN: ● Modify the RADIUS accounting server-group assigned in the AAA profile to a different server-group. ● Enable **multiple-server-accounting** which is originally disabled in the AAA profile. This issue is not limited to any specific switch model or AOS-W 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:** The timestamp in the syslog message for IPv4 address includes the year at the end, which is not according to the format defined in RFC-3164. This issue is not limited to any specific switch model or AOS-W version. **Workaround:** None.	Logging	All platforms	AOS-W 6.4.4.6

Table 5: *Known Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version
142678	**Symptom:** Adding an NTP server to a switch causes all the Remote APs to reconnect without notification. Many Instant AP VPNs cannot recover as well. **Scenario:** This issue occurs when the NTP server tries to correct the time difference in the switch. This issue is not limited to any specific switch model or AOS-W version. **Workaround:** Reboot the switch after configuring the NTP server.	IPsec	All platforms	AOS-W 6.4.2.13
142975	**Symptom:** An AP suddenly stops forwarding traffic until it is rebooted. **Scenario:** This issue occurs when a tunnel mode Virtual AP and a bridge mode Virtual AP or a wired AP are both configured on a single AP. This issue is not limited to any specific AP model or AOS-W version. **Workaround:** None.	AP Datapath	All platforms	AOS-W 6.4.4.6
143566	**Symptom:** A controller displays the **Module authentication is busy. Please try later** error when the **show reference user-role <role-name>** command is executed. **Scenario:** This issue occurs when more than 212 entries exist for a given role in user derivation-rules or server-group derivation rules. This issue is observed in a master-local topology with switches running AOS-W 6.4.2.16. **Workaround:** None.	Configuration	All platforms	AOS-W 6.4.2.16
145803	**Symptom:** A switch does not generate **wlsxNConnectionBackfromLocal** trap although the trap is enabled. **Scenario:** This issue occurs when a local switch is reloaded and the master switch does not generate the **wlsxNConnectionBackfromLocal** trap. This issue is observed in switches running AOS-W 6.4.4.6. **Workaround:** None.	SNMP	All platforms	AOS-W 6.4.4.6
148416 149211	**Symptom:** A crash is observed in the **Station Management (STM)** process due to memory corruption. **Scenario:** This issue occurs when there is an increase in the number of user roles and as a result the role bandwidth message does not fit into one PAPI message. This issue is observed in OAW-4550 switches running AOS-W 6.4.3.4. **Workaround:** None.	AP-Platform	OAW-4550 switches	AOS-W 6.4.3.4
147300	**Symptom:** A switch fails to respond and reboots. **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

Table 5: *Known Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version
148557	**Symptom:** Clients observed a sudden increase in the number of DHCPv6/Multicast messages from the access points. **Scenario:** This issue is observed in OAW-4650 switches running AOS-W 6.4.4.9. **Workaround:** None.	AP-Platform	OAW-4650 switches	AOS-W 6.4.4.9
148977 155343	**Symptom:** A branch office switch randomly loses configuration updates from the master switch. **Scenario:** This issue occurs after a new license is sent from the master switch to the branch office switch. Thereafter, license-dependent configuration updates are not sent to the branch office switch. This issue is observed in branch office switchesrunning AOS-W 6.4.4.8 or later versions. **Workaround:** None.	Licensing	All platforms	AOS-W 6.4.4.8

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 due to a RADAR detection. This issue is observed in APs running AOS-W 6.4.4.6.
	Workaround: Disable channel switch announcement on the AP using the following 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

149594	**Symptom:** The **AMON_USER_INFO_MESSAGE** does not contain the user-agent info, whereas the SNMP user info has the user-agent information. **Scenario:** This issue is observed in a master-local topology when choosing AMON over SNMP in AirWave. This issue is observed in switches running AOS-W 6.4.3.9. **Workaround:** Choose SNMP in AirWave.	Base OS Security	All platforms	AOS-W 6.4.3.9
150232 155810	**Symptom:** A switch crashes and reboots. **Scenario:** This issue occurs when running the Veriwave throughput test on the switch. This issue is observed in OWA-4005 and OAW-4030 switches running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	Switch-Datapath	OWA-4005 and OAW-4030 switches	AOS-W 6.4.4.9

Table 5: *Known Issues in 6.4.4.13*

Bug ID	Description	Component	Platform	Reported Version
152665	**Symptom:** A switch crashes unexpectedly on the FPCLI module. **Scenario:** This issue is observed in a master-standby topology with OAW-4550 switches running AOS-W 6.4.4.9 or later versions. **Workaround:** None.	Switch-Platform	OAW-4550 switches	AOS-W 6.4.4.9
153217	**Symptom:** Multiple processes in a switch are killed unexpectedly. **Scenario:** This issue occurs when a AAA server responds with more than one RADIUS-state attributes in the RADIUS packets. This issue is observed in switches running AOS-W 6.3.x, AOS-W 6.4.x, or AOS-W 6.5.x. **Workaround:** None.	Base OS Security	All platforms	AOS-W 6.4.3.6
153463	**Symptom:** The AP channel utilization graph shows multiple breaks and is incomplete. **Scenario:** This issue is observed in switches running AOS-W 6.4.3.10. **Workaround:** None.	AP-Wireless	All platforms	AOS-W 6.4.3.10
153824	**Symptom:** Data is not transmitted when static IPsec routing with ip-to-ip IPsec tunnel is enabled. **Scenario:** This issue occurs when the route cache entry is installed with the wrong flag. This issue is observed in switches running AOS-W 6.4.4.10. **Workaround:** None.	IPsec	All platforms	AOS-W 6.4.4.10
155090 156580	**Symptom:** The mDNS process in a switch crashes because of specific packets coming from the Cisco switch. **Scenario:** This issue occurs when AirGroup is enabled in a switch and a switch. However, specific switches (Cisco) replace the MAC address of the original packets with their own MAC address and send them to the switch. This issue is observed in switches running AOS-W 6.4.4.11. **Workaround:** None.	AirGroup	All platforms	AOS-W 6.4.4.11
158316 160400	**Symptom:** The BLE firmware upgrade in an AP fails. **Scenario:** This issue is observed in OAW-AP210 Series, OAW-AP220 Series, and OAW-AP320 Series APs running AOS-W 6.5.2.0. **Workaround:** Disable auto upgrade in the AP and use an application in a mobile device to perform an over-the-air upgrade of the BLE firmware in the AP.	Bluetooth Low Energy	OAW-AP210 Series, OAW-AP220 Series, or OAW-AP320 Series access points	AOS-W 6.5.2.0

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

![CAUTION] 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) 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 34.)

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.

⚠ **CAUTION**

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 33 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 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 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 33.

> *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 6.4.4.13

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 6.4.4.13

The following sections provide the procedures for upgrading the switch to AOS-W 6.4.4.13 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 32.
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 6.4.4.13.

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 to install the interim version of AOS-W, and then repeat steps 1 through 11 of the procedure to download and install AOS-W 6.4.4.13.

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 6.4.4.13 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 33 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 32.

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 6.4.4.13 on page 35.

Follow steps 2 through 7 of the procedure described in Upgrading to AOS-W 6.4.4.13 on page 35 to install the interim version of AOS-W, and then repeat steps 1 through 7 of the procedure to download and install AOS-W 6.4.4.13.

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 6.4.4.13 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>
```

NOTE: 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 33 for information on creating a backup.

Downgrading

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

> ⚠️ **CAUTION**
> 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 6.4.4.13 are lost after the downgrade (this warning does not apply to upgrades from AOS-W 3.4.x to AOS-W 6.1).

> ⚠️ **CAUTION**
> 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 6.4.4.13 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.

> ⚠️ **CAUTION**
> 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 33.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W 6.4.4.13 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 6.4.4.13 flash backup from the file stored on the switch. Do not restore the AOS-W 6.4.4.13 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 6.4.4.13, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W 6.4.4.13, 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 6.4.4.13 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.

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	Log Event Extended Format
LI	Lawful Interception
LLDP	Link Layer Discovery Protocol
LLDP-MED	LLDP–Media Endpoint Discovery
LMS	Local Management Switch
LNS	L2TP Network Server
LTE	Long Term Evolution
MAB	MAC Authentication Bypass
MAC	Media Access Control
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