AOS-W 6.4.4.12

Release Notes

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

AOS-W 6.4.4.12 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 13 lists the regulatory updates introduced in this release.
- Resolved Issues on page 14 describes the issues resolved in this release.
- Known Issues on page 27 describes the known and outstanding issues identified in this release.
- Upgrade Procedure on page 34 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 6.4.4.12.

DCHP

Character Limitation for DHCP Option

Starting from AOS-W 6.4.4.12, the number of characters for the text field under the DHCP pool option is increased from 128 to 256.

IPsec

Forced Tunnel Mode

Starting from AOS-W 6.4.4.12, the site-to-site IPsec SA can be switched to forced-tunnel mode, even if the protected network/mask and the peer-IP are the same. Enable or disable the forced-tunnel mode or the transport mode on both peers, otherwise a tunnel will not be established. The site-to-site IPsec SA can be switched between forced-tunnel and transport modes by using the **Force Tunnel Mode** parameter.

If the **Force Tunnel Mode** parameter is enabled, an IPsec tunnel is established in forced-tunnel mode instead of transport mode. By default, the **Force Tunnel Mode** parameter is disabled. The **Force Tunnel Mode** parameter can be configured from the WebUI or the CLI.

In the WebUI

To enable forced-tunnel mode using the WebUI:

1. Navigate to **Configuration > Advanced Services > VPN Services > Site-to-Site > IPSec Maps**.
2. Click **Edit** against one of the IPsec maps.
3. Select the **Force Tunnel Mode** check box.
4. Click **Done**.

In the CLI

To enable forced-tunnel mode using the CLI:

```
(host) #configure terminal
(host) (config) #crypto-local ipsec-map default 10
```

```
(host) (config-ipsec-map) #force-tunnel mode enable
(host) (config-ipsec-map) #write memory
```

New Command

The following new command is introduced in ArubaOS 6.4.4.12.

show iap subnet

```
show iap subnet <subnet-name>
```

Description

This command helps troubleshoot IAP-VPN distributed L3 Branch ID (BID) allocation-related issues. This command provides an increased granularity in searching the BID provided by the controller.

Syntax

Parameter	Description
`<subnet-name>`	Specific subnet name of the BID.

Example

The following example displays the BID subnet details. To know the subnet name, execute the **show iap table long** command.

```
(host) #show iap subnet 192.0.2.1-192.0.2.254,5

M       ax BID : 32
BID Bitmap :
1 : 03000000
2 : 00000000
Dead Branch List :
1 : 4d852f8d01a4dab1425dc14cc2e287cdc6d216b698bab1bea3 BID:6
2 : 7ba7671101a5c06850061b7330599d5a2a7d5d69b7fb865c59 BID:7
Allocated BID Branch List :
1 : 4d852f8d01a4dab1425dc14cc2e287cdc6d216b698bab1bea3 BID:6
2 : 7ba7671101a5c06850061b7330599d5a2a7d5d69b7fb865c59 BID:7
```

The output of this command includes the following fields.

Field	Description
`BID Bitmap`	Internal data structure to allocate BID to branches.
`Dead Branch List`	List of branches that are inactive at a time.
`Allocated BID Branch List`	List of branches that have valid BIDs.

WebUI

NAS IP Address

Starting from AOS-W 6.4.4.12, the NAS IP address of a branch office switch can be configured with a VLAN. If a NAS IP VLAN is not configured for a branch office switch, the IP address that is defined in the RADIUS server configuration is used as the NAS IP address.

In the WebUI

To configure a NAS IP address using the WebUI:

1. Navigate to **Configuration > BRANCH > Smart Config** page.
2. Select **Routing**.
3. Select a VLAN ID from the **Override NAS** drop-down list.
4. Click **Apply**.

Chapter 3
Regulatory Updates

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 6.4.4.12:

- DRT-1.0_58226

This chapter describes the issues resolved in AOS-W 6.4.4.12. The NTP security release ntp-4.2.8p9 is integrated in AOS-W 6.4.4.12. In addition, the following issues are resolved in this release.

Table 4: *Resolved Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
104874 139962 149550 150743 151483 155084	**Symptom:** Stale entries were present in both the switch and the AP association tables but not in the AP driver's client table or vice versa. This issue is resolved by removing the stale entries in the switch, AP association table, and the AP driver. **Scenario:** This issue occured when the APs were up for several weeks. This issue was not limited to any specific switch or AP model and AOS-W version.	Station Management	All platforms	AOS-W 6.4.3.0	AOS-W 6.4.4.12
125997 155420	**Symptom:** A switch displayed multiple debugging messages like **rdnssd[891]: 0: 2001:558:feed::2 expires at 8214312**. The fix ensures that the number of debugging messages displayed are controlled. **Scenario:** This issue occurred when the **IPv6 neighbor discovery** feature was enabled. This issue was observed in switches running AOS-W 6.4.4.10.	AP-Platform	All platforms	AOS-W 6.4.4.10	AOS-W 6.4.4.12
126244 133950 136632 136957 141924	**Symptom:** The status of an AP did not match between a master and a local switch. The fix ensures that the status of an AP is consistent between a master and a local switch. **Scenario:** This issue occurred when an AP moved from one local switch to another but its status was not updated in the master switch. This issue was observed in APs running AOS-W 6.4.4.8.	AP-Platform	All platforms	AOS-W 6.4.4.8	AOS-W 6.4.4.12

Table 4: *Resolved Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
126727 139011	**Symptom:** The maximum EIRP value mismatched between a mesh point and a mesh portal. This issue is resolved by setting the initial power of the mesh point to 127 dBm. **Scenario:** This issue was observed in OAW-AP270 Series access points that were configured as mesh point and mesh portal in a mesh network.	Mesh	OAW-AP270 Series access points	AOS-W 6.4.3.2	AOS-W 6.4.4.12
127362 149187 149188	**Symptom:** Memory leaks were observed in the **mDNS** process of a switch. The fix ensures that the **mDNS** process does not lose memory. **Scenario:** This issue occurred when an AirGroup service was added or deleted. This issue was observed in switches running AOS-W 6.4.4.8.	AirGroup	All platforms	AOS-W 6.4.4.8	AOS-W 6.4.4.12
127848 151629	**Symptom:** A Remote AP failed to re-establish a PPPoE connection to the backup LMS when the primary LMS was not available. The fix ensures that the Remote AP establishes a PPPoE connection to the backup LMS. **Scenario:** This issue was observed in OAW-AP205 and OAW-AP274 access points running AOS-W 6.4.4.0.	Remote Access Point	OAW-AP205 and OAW-AP274 access points	AOS-W 6.4.4.0	AOS-W 6.4.4.12
134147 150805	**Symptom:** Clients failed to discover Apple TV in an AirGroup-enabled network. The fix ensures that clients discover Apple TV. **Scenario:** This issue occurred when full configuration synchronization was enabled in an switch. During a full configuration synchronization, AirGroup deleted all AirGroup services and restored it back, but did not delete the cache entries and reset the AirGroup server count to zero. This issue was observed in a master-local deployment with switches running AOS-W 6.4.4.8.	AirGroup	All platforms	AOS-W 6.4.4.8	AOS-W 6.4.4.12

Table 4: *Resolved Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
140113 140886 144529 151560	**Symptom:** The user-table of a switch displayed an incorrect user-role for a wireless client connected to an Instant AP in an IAP-VPN deployment. This issue is resolved by allowing the client to retain its existing role as it moves from one SSID to the other. **Scenario:** This issue occurred because the switch failed to inherit the role from the previous user entry and derived an incorrect or new role for the client when it switched from one SSID to another across VLANs.	RAP-NG	All platforms	AOS-W 6.4.4.6	AOS-W 6.4.4.12
141200 142436	**Symptom:** A remote AP failed to establish a VPN connection with a switch. The fix ensures that the invalid branch ID values are not saved in a switch. **Scenario:** This issue was observed in OAW-RAP3WN remote access points running AOS-W 6.4.4.6.	Remote AP	OAW-RAP3WNremote access points	AOS-W 6.4.4.6	AOS-W 6.4.4.12
144082	**Symptom:** The **wlanApRadioAssocReqCount, wlanApRadioReAssocReqCount**, and **wlanAPRadioAssocSuccPercent** OIDs displayed **0** during an SNMP poll. The fix ensures that the OIDs display the correct values. **Scenario:** This issue occurred when SNMP was enabled in a switch running AOS-W 6.4.4.5.	SNMP	All platforms	AOS-W 6.4.4.5	AOS-W 6.4.4.12
144156 145374 145759 150408 156415	**Symptom:** A switch processed wrong instructions. The fix ensures that the switch processes the correct instructions. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.5.	Switch-Platform	All platforms	AOS-W 6.4.4.5	AOS-W 6.4.4.12
144229	**Symptom:** An administrator could not configure the CPPM credentials from the **Configuration > Security > Authentication > Servers > RADIUS Server** page of the WebUI. The fix ensures that the CPPM credentials can be configured successfully from the WebUI. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.x.	WebUI	All platforms	AOS-W 6.4.3.9	AOS-W 6.4.4.12

Table 4: *Resolved Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
144302 153465	**Symptom:** An AP stopped responding and rebooted. The log file listed the reason for the event as Reboot caused by kernel panic: Out of memory. Improvements in the wireless driver of the AP resolved the issue. **Scenario:** This issue occurred when clients roamed in an L2 network, resulting in a gradual decrease in the memory of the AP. This issue was observed in OAW-AP320 Series access points running AOS-W 6.4.4.10.	AP-Platform	OAW-AP320 Series access points	AOS-W 6.4.3.9	AOS-W 6.4.4.12
144768 145436	**Symptom:** Some APs rebooted randomly with a reboot cause as **Critical process /aruba/bin/stm [pid 4040] DIED** when Hotspot 2.0 was enabled in a virtual AP. Improvements in handling ANQP queries resolved this issue. **Scenario:** This issue occurred when an AP received and processed an invalid value in the ANQP query from a Hotspot 2.0 enabled client. This issue was observed in APs running AOS-W 6.2.2 or later versions.	Hotspot	All platforms	AOS-W 6.4.2.17	AOS-W 6.4.4.12
145385	**Symptom:** An AP rebooted frequently. The log file listed the reason for the event as **SAPD: Reboot requested by controller**. The fix ensures that the switch does not trigger an incorrect AP reboot. **Scenario:** This issue was observed in switches running AOS-W 6.3.1.14.	Local Database	All platforms	AOS-W 6.3.1.14	AOS-W 6.4.4.12
145934 149784 150173 155544 156308	**Symptom:** Multiple processes in a switch crashed unexpectedly. The log file listed the reason for the event as **KERNEL: Out of Memory signal 9: Killed process 30929 (httpd). Out of memory**. Improvements in the switch memory management resolves this issue. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.x and AOS-W 6.4.3.x.	Switch-Platform	All platforms	AOS-W 6.4.4.8	AOS-W 6.4.4.12

Table 4: *Resolved Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
147462	**Symptom:** The **Clients** page in AirWave did not display the IP addresses of some clients that were in bridge-forwarding mode. The fix ensures that the IP addresses of all clients are displayed in the **Clients** page in AirWave. **Scenario:** This issue was observed in switches running AOS-W 6.4.3.5.	Base OS Security	All platforms	AOS-W 6.4.3.5	AOS-W 6.4.4.12
148160 152187	**Symptom:** An AP stopped responding and rebooted. The log file listed the reason for the event as **Critical process /aruba/bin/stm [pid 3249] DIED, process marked as RESTART**. Improvements in the memory efficiency of the **STM** process resolved the issue. **Scenario:** This issue occurred because the AP did not detect some clients accurately. This issue was observed in OAW-AP320 Series access points running AOS-W 6.5.1.0.	Station Management	OAW-AP320 Series access points	AOS-W 6.5.1.0	AOS-W 6.4.4.12
148249 148251 148252 148263	**Symptom:** A switch was inaccessible after it was rebooted by unplugging the power multiple times. The fix ensures that the switch is accessible even after a hard reboot. **Scenario:** This issue occurred when a switch was hard rebooted multiple times immediately after saving the configuration. This issue was observed in OWA-4005 switches running AOS-W 6.4.3.9-FIPS or later versions.	Switch-Platform	OWA-4005 switches	AOS-W 6.4.3.9-FIPS	AOS-W 6.4.4.12
148635 151850 154284	**Symptom:** Database synchronization failed for FIPS build. The fix ensures that database synchronization succeeds. **Scenario:** This issue was observed in a master-standby deployment with switches running AOS-W 6.4.3.10-FIPS or later versions.	Database	All platforms	AOS-W 6.4.3.10-FIPS	AOS-W 6.4.4.12
148703 150890 150918	**Symptom:** The **WMS** process in a switch crashed unexpectedly. The fix ensures that the **WMS** process does not crash and works as expected. **Scenario:** This issue occurred when a switch reset during a power outage. This issue was observed in switches running AOS-W 6.4.4.5.	Air Management-IDS	All platforms	AOS-W 6.4.4.5	AOS-W 6.4.4.12

Table 4: *Resolved Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
148909 156395	**Symptom:** A local switch stopped responding resulting in user traffic disruption. This issue is resolved by fixing the datapath session leaks that were observed in the local switch. **Scenario:** This issue occurred when a large amount of traffic was generated and Web Content Classification (WebCC) and Deep Packet Inspection (DPI) features were enabled in a switch. This resulted in datapath session leaks. This issue was observed in a master-local deployment with OAW-4x50 Series switches running AOS-W 6.4.4.9 or later versions.	Switch-Datapath	OAW-4x50 Series switches	AOS-W 6.4.4.9	AOS-W 6.4.4.12
149131	**Symptom:** A switch sent Alcatel Mapping Adjacency Protocol (AMAP) packets only on one member interface instead of all member interfaces of the port-channel. This issue is resolved by sending the AMAP packets on all member interfaces of the port-channel. **Scenario:** This issue occurred when AMAP was enabled on the port-channel interface. This issue was not limited to any specific switch model or AOS-W version.	SNMP	All platforms	AOS-W 6.4.3.10	AOS-W 6.4.4.12
149718 150678 150679 150683 151336 152025 152572 153743 154141 154574 155315	**Symptom:** A switch processed wrong instructions. The fix ensures that the switch processes the correct instructions. **Scenario:** This issue was observed in OAW-4x50 Seriesswitches running AOS-W 6.4.4.11.	Switch-Platform	OAW-4x50 Seriesswitches	AOS-W 6.4.4.11	AOS-W 6.4.4.12
149766	**Symptom:** Clients failed to connect to an SSID after deleting an unused VLAN ID from the VLAN pool. The fix ensures that a change in the VLAN pool correctly updates the VLAN of the virtual AP profile. **Scenario:** This issue occurred when the **preserve-vlan** parameter was enabled in the virtual AP profile. This issue was observed in switches running AOS-W 6.4.4.6 or later versions.	AP-Platform	All platforms	AOS-W 6.4.4.6	AOS-W 6.4.4.12

Table 4: *Resolved Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
150759 154237 154576 154659 154660 155679	**Symptom:** An AP stopped responding and rebooted. The log file listed the reason for the event as **kernel panic: Fatal exception**. Improvements in the wireless driver of the AP resolved the issue.. **Scenario:** This issue was observed in OAW-AP320 Series access points running AOS-W 6.4.4.9.	Wi-Fi Driver	OAW-AP320 Series access points	AOS-W 6.4.4.9	AOS-W 6.4.4.12
150829 152809 153998	**Symptom:** A client failed to obtain an IP address from the DHCP server. As a result, the client entry was not displayed in the user table of the switch. The fix ensures that the clients get an IP address from the DHCP server. **Scenario:** This issue occurred when the **Enforce DHCP** option was enabled in the AAA profile of an AP operating in split-tunnel forwarding mode. This issue was observed in switches running AOS-W 6.5.0.2.	AP-Datapath	All platforms	AOS-W 6.5.0.2	AOS-W 6.4.4.12
150861	**Symptom:** A switch displayed the **Error, cert manager service is busy or not available for user** message. Improvements in handling the expired certificate resolves this issue. **Scenario:** This issue occurred in one of the following scenarios: • A user attempted to map a new certificate to an existing management user whose certificate had expired. • A user attempted to delete an existing management user whose certificate had expired. This issue was observed in switches running AOS-W 6.4.x or AOS-W 6.5.x.	Certificate Manager	All platforms	AOS-W 6.4.4.8	AOS-W 6.4.4.12
151431	**Symptom:** The proxy-state attribute was missing from the CoA request or Disconnect-ACK packet sent from a switch to a RADIUS proxy server. The fix ensures that the proxy-state attribute is included in the CoA request and Disconnect-ACK packet. **Scenario:** This issue was observed in switches running AOS-W 6.4.2.6.	RADIUS	All platforms	AOS-W 6.4.2.6	AOS-W 6.4.4.12

Table 4: *Resolved Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
151605 152410	**Symptom:** A client failed to pass traffic. The fix ensures that the client can pass traffic. **Scenario:** This issue occurred when a client sent an IP packet before the DHCP packet. This issue was observed in switches running AOS-W 6.4.4.6.	Base OS Security	All platforms	AOS-W 6.4.4.6	AOS-W 6.4.4.12
151855	**Symptom:** Some APs stopped responding and rebooted unexpectedly. The log file listed the reason for the event as **Unable to get IP address using DHCP after 10 tries, total DHCP retry:10** or **DHCP timed out**. Improvements in the AP memory management resolves this issue. **Scenario:** This issue was observed in OAW-AP90 Series, 100 Series, OAW-AP110 Series, OAW-AP120 Series, OAW-RAP108, OAW-RAP109, or OAW-RAP3WN access points running AOS-W 6.4.4.9.	AP-Platform	OAW-AP90 Series, 100 Series, OAW-AP110 Series, OAW-AP120 Series, OAW-RAP108, OAW-RAP109, or OAW-RAP3WN access points	AOS-W 6.4.4.9	AOS-W 6.4.4.12
151973 153597 153725 153731 154438	**Symptom:** The WebUI of a local switch was inaccessible. In addition, the local switch stopped responding and rebooted. The log file listed the reason for the event as **Nanny rebooted machine - fpapps process died**. The fix ensures that the local switch does not reboot and the WebUI of the local switch is accessible. **Scenario:** This issue occurred when Hotspot 2.0 was enabled and 802.1X termination was disabled on a switch. This issue was observed in a master-local deployment with switches running AOS-W 6.4.3.7.	Switch-Platform	All platforms	AOS-W 6.4.3.7	AOS-W 6.4.4.12
152062	**Symptom:** Intermittent kernel crash was observed in an AP. This issue is resolved by adding a crash protection mechanism during a PoE power change state in the AP. **Scenario:** This issue occurred when the PoE hardware detection on the AP was at 802.3AF but the LLDP negotiated at 802.3AT. Hence, a race condition occurred. This issue was observed in OAW-AP270 Series access points running AOS-W 6.4.4.8.	AP-Platform	OAW-AP270 Series access points	AOS-W 6.4.4.8	AOS-W 6.4.4.12

Table 4: *Resolved Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
152332	**Symptom:** A blank image was displayed on the logon wait screen before the user was redirected to the captive portal page. The fix ensures that the user is redirected without any delay and the captive portal page appears correctly. **Scenario:** This issue occurred when the **logon-wait cpu-threshold** parameter was configured and the CPU utilization was high. As a result, the **HTTPD** process returned a transitional HTML page before redirecting to the captive portal page.	Web Server	All platforms	AOS-W 6.4.4.9	AOS-W 6.4.4.12
152525	**Symptom:** A switch assigned IP address to clients from an incorrect VLAN. The fix ensures that a switch assigns IP address from the correct VLAN. **Scenario:** This issue occurred after the reauthentication timer set on the 802.1X profile expired. This issue was observed in switches running AOS-W 6.4.3.9.	Base OS Security	All platforms	AOS-W 6.4.3.9	AOS-W 6.4.4.12
152614 155789	**Symptom:** After a full configuration synchronization, the AirGroup chat ID **_presence._tcp** was found missing from the running configuration of the local switch. The fix ensures that the missing chat ID is included in the running configuration of the local switch. **Scenario:** This issue was observed in a master-local deployment with switches running AOS-W 6.5.0.0.	AirGroup	All platforms	AOS-W 6.5.0.0	AOS-W 6.4.4.12
152890 153324 156647	**Symptom:** A switch stopped responding and rebooted unexpectedly. The log file listed the reason for the event as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. Updating the SDK to the latest version resolved this issue. **Scenario:** This issue occurred when the WebCC feature was enabled in a switch. This issue was observed in switches running AOS-W 6.4.4.8.	Switch-Datapath	All platforms	AOS-W 6.4.4.8	AOS-W 6.4.4.12
153073	**Symptom:** An L2 GRE tunnel inside an IPsec tunnel failed. This issue is resolved by resetting the packet VLAN after GRE encapsulation. **Scenario:** This issue occurred when an L2 GRE tunnel VLAN was configured with policy-based routing rules. This issue was observed in switches running AOS-W 6.4.4.9.	GRE	All platforms	AOS-W 6.4.4.9	AOS-W 6.4.4.12

Table 4: *Resolved Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
154132	**Symptom:** The radio lights in an AP were turned off and clients were unable to associate with the AP. However, the **show ap bss-table** command showed that the AP was active and broadcasting an SSID. This issue is resolved by allowing an AP to reject HA configuration if the AP does not connect to LMS. **Scenario:** This issue occurred when an AP accepted HA configuration and connected to a standby switch even though the AP did not connect to LMS. This issue was observed in a HA topology with APs running AOS-W 6.4.4.10.	AP-Wireless	All platforms	AOS-W 6.4.4.10	AOS-W 6.4.4.12
154146	**Symptom:** The **BOCMGR** process in a switch attempted to contact an Activate server periodically. The fix ensures that the **BOCMGR** process in a switch does not contact an Activate server unnecessarily. **Scenario:** This issue was observed in OAW-4x04 Series or OAW-40xx Series switches running ArubaOS 6.4.4.11.	Configuration	OAW-4x04 Series or OAW-4x50 Series switches	AOS-W 6.4.4.11	AOS-W 6.4.4.12
154147	**Symptom:** A client failed to establish an IKE VPN connection over an existing IPsec/L2TP VPN connection. This issue is resolved by adding an exception for the IKE traffic coming as L2TP traffic and by allowing the encryption of this IKE traffic in transport mode IPsec tunnel. **Scenario:** This issue occurred because IKE traffic encryption over transport mode IPsec tunnel was blocked. This also blocked the IKE traffic coming into the L2TP tunnel.	IPsec	All platforms	AOS-W 6.4.4.9	AOS-W 6.4.4.12
154288	**Symptom:** 802.11V BSS transition management failures were observed during a client match event which directed a client to another BSSID. This issue is resolved by modifying 802.11V client match steering requests so that the target radio BSSID matches the BSSID used by the client, rather than the base BSSID of the radio. **Scenario:** This issue occurred when the clients were steered to another BSSID based on the base BSSID of the AP radio. This issue was observed in switches running AOS-W 6.5.1.1.	ARM	All platforms	AOS-W 6.5.1.1	AOS-W 6.4.4.12

Table 4: *Resolved Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
154381	**Symptom:** Clients failed to access the captive portal page. The fix ensures that the clients can successfully access the captive portal page. **Scenario:** This issue occurred when clients used L2TP over IPsec to connect to a switch. This issue was observed in switches running AOS-W 6.5.0.3 or later versions.	Captive Portal	All platforms	AOS-W 6.5.0.3	AOS-W 6.4.4.12
154407	**Symptom:** A VIA client failed to establish a connection with a switch. Improvements in the ISAKMP hash algorithm resolved the issue. **Scenario:** This issue occurred when a custom ISAKMP policy was configured on a switch. This issue was observed in switches running AOS-W 6.5.1.2.	IPsec	All platforms	AOS-W 6.5.1.2	AOS-W 6.4.4.12
154443	**Symptom:** A user was stuck in the machine authentication role after an 802.1X authentication. The fix ensures that the user role is updated in the AP datapath. **Scenario:** This issue occurred when a user attempted multiple L2 authentications in split-tunnel forwarding mode and the user role was not updated in the AP datapath. This issue was observed in a master-local deployment with switches running AOS-W 6.4.4.10.	Base OS Security	All platforms	AOS-W 6.4.4.10	AOS-W 6.4.4.12
154487	**Symptom:** The **FPCLI** process in a switch crashed unexpectedly. The fix ensures that the **FPCLI** process does not crash when a user executes the **show user authentication-method stateful-dot1x** command. **Scenario:** This issue occurred when a user executed the **show user authentication-method stateful-dot1x** command.This issue was observed in a master-local deployment with switches running AOS-W 6.4.2.16.	Base OS Security	All platforms	AOS-W 6.4.2.16	AOS-W 6.4.4.12
154581	**Symptom:** A saved spectrum view was not loaded. The fix ensures that a saved spectrum view is loaded. **Scenario:** This issue was observed in switches running AOS-W 6.4.4.9.	Spectrum	All platforms	AOS-W 6.4.4.9	AOS-W 6.4.4.12

Table 4: *Resolved Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
155038	**Symptom:** The TACACS accounting configuration was deleted. The fix ensures that the TACACS accounting configuration is retained after upgrading AOS-W. **Scenario:** This issue occurred after upgrading a switch from AOS-W 6.4.2.x to AOS-W 6.4.3.x or later versions.	Base OS Security	All platforms	AOS-W 6.4.4.11	AOS-W 6.4.4.12
155215	**Symptom:** A user could not access the RAP console page. The fix ensures that the user can access the RAP console page. **Scenario:** This issue occurred when a user was in bridge-forwarding mode and attempted to access the RAP console page. This issue was observed in Remote APs running AOS-W 6.4.3.x, AOS-W 6.4.4.x, or AOS-W 6.5.1.x.	AP Datapath	All Remote AP platforms	AOS-W 6.4.4.11	AOS-W 6.4.4.12
155425	**Symptom:** Auto Sign-On between a switch and ClearPass Policy Manager failed. The fix ensures that Auto Sign-On succeeds. **Scenario:** This issue occurred when the length of a username exceeded 25 characters. This issue was observed in switches running AOS-W 6.4.4.11.	Base OS Security	All platforms	AOS-W 6.4.4.11	AOS-W 6.4.4.12

Table 4: *Resolved Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
155527	**Symptom:** An AP stopped responding and rebooted. The log file listed the reason for the event as **Reboot caused by kernel panic: Fatal exception**. Improvements in the AP memory management resolved the issue. **Scenario:** This issue was observed in OAW-AP210 Series access points running AOS-W 6.5.0.3 or AOS-W 6.5.1.2.	AP-Wireless	OAW-AP210 Series access points	AOS-W 6.5.1.2	AOS-W 6.4.4.12
155977	**Symptom:** A switch prompted to reboot when a non-master VRRP instance was added. The fix ensures that the switch does not prompt to reboot when a non-master VRRP instance is added. **Scenario:** This issue occurred when the **no shutdown** command was executed after adding a non-master VRRP instance. This issue was observed in a master-standby topology with switches running AOS-W 6.3.1.18.	VRRP	All platforms	AOS-W 6.3.1.18	AOS-W 6.4.4.12
157279	**Symptom:** The heartbeats between two switches failed although the APs completed an HA failover. The fix ensures that the heartbeats function as expected. **Scenario:** This issue occurred when an IPSsec tunnel was not established between the two switches. This issue was observed in a master-local topology with switches running AOS-W 6.4.4.12.	Switch-Datapath	All platforms	AOS-W 6.4.4.12	AOS-W 6.4.4.12

This chapter describes the known and outstanding issues identified in AOS-W 6.4.4.12.

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 6.4.4.12*

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 error, **Not enough space on flash**. **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 6.4.2.12
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 LLDP-MED is connected to the downlink Ethernet port of an AP. This issue is observed in APs running AOS-W 6.4.3.3. **Workaround:** None.	AP-Platform	All platforms	AOS-W 6.4.3.3
124275 151661	**Symptom:** All clients continue to obtain IP addresses from the same VLAN even though a RADIUS server VSA specifies a VLAN pool with multiple VLANs. **Scenario:** This issue 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
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

Table 5: *Known Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version
130981	**Symptom:** A switch reboots unexpectedly. The log file for the event lists the reason as **datapath timeout**. **Scenario:** This issue occurs when the **copy** command has the **** characters at the end of the destination folder name. For example, AOS-W misinterprets the **** characters in the **copy flash: crash.tar ftp: 10.1.1.1.test-user \ArubaOS\\ crash.tar** command.. This issue is observed in switches running AOS-W 6.4.4.0. **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
132714	**Symptom:** When an administrator tries to add a static ARP entry, a switch displays the **Cannot add static ARP entry** error message. The log file lists the reason for the event as **Static ARP: too many entries (ipMapArpStaticEntryAdd)**. **Scenario:** This issue occurs because the static ARP counter continues to increment every time there is a change in the link status. This issue is observed in switches running AOS-W 6.4.3.4. **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 **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
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

Table 5: *Known Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version
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
142678	**Symptom:** Adding an NTP server to a switch causes all the Instant AP VPN/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

Table 5: *Known Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version
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	OAW-AP103H access points	AOS-W 6.4.4.6
143566	**Symptom:** A switch displays the **Module authentication is busy. Please try later** error when the **show reference user-role <role-name>** command is executed. **Scenario:** This issue occurs when more than 212 entries existed for a given role in user derivation-rules or server-group derivation rules. This issue is observed in a master-local deployment 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
145867	**Symptom:** An AP does not boot. The log file lists the reason for the event as **Kernel panic - not syncing: Fatal exception**. **Scenario:** This issue is observed in OAW-AP275 access points running AOS-W 6.4.3.9. **Workaround:** None.	AP-Wireless	OAW-AP275 access points	AOS-W 6.4.3.9
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

Table 5: *Known Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version
148977 155343	**Symptom:** A branch office switch randomly loses configuration updates from the master switch. **Scenario:** his 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 a master-branch office switch deployment with switches running AOS-W 6.5.0.0 or later versions. **Workaround:** None.	Licensing	All platforms	AOS-W 6.5.0.0

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

150693	**Symptom:** A datapath route-cache entry is not cleared when an L3 GRE tunnel is closed. **Scenario:** This issue occurs after a channel change is triggered on the APs due to a RADAR detection. This issue is observed in switches running AOS-W 6.4.3.9. **Workaround:** None.	Open Shortest Path First	All platforms	AOS-W 6.4.3.9

Table 5: *Known Issues in 6.4.4.12*

Bug ID	Description	Component	Platform	Reported Version
152602 154513	**Symptom:** The master switch fails to delete the stale route entries of the branch office switch. When you attempt to manually delete an entry, the switch does not delete the entry and displays the following error message: **ERROR: Cannot Delete Static Route**. **Scenario:** This issue occurs when you change the VLAN IP address of the branch office switch and upload the updated CSV file (static IP address template) on the master switch. This triggers a reboot of the branch office switch but fails to delete the stale route entries from the master switch. This issue is observed in a master-branch office switch deployment with switches running AOS-W 6.5.1.1 or later versions. **Workaround:** None.	Branch Office Switch	All platforms	AOS-W 6.5.1.1
153011	**Symptom:** An access point crashes unexpectedly. **Scenario:** This issue is observed in OAW-AP125 access points running AOS-W 6.4.4.10. **Workaround:** None.	AP-Wireless	OAW-AP125 access points	AOS-W 6.4.4.10
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

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

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

Topics in this chapter include:

Upgrade Caveats

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

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

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

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

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

- AOS-W 6.4.x supports only the newer MIPS switches (OAW-4306 Series, OAW-4504XM, OAW-4604, OAW-4704, OAW-M3, OAW-40xx Series, and OAW-4x50 Series). Legacy PPC switches (OAW-4302, OAW-4308, OAW-4324, SC1/SC2) 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 38.)

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 37 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 37 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 37 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 37.

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 6.4.4.12

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 6.4.4.12

The following sections provide the procedures for upgrading the switch to AOS-W 6.4.4.12 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 36.

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 6.4.4.12.

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 6.4.4.12 on page 39 to install the interim version of AOS-W, and then repeat steps 1 through 11 of the procedure to download and install AOS-W 6.4.4.12.

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 6.4.4.12 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 37 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 36.

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 6.4.4.12 on page 39.

Follow steps 2 through 7 of the procedure described in Upgrading to AOS-W 6.4.4.12 on page 39 to install the interim version of AOS-W, and then repeat steps 1 through 7 of the procedure to download and install AOS-W 6.4.4.12.

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 6.4.4.12 from the customer support site.
2. Open an SSH session on your master (and local) switches.
3. Execute the **ping** command to verify the network connection from the target switch to the SCP/FTP/TFTP server.

```
(host)# ping <ftphost>
```

or

```
(host)# ping <tftphost>
```

or

```
(host)# ping <scphost>
```

4. Execute the **show image version** command to check if the AOS-W images are loaded on the switch's flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

```
(host) #show image version
```

5. Execute the **copy** command to load the new image onto the nonboot partition.

```
(host)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
```

or

```
(host)# copy tftp: <tftphost> <image filename> system: partition <0|1>
```

or

```
(host)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
```

or

```
(host)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
```

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

6. Execute the **show image version** command to verify that the new image is loaded.

```
(host)# show image version
```

7. Reboot the switch.

```
(host)# reload
```

8. Execute the **show version** command to verify that the upgrade is complete.

```
(host)# show version
```

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

1. Log in to the CLI to verify that all your switches are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of access points and clients are what you expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 37 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 6.4.4.12 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 6.4.4.12 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 37.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W 6.4.4.12 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 6.4.4.12 flash backup from the file stored on the switch. Do not restore the AOS-W 6.4.4.12 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 6.4.4.12, the changes do not appear in RF Plan in the downgraded AOS-W version.
   - If you installed any certificates while running AOS-W 6.4.4.12, 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 6.4.4.12 image.

   ```
   #show image version
   ```

4. Set the backup system partition as the new boot partition.

   ```
   (host) # boot system partition 1
   ```

5. Reboot the switch.
   ```
   (host) # reload
   ```
6. When the boot process is complete, verify that the switch is using the correct software.
   ```
   (host) # show image version
   ```

Before You Call Technical Support

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

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

Appendix a
Acronyms and Abbreviations

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

Table 6: *List of Acronyms and Abbreviations*

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

Table 6: *List of Acronyms and Abbreviations*

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

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
BRE	Basic Regular Expression
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CA	Certification Authority
CAC	Call Admission Control
CALEA	Communications Assistance for Law Enforcement Act
CAP	Campus AP
CCA	Clear Channel Assessment
CDP	Cisco Discovery Protocol
CDR	Call Detail Records
CEF	Common Event Format
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CLI	Command-Line Interface
CN	Common Name
CoA	Change of Authorization
CoS	Class of Service
CPE	Customer Premises Equipment

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
CPsec	Control Plane Security
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSA	Channel Switch Announcement
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSR	Certificate Signing Request
CSV	Comma Separated Values
CTS	Clear to Send
CW	Contention Window
DAS	Distributed Antenna System
dB	Decibel
dBm	Decibel Milliwatt
DCB	Data Center Bridging
DCE	Data Communication Equipment
DCF	Distributed Coordination Function
DDMO	Distributed Dynamic Multicast Optimization
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
DFT	Discreet Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMO	Dynamic Multicast optimization
DN	Distinguished Name
DNS	Domain Name System
DOCSIS	Data over Cable Service Interface Specification
DoS	Denial of Service
DPD	Dead Peer Detection
DPI	Deep Packet Inspection
DR	Designated Router
DRT	Downloadable Regulatory Table
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum
DST	Daylight Saving Time
DTE	Data Terminal Equipment
DTIM	Delivery Traffic Indication Message
DTLS	Datagram Transport Layer Security
DU	Data Unit

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
EAP	Extensible Authentication Protocol
EAP-FAST	EAP-Flexible Authentication Secure Tunnel
EAP-GTC	EAP-Generic Token Card
EAP-MD5	EAP-Method Digest 5
EAP-MSCHAP EAP-MSCHAPv2	EAP-Microsoft Challenge Handshake Authentication Protocol
EAPoL	EAP over LAN
EAPoUDP	EAP over UDP
EAP-PEAP	EAP-Protected EAP
EAP-PWD	EAP-Password
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
ECC	Elliptical Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EIGRP	Enhanced Interior Gateway Routing Protocol
EIRP	Effective Isotropic Radiated Power
EMM	Enterprise Mobility Management
ESI	External Services Interface
ESS	Extended Service Set

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
ESSID	Extended Service Set Identifier
EULA	End User License Agreement
FCC	Federal Communications Commission
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FIB	Forwarding Information Base
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
FQLN	Fully Qualified Location Name
FRER	Frame Receive Error Rate
FRR	Frame Retry Rate
FSPL	Free Space Path Loss
FTP	File Transfer Protocol
GBps	Gigabytes per second
Gbps	Gigabits per second
GHz	Gigahertz
GIS	Generic Interface Specification
GMT	Greenwich Mean Time
GPP	Guest Provisioning Page
GPS	Global Positioning System

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
GVRP	GARP or Generic VLAN Registration Protocol
H2QP	Hotspot 2.0 Query Protocol
HA	High Availability
HMD	High Mobility Device
HSPA	High-Speed Packet Access
HT	High Throughput
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS	Internet Authentication Service
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IDS	Intrusion Detection System
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
IKE PSK	Internet Key Exchange Pre-shared Key
IoT	Internet of Things
IP	Internet Protocol
IPM	Intelligent Power Monitoring
IPS	Intrusion Prevention System
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
JSON	JavaScript Object Notation
KBps	Kilobytes per second
Kbps	Kilobits per second
L2TP	Layer-2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDPC	Low-Density Parity-Check
LEA	Law Enforcement Agency
LEAP	Lightweight Extensible Authentication Protocol

Table 6: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
LED	Light Emitting Diode
LEEF	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