AOS-W 6.5.1.2

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. (July 2016)

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 6.5.1.2 is a software patch release that includes fixes to issues identified in previous releases.

> **NOTE**
> See the Upgrade Procedure on page 19 for instructions on how to upgrade your switch to this release.

Chapter Overview

- New Features provides a description of features and enhancements introduced in this release.
- Regulatory Updates describes the regulatory updates in this release.
- Resolved Issues describes the issues resolved in this release.
- Known Issues describes the known and outstanding issues identified in this release.
- Upgrade Procedure describes the procedures for upgrading a switch to this release.

> **NOTE**
> For information regarding prior releases, refer to the corresponding Release Notes on https://support.esd.alcatel-lucent.com/.

Supported Browsers

The following browsers are officially supported for use with AOS-W 6.5.1.2 WebUI:

- Microsoft Internet Explorer 10.x and 11 on Windows 7 and Windows 8
- Mozilla Firefox 23 or later on Windows Vista, Windows 7, and Mac OS
- Apple Safari 5.1.7 or later on Mac OS
- Chrome 51.0.2704.103 m (64-bit)
- Microsoft Edge 25.10586.0.0 and Microsoft Edge HTML 13.10586

Contacting Support

Table 2: *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	
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 section describes the new features, enhancements, and hardware introduced in AOS-W 6.5.1.2. For more information about these features, refer to the *AOS-W 6.5.1.x User Guide*.

AP-Platform

PoE Optimization Support on OAW-AP205H

Starting from AOS-W 6.5.1.2, PoE optimization is supported on the OAW-AP205H access point. On enabling this feature, the following events occur on the AP:

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

You can enable PoE optimization on this AP from the WebUI or CLI.

In the WebUI

The following procedure performed in the WebUI enables PoE optimization on the OAW-AP205H access point:

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

In the CLI

Execute the following commands to enable PoE optimization on the OAW-AP205H access point using the CLI:

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

Branch Office Switch

L2 VLAN Support for Bulk Edit

Starting from AOS-W 6.5.1.2, you can add the L2 VLAN entries using the bulk edit CSV file. Once the CSV file is uploaded, the master switch pushes the configuration to the respective branch switches. To add the L2 VLAN entries using the master switch WebUI:

1. Navigate to **Configuration > BRANCH > Smart Config** and select the **Management** tab.

2. Click the **New** button under **Branch Config Group List**.
   You are prompted to enter a name for the new branch configuration group profile.

3. Enter a name for the branch configuration group profile.

4. Click **OK**.

5. Select the model type of your branch switch from the **Model** drop-down list.
   Each profile can support a single switch model.

6. Select **Static** from the **IP Address Management** drop-down list.

7. Select the **Export** option from the drop-down list and click **Download**.
   The switch downloads the *export-StaticBranchConfigGroup.csv* file.

8. In the *export-StaticBranchConfigGroup.csv* file, add the MAC address and VLAN ID under the **Mac address** and **Vlan1** fields respectively.

9. Save the file.

10. To upload the file, select the **Import** option from the drop-down list, choose the file from the client laptop, and click **Upload**.

11. Click **Apply** and **Save Configuration**.

This feature cannot be configured from the CLI.

Switch-Datapath

New Flag

A new flag, **W** (Wi-Fi), is introduced as a part of the **show datapath bridge** command to indicate that the source of the bridge entry is learned through a Wi-Fi tunnel. A sample output of the command is as follows:

```
(host) #show datapath bridge

Datapath Bridge Table Entries
-----------------------------

Flags: P - Permanent, D - Deny, R - Roamed Client, M - Mobile,
       X - Xsec, A - Auth, T - Trusted, W - Wifi

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

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

The following default Downloadable Regulatory Table (DRT) version is part of AOS-W 6.5.1.2:

- DRT-1.0_57440

For a complete list of countries certified with different AP models, refer to the DRT Release Notes at support.esd.alcatel-lucent.com.

This software release supports the channel requirements described in *ALE Support Advisory SA-N0033*, available for download from the support.esd.alcatel-lucent.com site.

This section describes the issues resolved in AOS-W 6.5.1.2

Table 3: *Resolved Issues in AOS-W 6.5.1.2*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
137617 143207 148674 150451 150737	**Symptom:** User was unable to access the WebUI. This issue is resolved by releasing HTTPD resources using a query timeout. **Scenario:** The issue occurred when the HTTP process was busy, because of which the switch no longer responded to new incoming connections. This issue was observed in switches running AOS-W 6.4.3.5 or later versions.	Web Server	All platforms	AOS-W 6.4.3.5	AOS-W 6.5.1.2
143836	**Symptom:** An Instant AP deployed as a campus AP, failed to come online on the switch using a 4G uplink. The fix ensures that the AP boots up successfully on the switch using a 4G uplink. **Scenario:**This issue occurred when the AP uplink router MTU was changed to a value lesser than the length of the packet sent by the AP. This issue was observed in OAW-AP100 Series access points running AOS-W 6.4.2.12 or later versions.	AP-Platform	OAW-AP100 Series access points	AOS-W 6.4.2.12	AOS-W 6.5.1.2
144570 148449	**Symptom:** An AP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**. Improvements in the WLAN driver of the AP resolved this issue. **Scenario:** This issue occurred when an IPsec tunnel was terminated and the queued cryptography context was cleared. This issue was observed in OAW-AP200 Series, OAW-AP210 Series, and OAW-AP220 Series access points running AOS-W 6.4.4.8 or later versions.	AP-Platform	OAW-AP200 Series, OAW-AP210 Series, and OAW-AP220 Series access points	AOS-W 6.4.4.8	AOS-W 6.5.1.2

Table 3: *Resolved Issues in AOS-W 6.5.1.2*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
145346 150273 150761	**Symptom:** An AP stopped responding and rebooted. The log files listed the reason for the event as **Badness at kernel/workqueue.c:495**. Improvements in the WLAN driver of the AP resolved this issue. **Scenario:** This issue was observed when the AP was configured as a spectrum monitor mode in 802.11g band and air monitor mode in 802.11a band. This issue was observed in OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, and OAW-AP270 Series access points running AOS-W 6.5.1.0.	AP-Wireless	OAW-AP200 Series, OAW-AP210 Series, OAW-AP220 Series, and OAW-AP270 Series access points	AOS-W 6.5.1.0	AOS-W 6.5.1.2
145852	**Symptom:** An AP stopped responding and rebooted unexpectedly. The log file for the event listed the reason as **Reboot caused by kernel panic: Rebooting the AP because of FW ASSERT**. This issue is resolved by checking incoming packets and dropping packets where: ● The source address is either multicast or the address is NULL. ● The source address corresponds with the VAP BSSID node. **Scenario:** This issue occurred when the firmware file displayed an incoming authentication frame where the source address was equivalent to broadcast. This issue was observed in OAW-AP325 access points running AOS-W 6.4.4.8.	AP-Wireless	OAW-AP325 access points	AOS-W 6.4.4.8	AOS-W 6.5.1.2
146685	**Symptom:** Clients experienced low throughput for specific SSIDs. This issue is resolved by adding an unallocated token into the traffic management shared pool. **Scenario:** This issue occurred under the following circumstances in the given order of sequence: ● When three VAPs were enabled with no clients ● When AOS-W recycled the bandwidth allocation tokens and added them in the traffic management shared pool ● When the three VAPs were disabled, the shared pool was empty and the tokens were lost This issue was observed in switches running AOS-W 6.4.2.6.	AP-Wireless	All platforms	AOS-W 6.4.2.6	AOS-W 6.5.1.2

Table 3: *Resolved Issues in AOS-W 6.5.1.2*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
146874	**Symptom:** The WLAN network experienced bad Lync sessions intermittently. The fix ensures that while processing the data frame from the client, the Traffic Identifier and the Access Category (AC) of the packets are checked, so that AP scan requests are also rejected on receiving voice and video frames from the client. **Scenario:** The voice and video aware scanning parameters allowed voice and video traffic passed by the AP to the client on the downlink port only. AP scan requests were rejected by the host driver so that the voice and video traffic was not interrupted. But, when the client passed the voice and video traffic to the AP on the uplink port only, AP scan requests were not rejected. This resulted in the AP missing frames from the client, and thereby affected the audio and video quality. 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 6.5.1.2
147543	**Symptom:** An AP sent Clear to Send (CTS) frames at 1 Mbps rate on the 2.4 GHz radio although the lower rates were removed from the SSID profile. Fixing the basic and transmit rates in the hardware register of the AP fixed the issue. **Scenario:** This issue was observed in OAW-AP300 Series, OAW-AP310 Series, and OAW-AP330 Series access points running AOS-W 6.5.0.0.	AP-Wireless	OAW-AP300 Series, OAW-AP310 Series, and OAW-AP330 Series access points	AOS-W 6.5.0.0	AOS-W 6.5.1.2
148103	**Symptom:** One-way audio was observed in Vocera communication badges. The fix ensures that the **R** (Roamed client) flag is added to the session if it belongs to a roamed user. **Scenario:** This issue was observed under the following circumstances: ● The clients performed an L3 roaming. ● The roamed client made a call to a client associated to the switch as a local client. For the roamed client, the switch acted as a foreign agent. This issue was observed in switches running AOS-W 6.4.2.x or later versions.	UCC	All platforms	AOS-W 6.4.2.13	AOS-W 6.5.1.2

Table 3: *Resolved Issues in AOS-W 6.5.1.2*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
148113	**Symptom:** A client failed to get an IP address when it roamed between APs. The fix ensures that the client gets an appropriate IP address when it roams between APs. **Scenario:** This issue was observed under the following circumstances: ● L3 mobility was enabled globally. ● Mobile-IP was disabled on the virtual AP. Mobile-IP changed the bridge entry even when the client roamed across APs terminating on the same switch. This issue was observed in switches running AOS-W 6.4.2.8.	Mobility	All platforms	AOS-W 6.4.2.8	AOS-W 6.5.1.2
148160 152187	**Symptom:** An AP stopped responding and rebooted. The log file for the event listed the reason as **Critical process /aruba/bin/stm [pid 3249] DIED, process marked as RESTART**. Improvements in the memory utilized by the station management process resolved the issue. **Scenario:** This issue occurred because the client did not have the capability to be detected accurately. This issue was observed in OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access points running AOS-W 6.5.1.0.	Station Management	OAW-AP300 Series, OAW-AP310 Series, OAW-AP320 Series, and OAW-AP330 Series access point	AOS-W 6.5.1.0	AOS-W 6.5.1.2
148371	**Symptom:** OV3600 displayed null data for **AP Operational Status**, **Duplex**, **Input Capacity**, and **Output Capacity** parameters. The fix ensures that the AP sends the port status to the switch when HA is enabled with CPsec. **Scenario:** This issue was observed when the AP did not send the port status update to the switch when HA was enabled with CPsec. This issue was observed in OAW-AP205H access points running AOS-W 6.4.4.8 in a master-local topology.	AP-Platform	OAW-AP205H access points	AOS-W 6.4.4.8	AOS-W 6.5.1.2
148671	**Symptom:** Few APs discovered the master switch using ADP although the DHCP options 43 and 60 were configured. The fix ensures that the APs discover the master switch using DHCP options 43 and 60. **Scenario:** This issue was observed when the AP received an IPv6 address and then discovered that the master switch using ADP. Post-ADP, when the AP received an IPv4 address and discovered another master switch using DHCP options, the AP was unable to recover the master switch from ADP. This issue was observed in switches running AOS-W 6.4.3.7.	AP-Platform	All platforms	AOS-W 6.4.3.7	AOS-W 6.5.1.2

Table 3: *Resolved Issues in AOS-W 6.5.1.2*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
149307 149555	**Symptom:** On HA failover, clients failed to get an IP address or connect to the WLAN network. The fix ensures that the clients get an IP address and successfully pass traffic. **Scenario:** This issue was observed under the following circumstances: ● During a brief interruption of communication to LMS and backup LMS simultaneously, the AP does not reboot. ● AP connects to the backup LMS. ● AP does not receive the HA information. ● Clients failed to get an IP address or connect to the WLAN network. On shutting down LMS and backup LMS, the AP attempted an HA failover to the standby switch but could not receive the **FAILOVER** response from the standby switch. This issue was observed in OAW-AP320 Series access points running AOS-W 6.4.4.8.	AP-Platform	OAW-AP320 Series access points	AOS-W 6.4.4.8	AOS-W 6.5.1.2
150176	**Symptom:** A Verifone e355 point-of-sale device failed to receive data from the switch when it went in power save mode. The fix ensures that the bridge entry does not age out from the bridge table as long as the device is associated with the AP. A new flag **W** (Wi-Fi) is introduced as part of the output of the **show datapath bridge** command to indicate that the bridge entry is learned through a Wi-Fi tunnel. **Scenario:** This issue occurred under the following circumstances: ● The device was in power save mode. ● The device did not send any L2/L3 traffic. As the device did not send any traffic, the switch removed the bridge entry from the bridge table after the age out timer of eight minutes. This issue occurred even when the device was associated to the AP. This issue was observed in switches running AOS-W 6.4.3.9 or later versions.	Switch-Datapath	All platforms	AOS-W 6.4.3.9	AOS-W 6.5.1.2
150433 151249	**Symptom:** An AP crashed and rebooted unexpectedly. The log files listed the reason for the event as **kernel panic**. This issue is resolved by supporting a bandwidth of 80 + 80 MHz / 160 MHz even when the configuration support of 160 MHz is not defined. **Scenario:** This issue was observed in OAW-AP300 Series, OAW-AP310 Series, and OAW-AP320 Series access points running AOS-W 6.5.0.1.	AP-Platform	OAW-AP300 Series, OAW-AP310 Series, and OAW-AP320 Series access points	AOS-W 6.5.0.1	AOS-W 6.5.1.2

Table 3: *Resolved Issues in AOS-W 6.5.1.2*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
150578	**Symptom:** An AP frequently stopped forwarding RTP packets to its wired uplink (in this case GRE tunnel) port. The fix ensures that the AP forwards the RTP packets to its wired uplink port consistently without any delay. **Scenario:** This issue was seen under the following circumstances: ● A busy 802.11g channel with channel utilization above 30%. ● Multiple voice session on the AP. This issue was observed in OAW-AP325 access points running AOS-W 6.5.0.1.	AP-Wireless	OAW-AP325 access points	AOS-W 6.5.0.1	AOS-W 6.5.1.2
151197	**Symptom: ENET0** and **ENET1** ethernet ports of the AP were connected to a switch. On disconnecting the **ENET0** port and keeping the **ENET1** port connected, the AP continued to broadcast the SSID, but clients did not pass any traffic. The fix ensures that the clients continue to pass traffic. **Scenario:** This issue was observed in OAW-AP330 Series access points running AOS-W 6.5.0.1.	AP-Datapath	OAW-AP330 Series access points	AOS-W 6.5.0.1	AOS-W 6.5.1.2
152677 153072	**Symptom:** Heart rate monitors failed to pass traffic when three or more devices connected to the AP. Improvements in the Wi-Fi driver of the AP resolved this issue. **Scenario:** This issue was seen with legacy non-WMM capable clients that operate in PS-POLL power saving mode. This issue was observed when such legacy clients associate with OAW-AP315 access points running AOS-W 6.5.0.0 or later versions.	AP-Platform	OAW-AP315 access points	AOS-W 6.5.0.0	AOS-W 6.5.1.2

This section describes the known and outstanding issues identified in AOS-W 6.5.1.2.

Table 4: *Known Issues in AOS-W 6.5.1.2*

Bug ID	Description	Component	Platform	Reported Version
148348 152019 152020	**Symptom:** An AP stops responding and reboots unexpectedly. The log files list the reason for the event as **kernel panic**. **Scenario:** This issue is observed in OAW-AP310 Series access points running AOS-W 6.5.0.1 or later versions. **Workaround:** None.	AP-Wireless	OAW-AP310 Series access points	AOS-W 6.5.0.1

This chapter details the 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

- OAW-AP120 Series access points, OAW-4306 Series, OAW-4x04 Series, OAW-S3, and OAW-6000 switches are not supported from AOS-W 6.5.x. Do not upgrade to AOS-W 6.5.x if your deployment contains a mix of these switches in a master-local setup.
- If your switch is running AOS-W 6.4.0.0 or later versions, do not use a Windows-based TFTP server to copy the AOS-W image to the nonboot partition of the switch for upgrading or downgrading. Use FTP or SCP to copy the image.
- Starting from AOS-W 6.4.x, you cannot 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 following 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) #!
(host)(config) #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
```

- 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 23.)

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 6.5.1.2 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 6.5.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 22 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 22 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 22 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 22.

> For proper operation, all switches in the network must be upgraded with the same version of AOS-W software. For redundant environments such as VRRP, 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 6.5.1.2

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

Instructions on Installing FIPS Software

> Before you install a FIPS version of the software on a switch that is currently running a non-FIPS version of the software, follow the procedure below. If you are currently running a FIPS version of the software on the switch, you do not have to perform a **write erase** to reset the configuration as mentioned in step 2.

Follow the steps below to install the FIPS software on a switch 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 6.5.1.2

The following sections provide the procedures for upgrading the switch to AOS-W 6.5.1.2 by using the WebUI and the CLI.

Install Using the WebUI

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 21.

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.

When upgrading from an existing AOS-W 6.4.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 6.4.3.9.

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 6.5.1.2 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 > Controller > 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. Choose the nonboot partition from the **Partition to Upgrade** radio button.

8. Choose **Yes** in the **Reboot Controller After Upgrade** radio button to automatically reboot after upgrading. Choose **No**, if you do not want the switch to reboot immediately.

NOTE: Upgrade will not take effect until you reboot the switch.

---

9. Choose **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 22 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

CAUTION: 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 21.

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

1. Download AOS-W 6.5.1.2 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**.

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-40xx Series and OAW-4x50 Series switches.

---

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

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 22 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 6.5.1.2 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 do not downgrade to a previously saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from AOS-W 6.5.1.2 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 22.
2. Verify that the control plane security is disabled.
3. Set the switch to boot with the previously saved pre-AOS-W 6.5.1.2 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 6.5.1.2 flash backup from the file stored on the switch. Do not restore the AOS-W 6.5.1.2 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 6.5.1.2, the changes do not appear in RF Plan in the downgraded AOS-W version.
    - If you installed any certificates while running AOS-W 6.5.1.2, 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 6.1.3.2. Partition 0, the default boot partition, contains the AOS-W 6.5.1.2 image.

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 5: *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 5: *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 5: *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 5: *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 5: *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 5: *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 5: *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 5: *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 5: *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 5: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
LED	Light Emitting Diode
LEEF	Long Event Extended Format
LI	Lawful Interception
LLDP	Link Layer Discovery Protocol
LLDP-MED	LLDP–Media Endpoint Discovery
LMS	Local Management Switch
LNS	L2TP Network Server
LTE	Long Term Evolution
MAB	MAC Authentication Bypass
MAC	Media Access Control
MAM	Mobile Application Management
MBps	Megabytes per second
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MD5	Message Digest 5
MDM	Mobile Device Management
mDNS	Multicast Domain Name System
MFA	Multi-factor Authentication
MHz	Megahertz

Table 5: *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 5: *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 5: *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 5: *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 5: *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 5: *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 5: *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 5: *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 5: *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 5: *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