AOS-W Instant 6.4.4.8-4.2.4.5

Release Notes

AOS-W Instant 6.4.4.8-4.2.4.5 is a patch release that introduces enhancements and fixes to the issues found in the previous release.

For information on upgrading OAW-IAPs to the new release version, refer to the *Upgrading an OAW-IAP* topic in the *AOS-W Instant 6.4.4.6-4.2.4.0 User Guide.*

Contents

Contacting Support

Table 1: *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 chapter lists the regulatory information, and fixed issues in the AOS-W Instant 6.4.4.8-4.2.4.5 release.

Regulatory Domain Updates

The following table lists the DRT file versions supported by Instant 6.4.4.x-4.2.4.x releases:

Table 2: *DRT Versions*

Instant Release Version	Applicable DRT Version
6.4.8.8-4.2.4.5	1.0_57815
6.4.4.8-4.2.4.4	1.0_57223
6.4.4.8-4.2.4.3	1.0_56643
6.4.4.8-4.2.4.2	1.0_56050
6.4.4.8-4.2.4.1	1.0_55489
6.4.4.6-4.2.4.0	1.0_54870

For a complete list of countries certified with different AP models, see the respective DRT release notes at support.esd.alcatel-lucent.com.

New Features and Enhancements

The following enhancement is introduced in this release:

Support for Huawei E3372H-153 Modem on OAW-IAP205H

Starting from Instant 6.4.4.8-4.2.4.5, the Huawei E3372H-153 modem is supported on OAW-IAP205H access points.

Resolved Issues in this Release

The following issues are fixed in the Instant 6.4.4.8-4.2.4.5 release.

AppRF

Table 3: *AppRF Fixed Issue*

Bug ID	Description
147010	**Symptom**: Skype for Business sessions marked with SESSION_FLAG_ALG flag which are not skipped or deleted for stale session entries. The fix ensures that the session entries are skipped if the entries are stale and ALG is set. **Scenario**: This issue was observed in IAP-335 access points running a software version prior to Instant 6.4.4.8-4.2.4.5.

Datapath/Firewall

Table 4: *Platform Fixed Issue*

Bug ID	Description
152782	**Symptom**: OAW-IAP275 was booting up with restriction mode on the Cisco 2960 switch if the native VLAN on the switch port is not 1.This issue is resolved by updating the socket binding protocol for LLDP packets. **Scenario**: This issue was observed in OAW-IAP275 access points running a software version prior to Instant 6.4.4.8-4.2.4.5.

Mesh

Table 5: *Mesh Fixed Issue*

Bug ID	Description
145637	**Symptom**: OAW-IAP225 was running into a network loop when the uplink was restored and mesh was enabled. The fix ensures that the network looping issue is resolved. **Scenario**: This issue was observed in OAW-IAP225 access points running a software version prior to Instant 6.4.4.8-4.2.4.5.

Platform

Table 6: *Platform Fixed Issues*

Bug ID	Description
154509 127848	**Symptom**: An OAW-IAP crashed unexpectedly when using Huawei E353 modem. The log file of the event listed the reason as **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the OAW-IAP does not crash unexpectedly **Scenario**: This issue was observed in OAW-IAP205H access points running a software version prior to Instant 6.4.4.8-4.2.4.5.
145634	**Symptom**: An OAW-IAP crashed unexpectedly when using 10Mbps half-duplex uplink and upstream traffic exceed 10Mbps. The log file of the event listed the reason as kernel panic. The fix ensures that the OAW-IAP works without kernel panic with same uplink. **Scenario**: This issue was observed in OAW-IAP215 and OAW-IAP225 access points running a software version prior to Instant 6.4.4.8-4.2.4.5.
144570	**Symptom**: An OAW-IAP crashed and rebooted unexpectedly. The log file listed the reason for the event as **Reboot caused by kernel panic: Fatal exception in interrupt**. This issue is resolved by directly accessing the saved context data when crypto context is cleared. **Scenario**: This issue occurred when IPsec tunnels were closed and the queued crypto context was cleared. This issue was observed in IAP-200 Series, IAP-210 Series, or IAP-220 Series access points running a software version prior to Instant 6.4.4.8-4.2.4.5.
152840	**Symptom**: An OAW-IAP crashed and rebooted unexpectedly due to kernel panic. The fix ensures that the OAW-IAP does not crash unexpectedly. **Scenario**: This issue occurred when large size packets were sent from Centralized, L2 IPsec clients during an IPsec rekey operation. This issue was observed in OAW-IAP215 access points running a software version prior to Instant 6.4.4.8-4.2.4.5.

VPN

Table 7: *VPN Fixed Issue*

Bug ID	Description
149319	**Symptom**: Traffic sent to the corporate network was getting blocked when the volume of the traffic was heavy during IPsec SA rekey. The fix ensures that the IPsec tunnel device remains active when IPsec SA rekey is done. **Scenario**: This issue occurred during IPsec SA rekey and heavy traffic was sent to the corporate network through the IPsec tunnel. This issue was observed in OAW-IAP215 access points running a software version prior to Instant 6.4.4.8-4.2.4.5.

Wi-Fi Driver

Table 8: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
151995	**Symptom**: An OAW-IAP crashed and rebooted with the reason: **Reboot caused by kernel panic: Fatal exception**. The fix ensures that the OAW-IAP does not crash during compiler optimization. **Scenario**: This issue occurred when the compiler optimization was in progress and was observed in OAW-IAP215 access points running a software version prior to Instant 6.4.4.8-4.2.4.5.

Known Issues

The following known issues are identified in the Instant 6.4.4.x-4.2.4.x releases:

AppRF

Table 9: *AppRF Known Issue*

Bug ID	Description
120228	**Symptom**: The Skype application is not getting blocked when the App enforcement ACL is configured. **Scenario**: This issue occurs with OAW-IAPs that support the App enforcement feature, and is observed in all the OAW-IAPs running Instant 6.4.3.1-4.2.0.0 or later versions. **Workaround**: None.

This chapter describes the features and enhancements introduced in previous AOS-W Instant 6.4.4.x-4.2.4.x releases.

Features and Enhancements

The following features and enhancements were introduced in Instant 6.4.4.x-4.2.4.x releases.

Support for Telus Aircard 340U Modem

Starting from Instant 6.4.4.8-4.2.4.1, the Telus Aircard 340U modem is supported.

Support for Hotspot 2.0 on OAW-IAP325 Access Points

Starting from Instant 6.4.4.6-4.2.4.0, the Hotspot 2.0 (Passpoint Release 1) feature is supported on OAW-IAP325 access points. For more information, see:

- *Hotspot Profiles* in *AOS-W Instant 6.4.4.6-4.2.4.0 User Guide*.

Enhancement to Routing Profile Capability

A new field called **metric** has been added as part of the routing profile configuration. When two or more routes with the same destination are available for data transfer, the route with the lowest metric value takes precedence. For more information, see:

- *Configuring Routing Profiles* in *AOS-W Instant 6.4.4.6-4.2.4.0 User Guide.*
- **routing-profile** command in *AOS-W Instant 6.4.4.6-4.2.4.0 CLI Reference Guide.*

Enhancement for Disabling Default Auto Topology Rules

Starting from Instant 6.4.4.6-4.2.4.0, the auto topology rules can be disabled using the Instant UI and CLI. For more information, see:

- *Configuring Firewall Settings to Disable Auto Topology Rules* in *AOS-W Instant 6.4.4.6-4.2.4.0 User Guide.*
- **Firewall** command in *AOS-W Instant 6.4.4.6-4.2.4.0 CLI Reference Guide.*
- **show Firewall** command in *AOS-W Instant 6.4.4.6-4.2.4.0 CLI Reference Guide.*

Enhancement to ALE Monitoring Capabilities

Starting from Instant 6.4.4.6-4.2.4.0, ALE monitoring capabilities have been enhanced to receive notifications on the Wireless Backup Unit (WBU) stats and status of LTE 3G/4G modems. ALE is now notified with the following monitoring statistics:

- A LTE 3G/4G modem is plugged in or unplugged from the OAW-IAP USB port.
- The modem is incorrectly plugged in to the USB port of the slave OAW-IAP instead of the master OAW-IAP.
- The current status of the SIM card used in the modem.
- The current status of the uplink in use when the modem is connected to the master OAW-IAP.
- The WBU Rx or Tx bytes from the modem traffic when there is an uplink connectivity between the modem and the master OAW-IAP.

Additionally, the Master OAW-IAP will now notify ALE through hearbeat messages indicating the status (UP or DOWN) of the slave OAW-IAPs.

Allow Zero Touch Provisioning When NTP Server is Unreachable

Starting from Instant 6.4.4.6-4.2.4.0, zero-touch provisioning is allowed even when the NTP server is unavailable.

Wildcard Server Certificate Support for Captive Portal

Instant 6.4.4.8-4.2.4.4 now supports the wildcard server certificate for captive portal authentication.

New Command for Using VC IP Address as Source IP Address

The following command is introduced in Instant 6.4.4.8-4.2.4.4 to use the VC IP address as the source IP address for a TFTP session.

(Instant AP)# download-source vcip

In the above command, the user enters **vcip** as a string which gets substituted by the real VC IP address when executed.

This chapter describes the issues fixed in previous AOS-W Instant 6.4.4.x-4.2.4.x releases.

Issues Resolved in 6.4.4.8-4.2.4.4

AppRF

Table 10: *AppRF Fixed Issues*

Bug ID	Description
139336 138868	**Symptom**: Whatsapp traffic was not blocked by the OAW-IAP although the deny ACL was applied. The fix ensures that the blocked whatsapp traffic is not allowed by the OAW-IAP. **Scenario**: The WhatsApp traffic block was not functional as the latest version of WhatsApp was not classified as WhatsApp in the OAW-IAP. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.4.
141891 142278 141898	**Symptom**: Some OAW-IAPs in the cluster were unable to pass traffic. This issue is resolved by introducing a mechanism to monitor and limiting the AppRF process memory. **Scenario**: The memory utilization on the affected OAW-IAPs was very high. This issue was observed on all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.4.

CLI

Table 11: *CLI Fixed Issue*

Bug ID	Description
151137	**Symptom**: The CLI for anOAW-IAP205 access point crashed and began generating multiple core files. This issue is resolved by making a change to the function used in the OAW-IAP code. **Scenario**: This issue was observed in OAW-IAP205 access points running a software version prior to Instant 6.4.4.8-4.2.4.4.

Configuration

Table 12: *Configuration Fixed Issue*

Bug ID	Description
145050 149491 149515	**Symptom**: The syslog messages from the OAW-IAP indicated a configuration mismatch between the VC and the slave OAW-IAPs in a cluster. This issue is resolved by initiating the enet-vlan configuration when the OAW-IAP restarts. **Scenario**: This issue occurred when mesh point was configured on the OAW-IAP and enet-vlan configuration was removed from the master OAW-IAP. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.4.

Datapath/Firewall

Table 13: *Platform Fixed Issues*

Bug ID	Description
135764	**Symptom**: OAW-IAPs operating on Instant 6.4.3.4-4.2.1.2 crashed and rebooted with the reboot reason: **Reboot caused by kernel panic: assert.** The fix resolves the kernel panic issue. **Scenario**: This issue was observed in OAW-IAP205 access points running Instant 6.4.3.4-4.2.1.2 and later versions.
151748	**Symptom**: AnOAW-IAP crashed and rebooted unexpectedly. The log file for the event listed the reason as **Reboot caused by kernel panic: softlockup: hung tasks**. This fix ensures that the deadlock issue causing the crash is resolved. **Scenario**: This issue occurred due a deadlock caused by a recursive lock on the anul lock function running on the CPU. This issue was observed in OAW-IAP325 access points running a software version prior to Instant 6.4.4.8-4.2.4.4.

GRE

Table 14: *GRE Fixed Issue*

Bug ID	Description
151725 152539 152619	**Symptom**: OAW-IAP was using unfixed MTU than the specified MTU for GRE fragmentation. This resulted in packets fragmentated with a different size which may cause possible loss during the transmission. The fix ensures that the OAW-IAP uses the specified MTU value for GRE fragmentation. **Scenario**: This issue was observed in OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.4.

Platform

Table 15: *Platform Fixed Issue*

Bug ID	Description
146564 149935	**Symptom**: The LLDP process in anOAW-IAP was unable to negotiate high power, shut down the wrong Ethernet port, and did not enable the radios. The fix ensures that the LLDP process in anOAW-IAP works correctly when both Ethernet ports are used. **Scenario**: This issue occurred when both Ethernet ports of anOAW-IAP were in use and connected to PoE+ power sources (which are reliant on LLDP protocol to provide high power). This issue was observed in OAW-IAP325 access points running a software version prior to Instant 6.4.4.8-4.2.4.4.

Wi-Fi Driver

Table 16: *Wi-Fi Driver Fixed Issues*

Bug ID	Description
147682 147681	**Symptom**: A slave OAW-IAP incorrectly classified another OAW-IAP belonging to the same cluster as a rogue OAW-IAP. The fix ensures that the OAW-IAPs can correct the wrong entry in very short time. **Scenario**: This issue occurred as the slave OAW-IAP lost the messages of the updated MAC address list from the VC. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.4.
141429	**Symptom**: Access points crashed and rebooted. The log file for the event listed the reason as **Reboot caused by out of memory**. The fix ensures that the issue with the memory is resolved. **Scenario**: This issue was observed in all OAW-IAP2xx series access points running a software version prior to Instant 6.4.4.8-4.2.4.4.
145852 152810	**Symptom**: AOAW-IAP crashed 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 correctly. **Scenario**: This issue was observed in OAW-IAP325 access points running a software version prior to Instant 6.4.4.8-4.2.4.4.
150704	**Symptom**: OAW-IAP did not send all the interference SSID details to OmniVista. This issue is resolved by extending the maximum number of entries in the IDS table to 2048. **Scenario**: This issue occurred as the IDS table was full and was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.4.
151866	**Symptom**: Laptops running a Windows 7 64-bit OS were experiencing crashes when using Intel wireless chipset Dual Band Wireless-AC 7265 or Dual Band Wireless-AC 8260. This issue is resolved by setting the right value for the beacon interval. **Scenario**: This issue occurred as the default value of the beacon interval was altered and was observed in OAW-IAP325 access points running a software version prior to Instant 6.4.4.8-4.2.4.4.

Issues Resolved in 6.4.4.8-4.2.4.3

OmniVista

Table 17: *OmniVista Fixed Issue*

Bug ID	Description
150262	**Symptom**: Configuration changes made on the OAW-IAP through the CLI, UI, or AMP were not recorded in the syslog by default. The fix ensures that the syslog message is generated when the configuration is changed. **Scenario**: This issue occurred as the syslog level for a configuration was lower than the OAW-IAPs default syslog level. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.3.

Authentication

Table 18: *Authentication Fixed Issues*

Bug ID	Description
147169	**Symptom**: The RADIUS server rejected successive authentication requests from the OAW-IAP. The fix ensures that the RADIUS authentication requests are handled successfully. **Scenario**: This issue occurred due to duplicate RADIUS session IDs and was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.3.
148693	**Symptom**: The browser kept displaying a warning or an error claiming the securelogin.arubanetworks.com certificate had been revoked, causing disruption to the captive portal work flow of the OAW-IAP. As a fix to this issue, the securelogin.arubanetworks.com certificate has been replaced by a different certificate for which the browser may only have warnings and not errors. However, the best practice is for customers to upload their own publically signed certificate instead of relying on the default securelogin.arubanetworks.com certificate. **Scenario**: This issue impacted all scenarios where captive portal is used and was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.3.

Platform

Table 19: *Platform Fixed Issue*

Bug ID	Description
147826	**Symptom**: OAW-IAP325 access points crashed and rebooted with a reason: **Reboot caused by kernel panic: Fatal exception.** The fix ensures that the duplicate entries are not added to the subnet table. **Scenario**: This issue occurred due to duplicate entries in the subnet table and was observed in OAW-IAP325 access points running a software version prior to Instant 6.4.4.8-4.2.4.3.

VC Management

Table 20: *VC Management Fixed Issue*

Bug ID	Description
146606	**Symptom**: Some OAW-IAPs were intermittently getting disconnected from the cluster. The fix resolves the out of memory issue that caused the OAW-IAPs to disconnect from the cluster. **Scenario**: This issue occurred when a large amount of ARP frames were sent through the wired network and resulted in the datapath running out of memory space. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.3.

VPN

Table 21: *VPN Fixed Issue*

Bug ID	Description
144326 148161	**Symptom**: When one OAW-IAP used another OAW-IAP as an uplink, the OAW-IAP was unable to re-establish a VPN connection if its VPN session was SRC-NAT'ted at the uplink OAW-IAP. The fix ensures that the OAW-IAPs can successfully reconnect to the VPN. **Scenario**: This issue occurred as the old VPN session was still active on the uplink OAW-IAP and was observed in OAW-IAP324/325, OAW-IAP205/205H access points running a software version prior to Instant 6.4.4.8-4.2.4.3.

Wi-Fi Driver

Table 22: *Wi-Fi Driver Fixed Issues*

Bug ID	Description
147682	**Symptom**: A slave OAW-IAP incorrectly classified another OAW-IAP belonging to the same cluster as a rogue OAW-IAP. The fix ensures that the OAW-IAPs can correct the wrong entry in very short time. **Scenario**: This issue occurred as the slave OAW-IAP lost the messages of the updated MAC address list from the VC. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.3.
140337 141943 145917 146032	**Symptom**: AnOAW-IAP325 access point rebooted due to FW assert while running multicast traffic for a long period of time. This issue is resolved by improving the checking mechanism for the Tx buffer getting stuck. **Scenario**: This issue was observed in OAW-IAP325 access points running a software version prior to Instant 6.4.4.8-4.2.4.3.
141239 148412	**Symptom**: Motorola MC75A0 handheld scanners were unable to associate to OAW-IAP325 access points. This fix ensures that the Motorola MC75A0 handheld scanner is able to connect to the OAW-IAP325 access point. **Scenario**: This issue occurred when the client always sent a deauthentication message before sending the authentication message to the OAW-IAP. Also, the OAW-IAP sent a deauthentication message to the client after receiving an association request. This issue was observed in OAW-IAP325 access points running a software version prior to Instant 6.4.4.8-4.2.4.3.
138637	**Symptom**: Frames with VLAN 0 were dropped and not retransmitted over the air. The fix ensures that frames with VLAN ID 0 are not dropped. **Scenario**: This issue was observed in OAW-IAP275 access points running a software version prior to Instant 6.4.4.8-4.2.4.3.

Issues Resolved in 6.4.4.8-4.2.4.2

ALE

Table 23: *ALE Fixed Issue*

Bug ID	Description
145729	**Symptom**: The **Age** field in the RSSI client message was not accurate. The issue is resolved by changing the calculation logic of the field. **Scenario**: This issue affected deployments in which OAW-IAPs were being used in combination with the ALE server for location-based services, resulting in inaccurate location calculations of the ALE server. This issue was observed in all the OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.2.

CLI

Table 24: *CLI Fixed Issue*

Bug ID	Description
144944	**Symptom**: The VPN routing profile of an OAW-IAP accepted invalid entries during CLI configuration. The issue is resolved by running a check on the CLI parameters, so that the OAW-IAP displays an error message when the users enter invalid parameters. **Scenario**: This issue was observed when the IAP-VPN profile accepted values such as ASCII and special characters without displaying an error message in the CLI. This issue was not limited to a specific OAW-IAP model or Instant software version.

Datapath/Firewall

Table 25: *Datapath/Firewall Fixed Issues*

Bug ID	Description
139022	**Symptom**: OAW-IAPs crashed and rebooted while receiving certain multicast packets from the SSID profile. The fix ensures that OAW-IAPs do not crash while receiving the multicast packets. **Scenario**: This issue was found in OAW-IAPs with the Dynamic Multicast Optimization (DMO) feature enabled. This issue was observed in OAW-IAP325 access points running Instant 6.4.4.3-4.2.2.0 and later releases.
146155	**Symptom**: When the SSID, WLAN access rule, and user-defined Src-NAT rule were in use, the bandwidth control did not have any effect on the clients associated to slave OAW-IAPs. The issue is resolved by changing the bandwidth control logic of the OAW-IAPs. **Scenario**: This issue was observed in all the OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.2.

Platform

Table 26: *Platform Fixed Issue*

Bug ID	Description
145808 136228	**Symptom**: OAW-IAPs in a cluster rebooted as they were running out of memory. The fix ensures that OAW-IAPs use the memory space appropriately. **Scenario**: This issue was observed in OAW-IAP205 and OAW-IAP275 access points running a software version prior to Instant 6.4.4.8-4.2.4.2.

PPPoE

Table 27: *PPPoE Fixed Issue*

Bug ID	Description
140549	**Symptom**: PPPoE session was not working when the uplink port of anOAW-IAP was fluctuating. The fix ensures that PPPoE works even when there are multiple fluctuations at the uplink port of the OAW-IAP. **Scenario**: This issue was observed in all the OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.2.

Wi-Fi Driver

Table 28: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
132990	**Symptom**: Wireless services were unstable when the Ethernet port of the OAW-RAP109 access point was fluctuating. The fix ensures that clients receive stable wireless services from the OAW-RAP. **Scenario**: This issue was observed in OAW-RAP109 access points running a software version prior to Instant 6.4.4.8-4.2.4.2.

3G/4G Management

Table 29: *3G/4G Management Fixed Issue*

Bug ID	Description
142944	**Symptom**: A 320U 4G modem was not working when connected to anOAW-IAP. This issue is resolved by a change in condition to match the module name of the modem. **Scenario**: This issue was observed in 320U modems connected to OAW-RAP155 access points running a software version prior to Instant 6.4.4.8-4.2.4.2.

Issues Resolved in 6.4.4.8-4.2.4.1

OmniVista

Table 30: *OmniVista Fixed Issue*

Bug ID	Description
140313	**Symptom**: OmniVista managing OAW-IAPs did not display some of the interfering OAW-IAPs. The fix ensures that the interfering OAW-IAPs are displayed on OmniVista. **Scenario**: This issue occurred when a large number of interfering OAW-IAPs were present in the same physical area of the WLAN network. This issue was not limited to a specific OAW-IAP model or Instant software version.

AppRF

Table 31: *AppRF Fixed Issue*

Bug ID	Description
143257	**Symptom**: DPIMGR trace logging spiked memory usage on the OAW-IAP. This issue is resolved by moving the syslog message from error log to debug level. **Scenario**: This issue occurred when the brightcloud DNS resolve process started before trace logging of DPIMGR, which triggered default trace logging to grow and caused memory spike in OAW-IAPs running Instant 6.4.4.4-4.2.3.0 and later versions.

Datapath/Firewall

Table 32: *Datapath/Firewall Fixed Issues*

Bug ID	Description
138649	**Symptom**: OAW-IAP225 access points crashed and rebooted with the reason: **Reboot caused by kernel panic: Fatal exception in interrupt.** This issue is resolved by preventing the watchdog timer from getting triggered when the bridge entries are deleted. **Scenario**: The watchdog timer was triggered when the bridge entries were deleted. This issue was observed in OAW-IAP225 access points running a software version prior to Instant 6.4.4.8-4.2.4.1.
143390	**Symptom**: Clients connecting to OAW-RAP109 using a 3G or 4G uplink were unable to get an IP address from all Ethernet ports with enet0-bridging enabled. This issue is resolved by bringing up the br0 port when enet0-bridging is enabled. **Scenario**: The br0 port is down when enet0-bridging is enabled. This issue was observed in OAW-RAP109 access points running a software version prior to Instant 6.4.4.8-4.2.4.1.
144543	**Symptom**: Apple devices connected to the slave OAW-IAPs via the guest VLAN were intermittently losing connectivity to the network. The fix ensures that the Apple devices are able to connect to the network without intermittency issues. **Scenario**: This issue was observed in all OAW-IAPs running Instant 6.4.4.4-4.2.3.0 and later versions.

SNMP

Table 33: *SNMP Fixed Issue*

Bug ID	Description
140180	**Symptom**: The Object aiRadioStatus value was always 1 irrespective of the radio status. The fix ensures that the Object aiRadioStatus is 0 when the radio is disabled and 1 when the radio is enabled. However, when mesh is enabled on the OAW-IAP, the object aiRadioStatus will be 1 even when the radio is disabled. **Scenario**: This issue was not limited to a specific OAW-IAP model or Instant software version.

STM

Table 34: *STM Fixed Issue*

Bug ID	Description
136795	**Symptom**: STM core files were found in several OAW-IAPs as a result of the memory being cleared twice. This issue is resolved by preventing the memory from being cleared twice when the auth-server ip address is changed. **Scenario**: This issue occurred when multiple OAW-IAPs were used and DRP was enabled on the SSID profile. This issue was not limited to a specific OAW-IAP model or Instant software version.

UI

Table 35: *UI Fixed Issues*

Bug ID	Description
137227	**Symptom**: Users were getting an error message when they tried logging in to the OAW-IAP UI using Internet Explorer 11. The warning message has been removed to resolve this issue. **Scenario**: This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.1.
140803	**Symptom**: One of the ACL parameters was incorrectly displaying as **scanning activieren** instead of **scanning deaktivieren** in the German version of the OAW-IAP UI. **Scenario**: This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.1.

Wi-Fi Driver

Table 36: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
129829	**Symptom**: External wi-fi devices were intermittently not displayed in the IDS table after they were re-classified as valid. The fix ensures that the external wi-fi devices are displayed in the IDS table until the device entry expires. **Scenario**: This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.1.

Issues Resolved in 6.4.4.6-4.2.4.0

AirGroup

Table 37: *AirGroup Fixed Issue*

Bug ID	Description
139943	**Symptom**: AirPrint information was not getting displayed on the AirGroup server list of the OAW-IAP. This issue is resolved by a change in code that records the response sent to the OAW-IAP query. **Scenario**: This issue was observed in OAW-IAP205 devices running a software version prior to Instant 6.4.4.6-4.2.4.0.

OmniVista

Table 38: *OmniVista Fixed Issue*

Bug ID	Description
136986	**Symptom**: OAW-IAPs were sending the tx power and channel information to OmniVista ven when the 2.4 GHz and 5 GHz radios were disabled. The fix ensures the OAW-IAP does not report the tx power, radio channel, noise floor, and channel busy values to OmniVista when the radios are disabled. **Scenario**: This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.6-4.2.4.0.

ARM

Table 39: *ARM Fixed Issue*

Bug ID	Description
139165	**Symptom**: The 2.4 GHz channels were disabled in OAW-IAPs that support the Nigerian country code. The issue is resolved by removing the code that is used to validate DRT content of the OAW-IAP. **Scenario**: This issue was observed in OAW-IAP205 devices running a software version prior to Instant 6.4.4.6-4.2.4.0.

Datapath/Firewall

Table 40: *Datapath/Firewall Fixed Issues*

Bug ID	Description
138095	**Symptom**: After upgrading the software version from Instant 6.4.2.6-4.1.1.6 to 6.4.3.4-4.2.1.0, MAC users were experiencing delays in connecting to the network. The fix ensures that the users are able to connect to the newtork without delay. **Scenario**: This issue occurred as there was a delay in receiving the DHCP IP address from the server and was observed in all OAW-IAPs running Instant 6.4.3.4-4.2.1.0 and later versions.
136169	**Symptom**: Some clients were getting a higher bandwidth than the allocated limit. The fix ensures that the bandwidth does not exceed the allocated limit. **Scenario**: This issue occurred as the bandwidth contract for some of the OAW-IAPs in the cluster was not taking effect correctly. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.6-4.2.4.0.

Hotspot 2.0

Table 41: *Hotspot 2.0 Fixed Issues*

Bug ID	Description
139116	**Symptom**: OAW-IAPs failed to send 3GPP-PLMN values in the ANQP response frame. The fix ensures that correct values for the 3GPP-PLMN element are sent by the OAW-IAP. **Scenario**: This issue was observed in OAW-IAP205H access points running Instant 6.4.4.4-4.2.3.0 and later versions.
138670	**Symptom**: Clients failed to automatically connect to OAW-IAPs even after the hotspot feature was configured in the OAW-IAPs. The fix ensures that an automatic connection between the hotspot clients and OAW-IAPs is successful. **Scenario**: This issue occurred as the OAW-IAPs were not adding hotspot information elements into the beacon.. This issue was observed in OAW-IAPs running Instant 6.4.3.4-4.2.1.0 and later versions.

L2/L3 Mobility

Table 42: *L2/L3 Mobility Fixed Issue*

Bug ID	Description
137726	**Symptom**: Clients were unable to pass traffic after successfully roaming from one OAW-IAP to another in the cluster. This issue is resolved by making a change in the code to use the client information in the user path when programming the user entry for the home OAW-IAP. **Scenario**: This issue occurred as the user entry was cleared from the home OAW-IAP when the client roamed from one OAW-IAP to another in the network and was not limited to a specific OAW-IAP model or software version.

Platform

Table 43: *Platform Fixed Issues*

Bug ID	Description
140867	**Symptom**: When clients upgraded anOAW-IAP, the RTLS server displayed an error message. This issue is resolved by enabling the server compatibility settings of the RTLS server. **Scenario**: This issue was observed in OAW-IAP103 access points running a software version prior to Instant 6.4.4.6-4.2.4.0.
142400	**Symptom**: OAW-IAPs were continuously crashing every 2 to 3 minutes, causing productivity issues with the clients. This issue is resolved by introducing a mechanism to lock the bridge entry of the OAW-IAP. **Scenario**: This issue occurred due to a kernel panic in the OAW-IAP code, resulting in continuous rebooting of the OAW-IAPs. This issue was observed in OAW-IAP325 access points running Instant 6.4.4.4-4.2.3.0 and later versions.
135787	**Symptom**: When a multicast server tried to send a file to the client through an OAW-IAP, the client failed to receive the entire file. This issue is resolved by applying a condition to verify the DHCP/DNS packets. **Scenario**: This issue occurred when the OAW-IAPs dropped a section of the fragmented packets during file transfer. This issue was observed in OAW-IAPs running a software version prior to Instant 6.4.4.6-4.2.4.0.
137637	**Symptom**: OAW-IAP225 devices crashed and rebooted with a response: Reboot caused by Kernel panic: asset. This issue is resolved by removing the L3 mobility tunnel creation for the CL2 VLAN. **Scenario**: This issue occurred as the memory space was low and was observed in all OAW-IAP running a software version prior to Instant 6.4.4.6-4.2.4.0.

3G/4G Management

Table 44: *3G/4G Management Fixed Issue*

Bug ID	Description
137180	**Symptom**: Clients using Windows laptops and mobile devices were unable to access certain websites while being connected to an OAW-IAP. The issue is resolved by checking and updating the MSS value of the TCP packets that are received from the OAW-IAP. **Scenario**: This issue was observed in all OAW-IAPs running Instant 6.4.3.1-4.2.0.0 and later versions.

UI

Table 45: *UI Fixed Issues*

Bug ID	Description
140506	**Symptom**: The following error was displayed when the user tried to create a periodic time-based service profile using a certain condition: **End day must be later than start day**. This issue is resolved by changing the code for validating when a time-based service profile is created. **Scenario**: This issue was observed in all OAW-IAPs running Instant 6.4.4.4-4.2.3.1 and later versions.
141593	**Symptom**: The column under the **RF Dashboard** that displays the signal strength of the OAW-IAP clients was missing in the Instant UI. The fix ensures that the signal strength of the clients is displayed in the UI. **Scenario**: This issue was observed in all OAW-IAPs running Instant 6.4.4.4-4.2.3.0.
141757	**Symptom**: OAW-IAP clients were still active even after they were manually disconnected using the Instant UI. The fix ensures that the manual disconnect of clients using the UI is successful. **Scenario**: This issue occurred as the information and the status of the client was not erased when the disconnect operation was performed using the UI. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.6-4.2.4.0.

VC Management

Table 46: *VC Management Fixed Issue*

Bug ID	Description
138089	**Symptom**: OAW-IAPs were experiencing a delay in establishing a connection with the SSH server when the reverse dns lookup failed. This issue is resolved by preventing the SSH server from performing a reverse dns lookup, to avoid the delay prior to establishing a connection with the OAW-IAP. **Scenario**: The issue occurred due to multiple retry attempts by the SSH server to perform a reverse dns lookup before establishing a connection with the OAW-IAP. This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.6-4.2.4.0.

VPN

Table 47: *VPN Fixed Issues*

Bug ID	Description
132490	**Symptom**: In a Distributed L3 network, windows clients were unable to open a few sites when connected to the wired network of the OAW-IAP. This issue is resolved by enabling MSS clamping in the upstream direction. **Scenario**: The issue occurred as the MSS clamping was enabled only in the downstream direction for the Distributed L3 clients. This issue was not limited to a specific OAW-IAP model or software version.
138468	**Symptom**: OAW-IAP clients were unable to connect to the corporate network. This issue is resolved by ensuring that the master OAW-IAPs receive the correct DHCP IP subnets from the VPN tunnel in the corporate network. **Scenario**: The issue was observed in all OAW-IAPs running Instant 6.4.3.4-4.2.1.0 and later versions.

Wi-Fi Driver

Table 48: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
138582	**Symptom**: Clients were unable to connect to the 5 GHZ radio channel and the error logs revealed there were TX Radio and Antenna probe failures. The fix enures the clients are now able to connect to the 5 GHz radio channel without errors. **Scenario**: This issue was observed in all OAW-IAPs running a software version prior to Instant 6.4.4.6-4.2.4.0.

Appendix A
Acronyms and Abbreviations

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

Table 49: *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
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

Table 49: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 49: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
CoA	Change of Authorization
CoS	Class of Service
CPE	Customer Premises Equipment
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
DFT	Discreet Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMO	Dynamic Multicast optimization
DN	Distinguished Name

Table 49: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 49: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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
GRE	Generic Routing Encapsulation

Table 49: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 49: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 49: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
mDNS	Multicast Domain Name System
MFA	Multi-factor Authentication
MHz	Megahertz
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
NetBIOS	Network Basic Input/Output System
NIC	Network Interface Card
Nmap	Network Mapper
NMI	Non-Maskable Interrupt
NMS	Network Management Server

Table 49: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 49: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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
RSA	Rivest, Shamir, Adleman

Table 49: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 49: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SMB	Small and Medium Business
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SNIR	Signal-to-Noise-Plus-Interference Ratio
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SoC	System on a Chip
SoH	Statement of Health
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

Table 49: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
TLS	Transport Layer Security
TLV	Type-length-value
ToS	Type of Service
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
VBN	Virtual Branch Networking
VBR	Virtual Beacon Report
VHT	Very High Throughput
VIA	Virtual Intranet Access
VIP	Virtual IP Address

Table 49: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over IP
VoWLAN	Voice over Wireless Local Area Network
VPN	Virtual Private Network
VRD	Validated Reference Design
VRF	Visual RF
VRRP	Virtual Router Redundancy Protocol
VSA	Vendor-Specific Attributes
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WebUI	Web browser User Interface
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
WIDS	Wireless Intrusion Detection System
WINS	Windows Internet Naming Service
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

Table 49: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
XAuth	Extended Authentication
XML	Extensible Markup Language
XML-RPC	XML Remote Procedure Call
ZTP	Zero Touch Provisioning