AOS-W Instant 6.5.0.0-4.3.0.0

Alcatel·Lucent Enterprise

Release Notes

AOS-W Instant 6.5.0.0-4.3.0.0 is a major software release that introduces new features and enhancements.

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

What's New in this Release on page 6 lists the regulatory information, new features and enhancements, and fixed issues in AOS-W Instant 6.5.0.0-4.3.0.0 release.

Known Issues and Limitations on page 14 lists the known issues and limitations identified in the AOS-W Instant 6.5.0.0-4.3.0.0 release.

Contacting Support

Table 1: *Contact Information*

Contact Center Online	
Main Site	http://www.alcatel-lucent.com/enterprise
Support Site	https://service.esd.alcatel-lucent.com
Email	esd.support@alcatel-lucent.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 6.5.0.0-4.3.0.0 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 6.5.0.0-4.3.0.0 release:

Table 2: *DRT Versions*

Instant Release Version	Applicable DRT Version
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 service.esd.alcatel-lucent.com.

New Features and Enhancements

The following new features and enhancements are introduced in this release:

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 an OAW-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 an OAW-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*.

Resolved Issues in this Release

The following issues are fixed in the Instant 6.5.0.0-4.3.0.0 release.

AppRF

Table 3: *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 4: *Authentication Fixed Issue*

Bug ID	Description
137879	**Symptom**: The LDAP custom filters were not correctly managed in an OAW-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 5: *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 6: *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 7: *Platform Fixed Issue*

Bug ID	Description
120526 115821 138155	**Symptom**: When an OAW-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 8: *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 9: *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.

This chapter lists the known issues and limitations identified in the Instant 6.5.0.0-4.3.0.0 release.

Known Issues

The following known issues are identified in the Instant 6.5.0.0-4.3.0.0 release:

AppRF

Table 10: *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 11: *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 12: *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 13: *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 14: *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.

Appendix A
Acronyms and Abbreviations

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

Table 15: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
AAA	Authentication, Authorization, 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
ADP	Aruba Discovery Protocol
AES	Advanced Encryption Standard
AIFSN	Arbitrary Inter-frame Space Number
ALE	Analytics and Location Engine
ALG	Application Level Gateway
AM	Air Monitor
AMON	Application Monitoring
A-MSDU	Aggregate MAC Service Data Unit
AP	Access Point
API	Application Programming Interface
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
AVF	AntiVirus Firewall
BCMC	Broadcast-Multicast
BGP	Border Gateway protocol
BLE	Bluetooth Low Energy

Table 15: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CN	Common Name
CLI	Command-Line Interface
CoA	Change of Authorization
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CRC	Cyclical 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

Table 15: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
CTS	Clear to Send
CW	Contention Window
DAS	Distributed Antenna System
dB	Decibel
dBm	Decibel Milliwatt
DCE	Data Communication Equipment
DCF	Distributed Coordination Function
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMO	Dynamic Multicast optimization
DDMO	Distributed Dynamic Multicast Optimization
DNS	Domain Name System
DoS	Denial of Service
DN	Distinguished Name
DPD	Dead Peer Detection
DPI	Deep Packet Inspection
DR	Designated Router
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum
DST	Daylight Saving Time
DTE	Data Terminal Equipment
DTIM	Delivery Traffic Indication Message
DTLS	Datagram Transport Layer Security
DU	Data Unit

Table 15: *List of Acronyms and Abbreviations*

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

Table 15: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
FRER	Frame Receive Error Rate
FRR	Frame Retry Rate
FSPL	Free Space Path Loss
FTP	File Transfer Protocol
Gbps	Giga bits per second
GBps	Giga Bytes per second
GHz	Gigahertz
GIS	Generic Interface Specification
GMT	Greenwich Mean Time
GPP	Guest Provisioning Page
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
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 Server
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

Table 15: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
IKE PSK	Internet Key Exchange Pre-shared Key
IoT	Internet of Things
IP	Internet Protocol
IPM	Intelligent Power Monitoring
IPS	Intrusion Prevention System
IPSec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
JSON	JavaScript Object Notation
Kbps	Kilo bits per second
KBps	Kilo Bytes per second
L2TP	Layer-2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDPC	Low-Density Parity-Check
LEAP	Lightweight Extensible Authentication Protocol
LED	Light Emitting Diode
LEEF	Long Event Extended Format
LLDP	Link Layer Discovery Protocol
LMS	Local Management Switch
LTE	Long Term Evolution
MAB	MAC Authentication Bypass
MAC	Media Access Control
MAM	Mobile Application Management
MDM	Mobile Device Management

Table 15: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
Mbps	Mega bits per second
MBps	Mega Bytes per second
MCS	Modulation and Coding Scheme
mDNS	Multicast Domain Name System
MD5	Message Digest 5
MFA	Multi-factor Authentication
MHz	Megahertz
MIB	Management Information Base
MIMO	Multiple-Input Multiple-Output
MPDU	MAC Protocol Data Unit
MPLS	Multiprotocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSSID	Mesh Service Set Identifier
MTU	Maximum Transmission Unit
MU-MIMO	Multi-User Multiple-Input Multiple-Output
NAC	Network Access Control
NAD	Network Access Device
NAK	Negative Acknowledgment Code
NAP	Network Access Protection
NAS	Network Access Server
NAT	Network Address Translation
NetBIOS	Network Basic Input/Output System
NIC	Network Interface Card
Nmap	Network Mapper
NOE	New Office Environment
NTP	Network Time Protocol

Table 15: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
PDU	Power Distribution Unit
PSU	Power Supply 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
PMK	Pairwise Master Key
PoE	Power over Ethernet

Table 15: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
POST	Power On Self Test
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-Shared Key
PVST	Per VLAN Spanning Tree
QoS	Quality of Service
RADAR	Radio Detection and Ranging
RADIUS	Remote Authentication Dial-In User Service
RAP	Remote AP
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
RSSI	Received Signal Strength Indication
RSTP	Rapid Spanning Tree Protocol
RTCP	Real-Time Control Protocol
RTLS	Real-Time Location Systems
RTP	Real-Time Transport Protocol
RTS	Request to Send
RW RoW	Rest of World
SA	Security Association
SAML	Security Assertion Markup Language

Table 15: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SAN	Subject Alternative Name
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy Protocol
SDN	Software Defined Networking
SD-WAN	Software-Defined Wide Area Network
SDR	Software-Defined Radio
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIRT	Security Incident Response Team
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SNTP	Simple Network Time Protocol
SNIR	Signal-to-Noise-and-Interference Ratio
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SoC	System on a Chip
SoH	Statement of Health
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket layer
SSO	Single Sign-On
STP	Spanning Tree Protocol
STBC	Space-Time Block Coding
STRAP	Secure Thin Remote Access Point
SU-MIMO	Single-User Multiple-Input Multiple-Output

Table 15: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SVP	Spectralink Voice Priority
TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFTP	Trivial File Transfer Protocol
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TLV	Type-length-value
TOS	Type of Service
TPM	Trusted Platform Module
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
UDP	User Datagram Protocol
UDID	Unique Device Identifier
UI	User Interface
UMTS	Universal Mobile Telecommunication Systems
UPnP	Universal Plug n Play
URL	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VBN	Virtual Branch Networking

Table 15: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
VBR	Virtual Beacon Report
VHT	Very High Throughput
VIA	Virtual Intranet Access
VIP	Virtual IP Address
VA	Virtual Appliance
VM	Virtual Machine
VLAN	Virtual Local Area Network
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	Virtual Trunking Protocol
WebUI	Web browser User Interface
WAN	Wide Area Network
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
WMI	Windows Management Instrumentation
WMM	Wi-Fi Multimedia
WMS	WLAN Management System

Table 15: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
WPA	Wi-Fi Protected Access
WSDL	Web Service Description Language
WWW	World Wide Web
WZC	Wireless Zero Configuration
XAuth	Extended Authentication
XML	Extensible Markup Language
XML-RPC	XML Remote Procedure Call
ZTP	Zero Touch Provisioning