AOS-W Instant 6.5.0.3-4.3.0.3

Release Notes

AOS-W Instant 6.5.0.3-4.3.0.3 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 6.5.0.0-4.3.0.0 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, features, enhancements, fixed issues, known issues and limitations in the AOS-W Instant 6.5.0.3-4.3.0.3 release.

Important Updates

End of Support for Legacy 802.11n Instant Access Points

Starting from Instant 6.5.0.0-4.3.0.0, the following 802.11n OAW-IAPs are not supported:

- OAW-IAP104 and OAW-IAP105
- OAW-RAP3WN and OAW-RAP3WNP
- OAW-IAP134 and OAW-IAP135
- OAW-IAP175P/175AC

Regulatory Domain Updates

The following table lists the DRT file versions supported by Instant 6.5.0.3-4.3.0.3 release:

Table 2: *DRT Versions*

Instant Release Version	Applicable DRT Version
6.5.0.3-4.3.0.3	1.0_58258
6.5.0.0-4.3.0.2	1.0_57440
6.5.0.0-4.3.0.1	1.0_57023
6.5.0.0-4.3.0.0	1.0_56308

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

Resolved Issues in this Release

The following issues are fixed in the Instant 6.5.0.3-4.3.0.3 release.

AppRF

Table 3: *AppRF Fixed Issue*

Bug ID	Description
147333	**Symptom**: Clients were able to download files through different torrent clients even though the App category deny ACL is configured on the SSIDs. The fix ensures that the torrent clients are inaccessible when the App deny ACLs are configured on the SSID. **Scenario**: This issue was observed in OAW-IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.

Captive Portal

Table 4: *Captive Portal Fixed Issue*

Bug ID	Description
148645	**Symptom**: The Captive Portal assistance page did not pop up automatically for Samsung devices. This issue is resolved by adding a space in the status line of the http response header. **Scenario**: This issue was observed in OAW-IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.

Configuration

Table 5: *Configuration Fixed Issues*

Bug ID	Description
145050 149491 149515	**Symptom**: The syslog messages from the 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 OAW-IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.

Datapath/Firewall

Table 6: *Datapath/Firewall Fixed Issues*

Bug ID	Description
145296	**Symptom**: Traffic to a Captive Portal client did not stop even after manually disconnecting it or by using CoA. The fix ensures that the traffic is stopped when the client is disconnected. **Scenario**: This issue was observed in OAW-IAP103 and OAW-IAP275 access points running a software version prior to Instant 6.5.0.3-4.3.0.3.
146666	**Symptom**: Slave OAW-IAPs connecting to a guest networks were unable to pass traffic. This issue is resolved by programming an ACL for the guest vlan to allow slave OAW-IAPs to successfully connect to the guest network. **Scenario**: This issue was observed in OAW-IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.
152421	**Symptom**: Some OAW-IAPs failed to obtain a private IP address during factory bootup as there was no external DHCP server in the uplink. As a result, the Web UI was unable to access the wireless clients connected to the Instant SSID. The fix ensures that the OAW-IAPs are able to otain a private IP address and the Web UI is able to connect to the wireless clients on the Instant SSID. **Scenario**: This issue was observed in OAW-IAP204/205, OAW-IAP314/315, OAW-IAP324/325 platforms running a software version prior to Instant 6.5.0.3-4.3.0.3.
151748	**Symptom**: An OAW-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 6.5.0.3-4.3.0.3.
154522	**Symptom**: Clients connected to the master OAW-IAP were unable to resolve the DNS SRV record queries. This issue is resolved by disabling the DNS proxy when Local, L2 is configured as the DHCP scope. **Scenario**: This issue was observed in OAW-IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.
155539	**Symptom**: Clients were losing packets intermittently. This issue is resolved by stopping the OAW-IAP from carrying out the pending session delete operation. **Scenario**: This issue occurred as the datapath user session count was continously increasing and was not getting aged out or reset. This issue was observed in OAW-IAPs running a software version prior to Instant 6.5.0.3.-4.3.0.3.
156718	**Symptom**: An OAW-IAP access point crashed after deny-inter-user-bridging was configured. This issue is resolved by running a check for valid destination. **Scenario**: This issue occurred when the p->gress is assigned to an incorrect VLAN. This issue was observed in OAW-IAPs running a software version prior to Instant 6.4.4.8-4.2.4.6.

GRE

Table 7: *GRE Fixed Issue*

Bug ID	Description
151725	**Symptom**: OAW-IAP was using unfixed MTU than the specified MTU for GRE fragmentation. This resulted in packets fragmented 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 6.5.0.3-4.3.0.3.

Hotspot 2.0

Table 8: *Hotspot 2.0 Fixed Issue*

Bug ID	Description
153024	**Symptom**: NAI realm list ANQP response contains EAP-AKA prime instead of EAP-AKA when configured with EAP-AKA. The fix ensures that expected response is obtained from the OAW-IAP. **Scenario**: This issue was observed in OAW-IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.

IPv6

Table 9: *IPv6 Fixed Issue*

Bug ID	Description
154827	**Symptom**: OAW-IAP200 series access points crashed due to kernel panic. The fix ensures that the OAW-IAP does not crash and reboot due to kernel panic. **Scenario**: This issue occurred when multiple IPv4 and IPv6 DNS mobility messages were sent by the OAW-IAP. This issue was observed in OAW-IAP200 series access points running a software version prior to Instant 6.5.0.3-4.3.0.3.

Other

Table 10: *Other Fixed Issue*

Bug ID	Description
152060	**Symptom**: OAW-IAP was using unfixed MTU than the specified MTU for GRE fragmentation. This resulted in packets fragmented 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 6.5.0.3-4.3.0.3.

Platform

Table 11: *Platform Fixed Issues*

Bug ID	Description
135764	**Symptom**: Some OAW-IAPs crashed and rebooted with the reason: **Reboot caused by kernel panic: assert. The fix resolves the kernel panic issue.** The fix resolves the kernel panic issue. **Scenario**: : This issue was observed in OAW-IAP205 access points running a software version prior to Instant 6.5.0.3-4.3.0.3.
152825	**Symptom**: Some OAW-IAPs crashed and rebooted with the reason: **Reboot caused by kernel panic: assert. The fix resolves the kernel panic issue.** The fix resolves the kernel panic issue. **Scenario**: : This issue was observed in OAW-IAP205 access points running a software version prior to Instant 6.5.0.3-4.3.0.3.
154738	**Symptom**: Some OAW-IAPs were encountering bitflip memory corruption. The fix ensures that the bitflip memory corruption issue is resolved. **Scenario**: : This issue occurred as the OAW-IAPs were using old SBL2 firmware. This issue was observed in OAW-IAP315 access points running a software version prior to Instant 6.5.0.3.-4.3.0.3.

SNMP

Table 12: *SNMP Fixed Issue*

Bug ID	Description
155081	**Symptom**: The **SNMP** process displayed an error - **OID not increasing**, when clients had a MAC address ending with **FF**. The fix ensures that the packets of clients having MAC address ending with FF are forwarded to the next node. **Scenario**: This issue occurred when the **SNMP** process used MAC address plus 1 and VLAN to search for the node. When the client had a MAC address ending with FF, the **SNMP** process used the MAC address ending with FF and VLAN to search for the next node, which resulted in an infinite loop. This issue was observed in OAW-IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.

UI

Table 13: *UI Fixed Issue*

Bug ID	Description
155081	**Symptom**: The response for the XML API query did not provde the correct XML API statistics. The fix ensures that the XMI API statics are periodically updated and the response to the XML API query provides the correct information. **Scenario**: This issue was observed in OAW-IAP205H access points running Instant 6.5.0.0-4.3.0.0 or later versions.

VPN

Table 14: *VPN Fixed Issues*

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 6.5.0.3-4.3.0.3.
156175	**Symptom**: There was an issue executing CLI commands that generate large outputs, when the VC was accessed using the VPN IP address. This issue is resolved by adding a check to update the MSS file when the OAW-IAP receives TCP sync packets from the client behind the VPN. **Scenario**: This issue was observed in OAW-IAPs running Instant 6.5.0.0-4.3.0.0 release or later versions.

Wi-Fi Driver

Table 15: *Wi-fi Driver Fixed Issues*

Bug ID	Description
118039 156391	**Symptom**: An OAW-IAP275 access point rebooted due to an out of memory issue. The fix ensures that the MAC returns to normal functionality when it goes into the suspended state. **Scenario**: The issue occurred when the radio channel was changed and the MAC was pushed to a suspended state for a short duration. This issue was observed in OAW-IAP275 access points running a software version prior to Instant 6.5.0.3-4.3.0.3.
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 6.5.0.3-4.3.0.3.
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 6.5.0.3-4.3.0.3.
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 6.5.0.3-4.3.0.3.
154237	**Symptom**: An OAW-IAP crashed and rebooted unexpectedly. The fix ensures that the OAW-IAP does not crash due to kernel panic. **Scenario**: This issue occurred as the OAW-IAP experienced a kernel panic due to softlockup hung tasks. This issue was observed in OAW-IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.
154370	**Symptom**: Motorola handheld scanners connected to OAW-IAP325 access points were getting disconnected every 10 seconds. This issue is resolved by making a change to the default CCA threshold value. **Scenario**:This issue was observed in OAW-IAP325 access points running a software version prior to Instant 6.5.0.3-4.3.0.3.

This chapter lists the known issues and limitations identified in the Instant 6.5.0.x-4.3.0.x releases.

Known Issues

The following known issues are identified in the Instant 6.5.0.x-4.3.0.x releases:

AppRF

Table 16: *AppRF Known Issue*

Bug ID	Description
147333	**Symptom**: Clients are able to download files through different torrent clients even when App deny ACLs are configured on the SSIDs. **Scenario**: This issue is observed in all OAW-IAPs running Instant 6.4.4.6-4.2.4.0 and later versions. **Workaround**: None.

Datapath/Firewall

Table 17: *Datapath/Firewall Known Issue*

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. **Scenario**: This issue is observed in OAW-IAP205 and OAW-IAP325 access points running Instant 6.4.3.4-4.2.1.2 and later versions. **Workaround**: None.
148017	**Symptom**: Media classification does not happen for Skype for Business calls during L2 roaming. **Scenario**: This issue occurs rarely when there are packets lost on a wired network during client roaming, resulting in loss of media classified information. This issue is observed in all the OAW-IAPs running Instant 6.5.0.0-4.3.0.0 and later versions. **Workaround**: None.

SNMP

Table 18: *SNMP Known Issue*

Bug ID	Description
145365	**Symptom**: SNMP trap generation for voice call tracking is inconsistent when the VoIP client roams multiple times between OAW-IAPs in the cluster. **Scenario**: This issue is observed in all OAW-IAPs running Instant 6.5.0.0-4.3.0.0 and later versions. **Workaround**: None.

VC Management

Table 19: *VC Management Known Issue*

Bug ID	Description
145903	**Symptom**: The OAW-IAP VC speed-test result displays the upstream and the downstream bandwidths in bytes per second (Bps) instead of Megabytes per second (MBps). **Scenario**: This issue is observed in all the OAW-IAPs running Instant 6.5.0.0-4.3.0.0 and later versions. **Workaround**: None.

VPN

Table 20: *VPN Known Issue*

Bug ID	Description
147016	**Symptom**: Aruba-GRE VPN tunnel shows down in the OAW-IAP table and the GRE tunnel entry is missing from the datapath tunnel table. **Scenario**: This issue is observed in all the OAW-IAPs running Instant 6.5.0.0-4.3.0.0 and later versions. **Workaround**: None.

Limitations

The following limitation is identified in the Instant 6.5.0.0-4.3.0.0 release:

ARM Quick Channel Selection

Starting from Instant 6.5.0.0-4.3.0.0, OAW-IAPs can search for new environments triggering the ARM profile to perform frequent scanning of valid channels, if the following conditions are met:

- The OAW-IAP must work on stand-alone mode.
- The client-aware setting must be disabled in the ARM profile.
- All DFS channels must be removed.

This chapter describes the features and enhancements introduced in previous AOS-W Instant 6.5.x.x-4.3.x.x releases.

Features and Enhancements

This section describes the features and enhancements introduced in Instant 6.5.x.x-4.3.x.x releases.

Support for New OAW-IAP Devices

OAW-IAP310 Series

The OAW-IAP310 Series (OAW-IAP314/315) wireless access points support IEEE 802.11ac standards for high-performance WLAN, and are equipped with two single-band radios, which can provide network access and monitor the network simultaneously. Multi-User Multiple-In Multiple-Output (MU-MIMO) technology allows these access points to deliver high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a/b/g wireless services.

The OAW-IAP310 Series wireless access points provide the following capabilities:

- IEEE 802.11a/b/g/n/ac wireless access point
- IEEE 802.11a/b/g/n/ac wireless air monitor
- IEEE 802.11a/b/g/n/ac spectrum analysis
- Compatible with IEEE 802.3at PoE and 802.3af PoE
- Support for MCS8 and MCS9
- Centralized management, configuration and upgrades
- Integrated Bluetooth Low Energy (BLE) radio

OAW-IAP330 Series

The OAW-IAP330 Series (OAW-IAP334/335) wireless access points support IEEE 802.11ac standards for high-performance WLAN, and are equipped with two dual-band radios, which can provide network access and monitor the network simultaneously. MU-MIMO technology allows these access points to deliver high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a/b/g wireless services.

The OAW-IAP330 wireless access points provide the following capabilities:

- IEEE 802.11a/b/g/n/ac wireless access point
- IEEE 802.11a/b/g/n/ac wireless air monitor
- IEEE 802.11a/b/g/n/ac spectrum analysis
- Compatible with IEEE 802.3at PoE and 802.3af PoE
- Centralized management, configuration and upgrades
- Integrated BLE radio

Support for High Multicast Rate on WLAN SSID Profiles

Starting from Instant 6.5.0.0-4.3.0.0, a new parameter called **multicast-rate** has been introduced in the Instant CLI. This parameter increases the video transmission rate of the OAW-IAP. You can also set the MCS rates for greater OAW-IAP throughput. For more information, see:

- **wlan ssid-profile** command in *Aruba Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*

Configuring Trusted Ports on anOAW-IAP

Starting from Instant 6.5.0.0-4.3.0.0, the enhancements, **Port type** and **trusted** are made in the Instant UI and the CLI, respectively. These parameters support the trusted ports in anOAW-IAP.

A predefined ACL is applied to the trusted ports in order to control client traffic that needs to be src-NATed. For more information, see:

- *Wired Profiles* in *Aruba Instant 6.5.0.0-4.3.0.0 User Guide*
- **wired-port-profile** and **show wired-port-settings** commands in *Aruba Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*

ARM Quick Channel Selection

Starting from Instant 6.5.0.0-4.3.0.0, a new command, **ap-frequent-scan** is introduced to allow the OAW-IAPs to search for a new environment in a short span of time, triggering the radio profile to perform frequent scanning of transmission signals. The radio profile selects a valid channel once the scanning is completed.

The following checks must be performed before frequent scanning of the transmission channels is performed:

- The OAW-IAP must work on stand-alone mode.
- The client-aware setting must be disabled in the ARM profile.
- All DFS channels must be removed.

For more information, see:

- *Adaptive Radio Management* in *Aruba Instant 6.5.0.0-4.3.0.0 User Guide*
- **ap-frequent-scan** and **show ap debug am-config** commands in *Aruba Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*

New Option Added for Broadcast Filtering

A new option called **Unicast-ARP-Only** has been added to broadcast filtering. This option converts the ARP requests to unicast frames and sends them directly to the associated clients. For more information, see:

- *Configuring WLAN Settings for an SSID profile* in *AOS-W Instant 6.5.0.0-4.3.0.0 User Guide*
- **wlan ssid-profile** command page in *AOS-W Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*

Media Classification for Voice and Video

Starting from Instant 6.5.0.0-4.3.0.0, OAW-IAPs support media classification for Skype for Business and other applications such as Apple Facetime and Jabber. There are two types of media classification techniques for prioritizing voice and video calls. You can use an ACL with the classify-media option enabled in the WLAN configuration setting for an SSID or use the STUN method where the classify-media flag and the ACE need not be explicitly configured. For more information, see:

- *Media Classification for Skype for Business* and *STUN Based Media Classification* sections in *AOS-W Instant 6.5.0.0-4.3.0.0 User Guide*
- **show datapath session ucc** command in *AOS-W Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*.

Enabling Enhanced Voice Call Tracking

Starting from AOS-W Instant 6.5.0.0-4.3.0.0, OAW-IAP provides seamless support for tracking VoIP calls in the Aruba network by interoperating with third-party SNMP servers. An SNMP trap is generated in the following scenarios:

- VoIP calls made from SKype for Business and other applications, and

- The voice or video client is moving from one OAW-IAP to another in the network during an active call.

In order to find the location of a particular emergency caller, the third-party server can send a query to Master OAW-IAP using SNMP GET. The Master OAW-IAP responds back to the third-party server with the location of the VoIP caller.

Redirect Blocked HTTS Websites to a Custom Error Page

Starting from Instant 6.5.0.0-4.3.0.0, you can configure a new rule to redirected blocked https traffic to a custom error page. For more information, see:

- *Configuring ACL Rules to Redirect Blocked HTTPS Websites to a Custom Blocked Page URL* in *AOS-W Instant 6.5.0.0-4.3.0.0 User Guide*
- **wlan access-rule** command in *Aruba Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*

Enhancement to Modify Calling-Station-ID and Called-Station-ID Values

Starting from AOS-W Instant 6.5.0.0-4.3.0.0, users are allowed to modify the values set for the Calling-Station-ID and Called-Station-ID parameters in the wlan ssid-profile configuration using the OAW-IAP CLI. For more information, see:

- **wlan ssid-profile** command in *Aruba Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*

USB Modem Support for Newly Introduced Platforms

The OAW-IAP324/325, OAW-IAP314/315, OAW-IAP334/335 platforms can now be used with external USB modems.

User Limit for Per-AP Radio Profiles

Starting from Instant 6.5.3.0.0-4.3.0.0, the maximum clients configuration can be set indiviually for an SSID radio profile, using the OAW-IAP CLI. For more information, see:

- *Configuring Maximum Clients on SSID Radio Profiles* in *AOS-W Instant 6.5.0.0-4.3.0.0 User Guide*.
- **a-max-clients**, **g-max-clients**, **show a-max-clients**, **show g-max-clients** commands in *Aruba Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*.

Client Match Support for Newly Introduced Platforms

Starting from Instant 6.5.0.0-4.3.0.0, Client Match is supported on OAW-IAP334/335 and OAW-IAP314/315 access points. For information on configuring client match on OAW-IAPs, see:

- *Adaptive Radio Management* in *AOS-W Instant 6.5.0.0-4.3.0.0 User Guide*.
- **arm** command in *Aruba Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*.

Hashing of Management User Password

Starting from Instant 6.5.0.0-4.3.0.0, an optional setting is introduced in the Instant UI and the CLI where the management user passwords can be stored and displayed in hash format. Hashed passwords are more secure as they cannot be reversed. For more information, see:

- *Hashing of Management User Password* in *AOS-W Instant 6.5.0.0-4.3.0.0 User Guide*.
- **hash-mgmt-user**, **hash-mgmt-password**, and **show mgmt-user** commands in *Aruba Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*.

UI support for Enet-VLAN Setting

Starting from Instant 6.5.0.0-4.3.0.0, a new parameter **Uplink switch native VLAN** is introduced in the InstantUI. The CLI setting for this feature is already available through the **enet-vlan** command.

The newly introduced Instant UI parameter restricts the OAW-IAP from sending out tagged frames to clients connected on an SSID with the same VLAN as the native VLAN of the upstream switch, to which the OAW-IAP is connected. For more information, see:

- *Configuring System Parameters* in *AOS-W Instant 6.5.0.0-4.3.0.0 User Guide*.

Banner and Loginsession Configuration using CLI

Starting from Instant 6.5.0.0-4.3.0.0, the commands, **banner** and **loginsession** are introduced in the Instant CLI.

Users on a management session can view the text banner displayed at the login prompt of the OAW-IAP. The management session can also be configured to remain active without any user activity. For more information, see:

- *Banner and Loginsession Configuration using CLI* in *AOS-W Instant 6.5.0.0-4.3.0.0 User Guide*.
- **banner** , **show banner**, and **loginsession** commands in *Aruba Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*.

Temporal diversity and retries using CLI

Starting from Instant 6.5.0.0-4.3.0.0, the parameters **temporal-diversity** and **max-retries** are introduced in the Instant CLI. OAW-IAPs can perform and manage software retry attempts when clients are not responding to 802.11 packets. For more information, see:

- *Temporal Diversity and Maximum Retries using CLI* in *AOS-W Instant 6.5.0.0-4.3.0.0 User Guide*.
- **wlan ssid-profile** command in *Aruba Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*.

Enhancements to Image Upgrade and Image Sync Operations

Starting from Instant 6.5.0.0-4.3.0.0, the following enahcements have been made to the OAW-IAP image upgrade and image sync processes:

- If an automatic image upgrade fails, rebooting the OAW-IAP cluster is no longer required to proceed with the next image upgrade attempt.
- Previously, all the OAW-IAPs in the cluster were required to download the image from external server. Starting from this release, only OAW-IAP from each image class is required to download the image from the external server. This method helps in minimizing the network bandwidth used for the image download.
- When a new slave OAW-IAP joins a cluster:
  - If the cluster already contains the same image class of OAW-IAPs as the new slave OAW-IAP, the new slave OAW-IAP does not have to download the image from the external server. The newly added slave OAW-IAP will perform an image sync with an existing slave OAW-IAP of the same class.
  - If the cluster does not contain the same image class of OAW-IAPs as the new slave OAW-IAP, the new slave OAW-IAP has to download the image from the external server.
- If the new slave OAW-IAP joining the cluster is unable to download the image from an AMP server located behind the VPN tunnel, the master OAW-IAP will create a proxy request for the download and ensures the image sync is done successfully.

You can use the show swarm image-sync command to view the list of OAW-IAPs of the same class in the cluster

Support for IPv6

Instant 6.5.0.0-4.3.0.0 introduces support for IPv6 and enables the OAW-IAP to access control capabilities to clients, firewall enhancements, management of OAW-IAPs through a static IPv6 address, and support for IPv6 RADIUS server. For more information, see:

- *IPv6 Support* in *AOS-W Instant 6.5.0.0-4.3.0.0 User Guide*.
- **ip-mode**, **virtual-controller-ipv6**, **show ipv6 interface**, and **show ipv6 route** commands in *Aruba Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*.

Management Frame Protection

Instant 6.5.0.0-4.3.0.0 introduces support for MFP, an IEEE 802.11w standard that increases security by providing data confidentiality of management frames. For more information, see:

- *Management Frame Protection* in *AOS-W Instant 6.5.0.0-4.3.0.0 User Guide*.
- **wlan ssid-profile** command in *Aruba Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*.

Wildcard Server Certificate Support for Captive Portal

Instant 6.5.0.0-4.3.0.0 now supports the wildcard server certificate for captive portal authentication.

This chapter describes the issues fixed in previous AOS-W Instant 6.5.x.x-4.3.x.x releases.

Issues Resolved in 6.5.0.0-4.3.0.2

Captive Portal

Table 21: *Captive Portal Fixed Issue*

Bug ID	Description
151119	**Symptom**: Clients are stuck on the Captive Portal authentication page, when they try to use external captive portal over HTTP. The fix ensures that the captive portal authentication is successful. **Scenario**: This issue was observed in OAW-IAPs running Instant 6.5.0.0-4.3.0.0 release and later versions.

Datapath/Firewall

Table 22: *Datapath/Firewall Fixed Issues*

Bug ID	Description
146942	**Symptom**: The custom DSCP values set for the voice and video traffic was not applied and instead the default value of 48 and 40 was taking effect. The fix involves the following actions: • On the server side the ports for voice and video must be clearly defined to a specific subset. • On the OAW-IAP side, user must open up the voice and video UDP ports and assign the custom DSCP values using the ACL in the SSID configuration, in addition to the classify media ACL for the control session. **Scenario**: This issue was observed in OAW-IAPs running Instant 6.5.0.0-4.3.0.0 and later releases.
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 6.5.0.0-4.3.0.2.

Mesh

Table 23: *Mesh Fixed Issue*

Bug ID	Description
145637	**Symptom**: OAW-IAP225 access point was running into a network loop when the uplink for the mesh point was restored. 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 6.5.0.0-4.3.0.2.

Platform

Table 24: *Platform Fixed Issues*

Bug ID	Description
145634 150907	**Symptom**: AnOAW-IAP crashed unexpectedly when using a10Mbps 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 as expected. **Scenario**: This issue was observed in OAW-IAP215 and OAW-IAP225 access points running a software version prior to Instant 6.5.0.0-4.3.0.2.
152840 153318	**Symptom**: AnOAW-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 6.5.0.0-4.3.0.2.

Wi-Fi Driver

Table 25: *Wi-fi Driver Fixed Issue*

Bug ID	Description
151995	**Symptom**: AnOAW-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 6.5.0.0-4.3.0.2.

Issues Resolved in 6.5.0.0-4.3.0.1

OmniVista

Table 26: *OmniVista Fixed Issue*

Bug ID	Description
145304	**Symptom**: Whenever the OAW-IAP rebooted, an Instant SSID was broadcasted, although the user did not configure any SSIDs on the OAW-IAP. This issue is resolved by adding a function to stop the SSIDs from being automatically created when the OAW-IAP reboots. **Scenario**: This issue was observed on all OAW-IAPs running a software version prior to Instant 6.5.0.0-4.3.0.1.

Authentication

Table 27: *Authentication Fixed Issues*

Bug ID	Description
148759	**Symptom**: OAW-IAP did not fall back to the local authentication when the TACACS shared key for management authentication was incorrect. This issue is resolved by enabling the fall back feature on the IAP when the TACACS shared key is incorrect or the management authentication fails. **Scenario**: This issue was not limited to a specific OAW-IAP model or Instant software version.
149532	**Symptom**: Dynamic domain names were not supported by the Facebook feature for customized certificates uploaded on the server. As a fix, the dynamic domain name is input to the url for customized certificates. **Scenario**: This issue was observed in all OAW-IAPs running a software version prior to Instant 6.5.0.0-4.3.0.1.

CLI

Table 28: *CLI Fixed Issue*

Bug ID	Description
151137	**Symptom**: The CLI for an OAW-IAP205 access point crashed and began generating multiple core files. This issue is resolved by making a change to the function used in the IAP code. **Scenario**: This issue was observed in OAW-IAP205 access points running a software version prior to Instant 6.5.0.0-4.3.0.1.

Platform

Table 29: *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 6.5.0.0-4.3.0.1.

VC Management

Table 30: *VC Management Fixed Issue*

Bug ID	Description
147826	**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 6.5.0.0-4.3.0.1.

Wi-Fi Driver

Table 31: *Wi-fi Driver Fixed Issue*

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 6.5.0.0-4.3.0.1.

Issues Resolved in 6.5.0.0-4.3.0.0

AppRF

Table 32: *AppRF Fixed Issue*

Bug ID	Description
120228	**Symptom**: Skype application was not getting blocked when the App enforcement ACL was configured. The issue is resolved by upgrading the App protocol bundle version in the OAW-IAP. **Scenario**: This issue was observed in all the OAW-IAPs running a software version prior to Instant 6.5.0.0-4.3.0.0.
142278 141891	**Symptom**: Some OAW-IAPs in the cluster were unable to pass traffic. This issue is resolved by adding a mechanism to monitor and limit the AppRF process memory. **Scenario**: The memory utilization on the affected OAW-IAPs was very high. This issue was observed in all OAW-IAPs running Instant 6.4.4.3-4.2.2.0 and later versions.
145714	**Symptom**: Streaming videos on YouTube works even with the deny DPI WEBCC streaming-media ACL. The fix ensures that all live streaming channels are blocked if the deny ACL rule is applied **Scenario**: This issue occurred as the cached YouTube data was not getting blocked by the deny DPI WEBCC streaming-media ACL. This issue was observed in all OAW-IAPs running Instant 6.4.4.3-4.2.2.1 and later versions.

Authentication

Table 33: *Authentication Fixed Issue*

Bug ID	Description
137879	**Symptom**: The LDAP custom filters were not correctly managed in anOAW-IAP. The issue is resolved by inserting quotes to the custom filter strings of the OAW-IAP. **Scenario**: This issue occurred when spaces were found in the custom filter strings of the OAW-IAP. This issue was observed in all the OAW-IAPs running a software version prior to Instant 6.5.0.0-4.3.0.0.
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 6.5.0.0-4.3.0.0.

Configuration

Table 34: *Configuration Fixed Issue*

Bug ID	Description
138185	**Symptom**: Clients were facing security issues when OAW-IAPs were connected to the AMP. This issue is resolved by protecting the passwords sent by the AMP to OAW-IAPs. **Scenario**: This issue occurred when factory reset OAW-IAPs did not verify the password encryption when configured by the AMP. This issue was observed in all the OAW-IAPs running a software version prior to Instant 6.5.0.0-4.3.0.0.

DHCP Server

Table 35: *DHCP Server Fixed Issue*

Bug ID	Description
139264	**Symptom**: OAW-IAP were dropping proxy ARP packets received from a GRE tunnel. The issue is resolved by ensuring that OAW-IAPs drop the duplicate ARP packets received from the GRE tunnel. **Scenario**: This issue was observed in all the OAW-IAPs running a software version prior to Instant 6.5.0.0-4.3.0.0.

Platform

Table 36: *Platform Fixed Issue*

Bug ID	Description
120526 115821 138155	**Symptom**: When anOAW-IAP firmware upgrade was not successful due to invalid image URL, invalid image file, or server downtime, the new upgrade took effect only after the OAW-IAPs rebooted. The fix ensures that the new upgrade is triggered without rebooting the OAW-IAPs. **Scenario**: This issue was observed in all the OAW-IAPs running a software version prior to Instant 6.5.0.0-4.3.0.0.

UI

Table 37: *UI Fixed Issue*

Bug ID	Description
141904	**Symptom**: Clients were unable to authenticate to an LDAP server for 802.1x authentication when the customer filter contains a special character. The fix ensures that the escape characters are getting automatically added when the LDAP server is configured with a special customized entry in the **Filter** textbox in the Instant UI. **Scenario**: This issue occurred when the client entered special customized text in the **Filter** textbox when configuring an LDAP server for 802.1x authentication and was not limited to a specific OAW-IAP model or software version.

Wi-Fi Driver

Table 38: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
133845 138557 138559	**Symptom**: Clients were facing network issues when scanners were connected to the OAW-IAPs. This issue is resolved by modifying the maximum retries of frames launched by the OAW-IAPs. **Scenario**: This issue occurred when clients were unable to respond to 802.11 packets sent by the OAW-IAPs. This issue was observed in MC17 scanners connected to IAP-1xx series access points running a software version prior to Instant 6.5.0.0-4.3.0.0.
145298	**Symptom**: After reaching the allowed maximum client threshold, OAW-IAP2xx series access points and OAW-IAP3xx series access points did not send an alert when a new client attempted to connect to the OAW-IAP. The fix ensures that an alert is sent when a new client tries to connect to the OAW-IAP after it reaches the maximum client threshold. **Scenario**: This issue was observed in all OAW-IAP2xx series access points and OAW-IAP3xx series access points running a software version prior to Instant 6.5.0.0-4.3.0.0.
145718	**Symptom**: Starting from Instant 6.4.4.4-4.2.3.2, DFS channels were not broadcasted by OAW-IAP225-US access points unless they were specifically customized under the ARM profiles for OAW-IAP225-US. Additionally, the radio should be disabled on the Master OAW-IAP but enabled on the slave OAW-IAPs. However, the OAW-IAP225-US devices were displaying DFS channels without the special configuration. As a fix, the master and slave OAW-IAPs will each randomly select a valid channel under the special configuration. **Scenario**: This issue occurred due to an error in the channel select logic for the ARM channels and was observed in all OAW-IAP225-US access points running Instant 6.4.4.4-4.2.3.2 and later versions.

Appendix A
Acronyms and Abbreviations

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

Table 39: *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 39: *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 39: *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 39: *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 39: *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 39: *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 39: *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 39: *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 39: *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 39: *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 39: *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 39: *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 39: *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 39: *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 39: *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