AOS-W Instant
6.5.1.0-4.3.1.2

Alcatel·Lucent

Enterprise

Copyright

Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit:

enterprise.alcatel-lucent.com/trademarks

All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. (January 2017)

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses.

Contents

AOS-W Instant 6.5.1.0-4.3.1.2 is a software patch release that introduces enhancements and fixes to the issues identified in the previous releases.

For information on upgrading OAW-IAPs to the new release version, refer to the *Upgrading an OAW-IAP* topic in the *AOS-W Instant 6.5.1.0-4.3.1.0 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 6.5.1.0-4.3.1.2 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

Updates for Instant 6.5.1.x-4.3.1.x

- The Application and Application Category features for AppRF is temporarily disabled for OAW-IAP205/205H platforms in the Instant 6.5.1.x-4.3.1.x release. However, the Web Category feature is still supported.
- Cluster Security with DTLS is a beta feature. Currently 16 OAW-IAPs and 256 clients are supported in an OAW-IAP cluster when this feature is enabled.
- OAW-IAP205H does not have BLE support.

Regulatory Domain Updates

The following table lists the DRT file versions supported by Instant 6.5.1.0-4.3.1.2 release:

Table 2: *DRT Versions*

Instant Release Version	Applicable DRT Version
6.5.1.0-4.3.1.2	1.0_58258
6.5.1.0-4.3.1.1	1.0_57815
6.5.1.0-4.3.1.0	1.0_57440

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:

UI Enhancement

The WPA Enterprise AES setting was not available in the Instant UI. In this release, a new field is added in the Instant UI for the WPA Enterprise AES setting.

Resolved Issues in this Release

The following issues are fixed in the Instant 6.5.1.0-4.3.1.2 release.

CLI

Table 3: *CLI Fixed Issue*

Bug ID	Description
154713	**Symptom**: The response for the XML API query did not provide 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-IAPs running a software version prior to Instant 6.5.1.0-4.3.1.2.

Datapath

Table 4: *Datapath Fixed Issues*

Bug ID	Description
154065	**Symptom**: Users were unable to access the internet periodically. This issue is resolved by changing the threshold for dropping packets from 8MB to 4MB. **Scenario**: This issue occurred when the system dropped downstream packets to avoid an out of memory issue as the available system memory was between 4MB - 8MB. This issue was observed in OAW-IAP205 access points and is not limited to specific Instant software version.
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 6.5.1.0-4.3.1.0

IPv6

Table 5: *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 6.5.1.0-4.3.1.2.

L2 Mobility

Table 6: *L2 Mobility Fixed Issue*

Bug ID	Description
154328	**Symptom**: The user ID sent for radius accounting was incorrect. The fix ensures that the correct user ID is sent for radius accounting. **Scenario**: This issue occurred when the client roamed from one OAW-IAP to another in the cluster and was observed in OAW-IAPs running a software version prior to Instant 6.5.1.0-4.3.1.2.

Platform

Table 7: *Platform Fixed Issue*

Bug ID	Description
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 6.5.1.0-4.3.1.2.

SNMP

Table 8: *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 was observed 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 Instant 6.5.1.0-4.3.1.2.

UI

Table 9: *UI Fixed Issue*

Bug ID	Description
156458 156662	**Symptom**: Static radio channels with 80MHz channel bonding enabled could not be configured using the Instant UI.The fix ensures that the configuration changes are applied successfully. **Scenario**: This issue was observed in OAW-IAP215 access points running a software version prior to Instant 6.5.1.0-4.3.1.2.

VPN

Table 10: *VPN Fixed Issue*

Bug ID	Description
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 IAP receives TCP sync packets from the client behind the VPN. **Scenario**: This issue was observed in OAW-IAPs running a software version prior to Instant 6.5.1.0-4.3.1.2.

Wi-Fi Driver

Table 11: *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 6.5.1.0-4.3.1.2.
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 6.5.1.0-4.3.1.2.
154370	**Symptom**: Motorola handheld scanners connected to OAW-IAP305 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-IAP305 access points running a software version prior to Instant 6.5.1.0-4.3.1.2.

This chapter lists the known issues and limitations identified in the Instant 6.5.1.x-4.3.1.x releases.

Known Issues

The following known issues are identified in the Instant 6.5.1.x-4.3.1.x releases:

AppRF

Table 12: *AppRF Known Issue*

Bug ID	Description
154066	**Symptom**: Application throttling ACL is throttling the bandwidth of all OAW-IAP traffic. **Scenario**: This issue is observed on OAW-IAPs running Instant 6.5.1.0-4.3.1.0. **Workaround**: Turn on full DPI visibility. However, this workaround applied to all platforms except for OAW-IAP205/205H.

L2 and L3 Mobility

Table 13: *L2 and L3 Mobility Known Issue*

Bug ID	Description
152180	**Symptom**: Data packets are dropped when the client roams from the home OAW-IAP to a new OAW-IAP. **Scenario**: The issue occurs due to inconsistency in the L3 tunnel formed between the new OAW-IAP and the home OAW-IAP and is observed in OAW-IAPs running Instant 6.5.1.0-4.3.1.0. **Workaround**: None.

Platform

Table 14: *Platform Known Issue*

Bug ID	Description
153710	**Symptom**: OAW-IAP335 crashed unexpectedly as skb is double freed somehow. **Scenario**: The crash occurs when OAW-IAP335 is using a 4G uplink with the 3272 modem. **Workaround**: None.

VC Management

Table 15: *VC Management Known Issue*

Bug ID	Description
145903	**Symptom**: OAW-IAP is sending non-existent image to Orion slave OAW-IAPs. **Scenario**: This issue occurred when an OAW-IAP105 joined a cluster with an OAW-IAP325 access point as the VC running Instant 6.5.0.0-4.3.0.0 release and later versions. **Workaround**: None.

This chapter describes the features and enhancements introduced in previous AOS-W Instant 6.5.1.x-4.3.1.x releases.

Features and Enhancements

This section describes the features and enhancements introduced in Instant 6.5.1.0-4.3.1.0 release.

Support for New IAP Devices

OAW-IAP300 Series

The OAW-IAP300 Series (OAW-IAP304/305) wireless access points are equipped with one 10/100/1000Base-T autosensing MDI/MDX Ethernet port. This port supports wired-network connectivity, in addition to Power over Ethernet (PoE) from IEEE 802.3af and 802.3at compliant power sources. They also have two LEDs that indicate the system and radio status of the device and are equipped with three external antenna connectors.

OAW-IAP207

The OAW-IAP207 access points are equipped with one 10/100/1000Base-T (RJ-45) auto-sensing, MDI/MDX Ethernet port ENET0) for wired network connectivity. This port supports IEEE 802.3af Power over Ethernet (PoE), as a standard defined Powered Device (PD) from a Power Sourcing Equipment (PSE) such as a PoE midspan injector or network infrastructure that supports PoE. The 207 Series access points have two LEDs that indicate the system and radio status of the device.

Support for Cluster Security

Instant 6.5.1.0-4.3.1.0 introduces support for cluster security on OAW-IAPs to secure the control plane communication between OAW-IAPs in a cluster. Additionally, DTLS is used with cluster security for extended security facilities. Cluster security also provides the option of logging and debugging by organizing the logs into modules which are later used for debugging. For more information, see:

- *Cluster Security* in *AOS-W Instant 6.5.1.0-4.3.1.0 User Guide*.
- **cluster-security**, **cluster-security logging**, **show cluster-security**, and **show log papi-handler** commands in the *AOS-W Instant 6.5.1.0-4.3.1.0 CLI Reference Guide*.

Support for RFC5997

Starting from Instant 6.5.1.0-4.3.1.0, you can configure the RFC5997 feature on the OAW-IAP to send a status request query to the RADIUS server each time there is an authentication or accounting request timeout. This helps determine if the server is actually down before marking the server as unavailable. For more information, see:

- *Configuring an External Server for Authentication* in *AOS-W Instant 6.5.1.0-4.3.1.0 User Guide.*
- **wlan auth-server** in *AOS-W Instant 6.5.1.0-4.3.1.0 CLI Reference Guide.*

Clarity Live

Instant now supports inline monitoring through Clarity Live to identify client connectivity issues and send the data to OmniVista for analysis. It helps in isolating the root cause of the connectivity issues experienced by receiving regular statistics and updates generated by the events. For more information, see:

- *Clarity Live* in *AOS-W Instant 6.5.1.0-4.3.1.0 User Guide.*

- **clarity,show clarity config**, and **show clarity history** in *AOS-W Instant 6.5.1.0-4.3.1.0 CLI Reference Guide.*

Client Match for Access Points in a Zone

Starting from Instant 6.5.1.0-4.3.1.0, the decision to move a client from a home OAW-IAP to a target OAW-IAP will be made at the SSID level instead of the radio level, by adding the SSID name to the client match radio database. Client Match will check if the same SSID (zone specific SSID on Home OAW-IAP) is available on the target OAW-IAP before it moves the client. For more information, see:

- *Client Match for Access Points in a Zone* in *AOS-W Instant 6.5.1.0-4.3.1.0 User Guide.*
- **show ap client-match-ssid-table** and **show ap client-match-ssid-table radio-mac <mac>** commands in *AOS-W Instant 6.5.1.0-4.3.1.0 CLI Reference Guide.*

Changing the Installation Mode

Instant now allows users to change the installation type of the OAW-IAPs from indoor to outdoor or vice-versa. For more information, see:

- *Changing the OAW-IAP Installation Mode* in *AOS-W Instant 6.5.1.0-4.3.1.0 User Guide.*
- **ap-installation** command in *AOS-W Instant 6.5.1.0-4.3.1.0 CLI Reference Guide.*

Support for Mesh in OAW-IAP31x and OAW-IAP-32x Access Points

Starting from Instant 6.5.1.0-4.3.1.0, support for Mesh is introduced in OAW-IAP31x and OAW-IAP-32x access points.

Enhancement to VPN Monitoring in AirWave

Starting from Instant 6.5.1.0-4.3.1.0, AMP receives a notification from the OAW-IAP every time the status of the VPN tunnel changes between UP and Down. For more information, see the OmniVista 8.2.3.1 User Guide.

Enhancements in OAW-IAP300 Series Access Points

The following enhancements have been introduced in OAW-IAP304/305 to improve the 5G radio throughput for the bridge mode:

- Use Core-2 to reduce Core-0 load on RX processing for bridge mode.
- Porting linux kernel code to reduce CPU cycles for skb allocation.
- Improved downstream throughput when WIDS overriding setting is dynamic.

This chapter describes the issues fixed in previous AOS-W Instant 6.5.1.x-4.3.1.x releases.

Issues Resolved in 6.5.1.0-4.3.1.0

There are no fixed issues in this release.

Issues Resolved in 6.5.1.0-4.3.1.0

AppRF

Table 16: *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 all the OAW-IAPs running a software version prior to Instant 6.5.1.0-4.3.1.0.

Captive Portal

Table 17: *Captive Portal Fixed Issues*

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 6.5.1.0-4.3.1.0.
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 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.

Datapath/Firewall

Table 18: *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 6.5.1.0-4.3.1.0.
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 6.5.1.0-4.3.1.0.
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 6.5.1.0-4.3.1.0.

Hotspot 2.0

Table 19: *Hotspot 2.0 Fixed Issues*

Bug ID	Description
144180	**Symptom**: Hotspot based auto connection was not happening when clients are configured with just the Roaming Consortium OI present in hs-profile. The fix ensure that the expected result is obtained. **Scenario**: This issue was observed in OAW-IAPs running a software version prior to Instant 6.5.1.0-4.3.1.0.
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 6.5.1.0-4.3.1.0.

Other

Table 20: *Other Fixed Issue*

Bug ID	Description
120526	**Symptom**: A vulnerability scan performed on the OAW-IAP cluster indicated the Dropbear SSH Server had multiple vulnerabilities. This issue is resolved by upgrading to a higher Dropbear firmware. **Scenario**: This issue was observed in OAW-IAP105 access points and was not limited to a specific Instant software version.

UI

Table 21: *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 22: *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.

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

Table 23: *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 23: *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 23: *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 23: *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 23: *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 23: *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 23: *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 23: *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 23: *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 23: *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 23: *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 23: *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 23: *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 23: *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 23: *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