

Aruba Instant 6.5.0.3-4.3.0.4



Copyright Information

© Copyright 2017 Hewlett Packard Enterprise Development LP.

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. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

- Contents 3**
- Revision History 5
- Release Overview 6**
- Chapter Overview 6
- Important Updates 6
- Supported Browsers 6
- Contacting Support 7
- Features and Enhancements 8**
- Features and Enhancements in Instant 6.5.0.3-4.3.0.4 8
- Features and Enhancements in Instant 6.5.0.3-4.3.0.3 8
- Features and Enhancements in Instant 6.5.0.0-4.3.0.2 8
- Features and Enhancements in Instant 6.5.0.0-4.3.0.1 8
- Features and Enhancements in Instant 6.5.0.0-4.3.0.0 8
- Regulatory Updates 14**
- Regulatory Updates in Instant 6.5.0.3-4.3.0.4 14
- Regulatory Updates in Instant 6.5.0.3-4.3.0.3 14
- Regulatory Updates in Instant 6.5.0.0-4.3.0.2 14
- Regulatory Updates in Instant 6.5.0.0-4.3.0.1 14

Regulatory Updates in Instant 6.5.0.0-4.3.0.0	14
Resolved Issues	15
Resolved Issues in Instant 6.5.0.3-4.3.0.4	15
Resolved Issues in Instant 6.5.0.3-4.3.0.3	19
Resolved Issues in Instant 6.5.0.0-4.3.0.2	25
Resolved Issues in Instant 6.5.0.0-4.3.0.1	26
Resolved Issues in Instant 6.5.0.0-4.3.0.0	29
Known Issues	32
Glossary of Terms	34

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release

Instant 6.5.0.3-4.3.0.4 is a software patch release that includes the known issues and resolved issues in this release, and fixes to issues identified in previous releases.

Chapter Overview

- [Regulatory Updates on page 14](#) lists the regulatory updates in the Instant 6.5.0.x-4.3.0.x releases.
- [Resolved Issues on page 15](#) describes the issues resolved in the Instant 6.5.0.x-4.3.0.x releases.
- [Known Issues on page 32](#) describes the known issues identified in the Instant 6.5.0.x-4.3.0.x releases.
- [Glossary of Terms on page 34](#) lists the acronyms and abbreviations used in the document.

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 IAPs are not supported.

- IAP-104 and IAP-105
- RAP-3WN and RAP-3WNP
- IAP-134 and IAP-135
- IAP-175

Supported Browsers

The following browsers are officially supported for use with Instant Web User Interface (WebUI):

- Microsoft Internet Explorer 10.x and 11 on Windows 7 and Windows 8
- Mozilla Firefox 23 or later on Windows Vista, Windows 7, Windows 8, and Mac OS
- Apple Safari 5.1.7 or later on Mac OS

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	hpe.com/networking/support
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

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

Features and Enhancements in Instant 6.5.0.3-4.3.0.4

There are no new features and enhancements in this release.

Features and Enhancements in Instant 6.5.0.3-4.3.0.3

There are no new features and enhancements in this release.

Features and Enhancements in Instant 6.5.0.0-4.3.0.2

There are no new features and enhancements in this release.

Features and Enhancements in Instant 6.5.0.0-4.3.0.1

There are no new features and enhancements in this release.

Features and Enhancements in Instant 6.5.0.0-4.3.0.0

This section describes the features and enhancements introduced in the Instant 6.5.0.0-4.3.0.0 release.

Support for New IAP Devices

IAP-310 Series

The IAP-310 Series (IAP-314/315) 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 802.11 a/b/g wireless services.

The IAP-310 Series wireless access points provide the following capabilities:

- IEEE 802.11 a/b/g/n/ac wireless access point

- IEEE 802.11 a/b/g/n/ac wireless air monitor
- IEEE 802.11 a/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

IAP-330 Series

The IAP-330 Series (IAP-334/335) wireless access points support IEEE 802.11 ac 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 802.11 n 2.4 GHz and 802.11 ac 5 GHz functionality, while also supporting 802.11 a/b/g wireless services.

The IAP-330 wireless access points provide the following capabilities:

- IEEE 802.11 a/b/g/n/ac wireless access point
- IEEE 802.11 a/b/g/n/ac wireless air monitor
- IEEE 802.11 a/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 IAP. You can also set the MCS rates for greater 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 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 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 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 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 *Aruba Instant 6.5.0.0-4.3.0.0 User Guide*
- **wlan ssid-profile** command page in *Aruba 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, 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 *Aruba Instant 6.5.0.0-4.3.0.0 User Guide*
- **show datapath session ucc** command in *Aruba Instant 6.5.0.0-4.3.0.0 CLI Reference Guide*.

Enabling Enhanced Voice Call Tracking

Starting from Aruba Instant 6.5.0.0-4.3.0.0, 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 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 IAP using SNMP GET. The Master IAP responds back to the third-party server with the location of the VoIP caller.

Redirect Blocked HTTPS 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 *Aruba 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 Aruba 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 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 IAP-324/325, IAP-314/315, IAP-334/335 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 individually for an SSID radio profile, using the IAP CLI. For more information, see:

- *Configuring Maximum Clients on SSID Radio Profiles* in *Aruba 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 IAP-334/335 and IAP-314/315 access points. For information on configuring client match on IAPs, see:

- *Adaptive Radio Management* in *Aruba 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 Aruba 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 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 IAP is connected. For more information, see:

- *Configuring System Parameters in Aruba 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 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 Aruba 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. 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 Aruba 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 enhancements have been made to the IAP image upgrade and image sync processes:

- If an automatic image upgrade fails, rebooting the IAP cluster is no longer required to proceed with the next image upgrade attempt.
- Previously, all the IAPs in the cluster were required to download the image from external server. Starting from this release, only 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 IAP joins a cluster:
 - If the cluster already contains the same image class of IAPs as the new slave IAP, the new slave IAP does not have to download the image from the external server. The newly added slave IAP will perform an image sync with an existing slave IAP of the same class.

- If the cluster does not contain the same image class of IAPs as the new slave IAP, the new slave IAP has to download the image from the external server.
- If the new slave IAP joining the cluster is unable to download the image from an AMP server located behind the VPN tunnel, the master 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 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 IAP to access control capabilities to clients, firewall enhancements, management of IAPs through a static IPv6 address, and support for IPv6 RADIUS server. For more information, see:

- *IPv6 Support* in *Aruba 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 *Aruba 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.

The chapter describes the Downloadable Regulatory Table (DRT) updates in Instant 6.5.0.x-4.3.0.x. releases.

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



The FCC has changed the rules for operation in all of the 5 GHz bands. For more information, refer to the *FCC DFS Regulatory Change Impact and Resolution Plan - Support Advisory* available in [Support Advisories](#).

Regulatory Updates in Instant 6.5.0.3-4.3.0.4

The following DRT file version is part of the Instant 6.5.0.3-4.3.0.4 release.

- DRT-1.0_59118

Regulatory Updates in Instant 6.5.0.3-4.3.0.3

The following DRT file version is part of the Instant 6.5.0.3-4.3.0.3 release.

- DRT-1.0_58258

Regulatory Updates in Instant 6.5.0.0-4.3.0.2

The following DRT file version is part of the Instant 6.5.0.0-4.3.0.2 release.

- DRT-1.0_57440

Regulatory Updates in Instant 6.5.0.0-4.3.0.1

The following DRT file version is part of the Instant 6.5.0.0-4.3.0.1 release.

- DRT-1.0_57023

Regulatory Updates in Instant 6.5.0.0-4.3.0.0

The following DRT file version is part of the Instant 6.5.0.0-4.3.0.0 release.

- DRT-1.0_56308

This chapter describes the issues resolved in the Aruba Instant 6.5.0.x-4.3.0.x releases.

Resolved Issues in Instant 6.5.0.3-4.3.0.4

AirWave

Table 3: *AirWave Fixed Issue*

Bug ID	Description
153781 155617	<p>Symptom: Inactive clients were reported to AirWave only after a full timeout occurred. The fix ensures that the IAPs report inactive clients to AirWave in a timely fashion.</p> <p>Scenario: This issue was observed in IAPs running any software version prior to Instant 6.5.0.3-4.3.0.4.</p>

ARM

Table 4: *ARM Fixed Issue*

Bug ID	Description
153576	<p>Symptom: ARM changed channels frequently. The fix ensures that ARM does not change channels frequently.</p> <p>Scenario: This issue was observed in IAPs running Instant 6.5.0.0-4.3.0.0 or later versions.</p>

Authentication

Table 5: *Authentication Fixed Issue*

Bug ID	Description
148031	<p>Symptom: The CLI output of the show clients debug command was unable to display the correct client role value. The issue is resolved by setting a role name from a 802.11r cache.</p> <p>Scenario: This issue occurred when clients roaming on a 802.11r enabled network were assigned incorrect roles. This issue was observed in IAP-205 access points running any software version prior to Instant 6.5.0.3-4.3.0.4.</p>

Captive Portal

Table 6: *Captive Portal Fixed Issue*

Bug ID	Description
156360	<p>Symptom: Apple users were sometimes not redirected to the ClearPass Guest welcome page after a captive portal authentication was successful. The fix ensures that the clients are redirected to the URL after a captive portal authentication is successful.</p> <p>Scenario: This issue occurred because clients used the HTTPS post on ClearPass Policy Manager. This issue was observed in IAPs running any software version prior to Instant 6.5.0.3-4.3.0.4.</p>

Central

Table 7: *Central Fixed Issue*

Bug ID	Description
155630 157024	<p>Symptom: The username field on Cloud Guest showed up as encrypted. The fix ensures that the username text is not encrypted.</p> <p>Scenario: The issue occurred when the Cloud Guest was integrated with Central, and was observed in IAPs running any software version prior to Instant 6.5.0.3-4.3.0.4.</p>
158008	<p>Symptom: The IAP VC was unable to recover the connection with Central after getting disconnected. This issue is resolved by ensuring that the start connect time is triggered as soon as the IAP disconnects and attempts to reconnect to Central.</p> <p>Scenario: This issue was observed only once in an IAP-225 access point running any software version prior to Instant 6.5.0.3-4.3.0.4.</p>

CLI

Table 8: *CLI Fixed Issue*

Bug ID	Description
156295	<p>Symptom: The NAS ID was sent with extra double quotes to the RADIUS server. The fix ensures that the NAS ID is not sent with the extra double quotes.</p> <p>Scenario: This issue occurred when there was a space in the NAS ID string. This issue was observed in IAPs running any software version prior to Instant 6.5.0.3-4.3.0.4</p>

Datapath/Firewall

Table 9: *Datapath/Firewall Fixed Issue*

Bug ID	Description
154065	<p>Symptom: Users were unable to access the Internet periodically. The issue is resolved by changing the threshold for dropping packets from 8 MB to 4 MB.</p> <p>Scenario: This issue occurred when the system dropped downstream packets to avoid an out-of-memory issue as the available system memory was between 4 MB and 8 MB. This issue was observed in IAP-205H access points and is not limited to specific Instant software version.</p>
154464	<p>Symptom: Continuous packet drops were observed when traffic was sent through the Eth1 port at 100 Mbps. The issue is resolved by enabling flow control inside the ethernet switch clip.</p> <p>Scenario: This issue occurred due to the difference in speeds between the uplink and downlink ports. This issue was observed in IAP-205H access points running a software version prior to Instant 6.5.0.3-4.3.0.4.</p>
157343	<p>Symptom: The DHCP server was active even when there was a mismatch in the uplink VLAN configuration. The issue resolved by performing a VLAN validation of the DHCP packets during IAP boot.</p> <p>Scenario: This issue was observed in all the IAPs running any software version prior to Instant 6.5.0.3-4.3.0.4.</p>

L2 Mobility

Table 10: *L2 Mobility Fixed Issue*

Bug ID	Description
154328	<p>Symptom: The user ID sent for RADIUS accounting was incorrect. The issue is resolved by adding a username selection logic with the timestamp comparison of online and offline clients.</p> <p>Scenario: This issue occurred when the client roamed from one IAP to another in a cluster. This issue was observed in IAPs running anysoftware version prior to Instant 6.5.0.3-4.3.0.4.</p>

Platform

Table 11: *Platform Fixed Issue*

Bug ID	Description
152062	Symptom: Some IAPs randomly rebooted due to a kernel panic. The issue is resolved by adding a crash protection mechanism to the power state code of the IAP. Scenario: This issue occurred within the first few minutes of boot, and was observed in IAP-275 access points running any software version prior to Instant 6.5.0.3-4.3.0.4.
158297	Symptom: The ESSID name in DHCP option 82 was missing for some access points. This issue is resolved by making a change in the driver function to display the ESSID. Scenario: This issue was observed in IAP-315 access points running any software version prior to Instant 6.5.0.3-4.3.0.4.

WiFi Driver

Table 12: *WiFi Driver Fixed Issue*

Bug ID	Description
159343	Symptom: A slave IAP crashed and rebooted without displaying any reason for the error. Scenario: This issue was observed in IAP-103 access points running any software version prior to Instant 6.5.0.3-4.3.0.4 version

WebUI

Table 13: *WebUI Fixed Issue*

Bug ID	Description
151749 152092	Symptom: The WPA Enterprise AES setting was not available in the Instant WebUI. This issue is resolved by adding a new field in the Instant WebUI for AES setting. Scenario: This issue was observed in IAPs running any software version prior to Instant 6.5.0.3-4.3.0.4.
154558	Symptom: The IAP WebUI did not load on the Internet Explorer or Mozilla Firefox browsers if the IAP name contained special characters. The fix ensures that the IAP WebUI is able to load on the Internet Explorer and Mozilla Firefox browsers. Scenario: This issue was observed in IAPs running any software version prior to Instant 6.5.0.3-4.3.0.4.

XML-API

Table 14: XML-API Fixed Issue

Bug ID	Description
158869	Symptom: XML API did not return calls made through port 443. The fix ensures that calls are successfully made through port 443. Scenario: This issue was observed in IAPs running Instant 6.5.0.0-4.3.0.0 or later versions.

Resolved Issues in Instant 6.5.0.3-4.3.0.3

AppRF

Table 15: 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 IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.

Captive Portal

Table 16: 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 IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.

Central

Table 17: Central Fixed Issue

Bug ID	Description
151981	Symptom: The output for the show ap debug cloud-server command showed the VC is connected to Central, however the VC was not sending any updates to the cloud server. The fix ensures that the VC successfully sends the updates to the cloud server. Scenario: This issue occurred due to inconsistencies in the awc process and was observed in IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.

Configuration

Table 18: Configuration Fixed Issues

Bug ID	Description
145050 149491 149515	<p>Symptom: The syslog messages from the IAP indicated a configuration mismatch between the VC and the slave IAPs in a cluster. This issue is resolved by initiating the enet-vlan configuration when the IAP restarts.</p> <p>Scenario: This issue occurred when mesh point was configured on the IAP and enet-vlan configuration was removed from the master IAP. This issue was observed in IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>

Datapath/Firewall

Table 19: Datapath/Firewall Fixed Issues

Bug ID	Description
145296	<p>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.</p> <p>Scenario: This issue was observed in IAP-103 and IAP-275 access points running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>
146666	<p>Symptom: Slave 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 IAPs to successfully connect to the guest network.</p> <p>Scenario: This issue was observed in IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>
152421	<p>Symptom: Some 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 IAPs are able to obtain a private IP address and the Web UI is able to connect to the wireless clients on the Instant SSID.</p> <p>Scenario: This issue was observed in IAP-204/205, IAP-314/315, IAP-324/325 platforms running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>
151748	<p>Symptom: AnIAP 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.</p> <p>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 IAP-325 access points running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>

Bug ID	Description
154522	Symptom: Clients connected to the master 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 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 IAP from carrying out the pending session delete operation. Scenario: This issue occurred as the datapath user session count was continuously increasing and was not getting aged out or reset. This issue was observed in IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.
156718	Symptom: AnIAP 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 IAPs running a software version prior to Instant 6.4.4.8-4.2.4.6.

GRE

Table 20: *GRE Fixed Issue*

Bug ID	Description
151725	Symptom: 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 IAP uses the specified MTU value for GRE fragmentation. Scenario: This issue was observed in IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.

Hotspot 2.0

Table 21: *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 IAP. Scenario: This issue was observed in IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.

IPv6

Table 22: IPv6 Fixed Issue

Bug ID	Description
154827	<p>Symptom: IAP-200 series access points crashed due to kernel panic. The fix ensures that the IAP does not crash and reboot due to kernel panic.</p> <p>Scenario: This issue occurred when multiple IPv4 and IPv6 DNS mobility messages were sent by the IAP. This issue was observed in IAP-200 series access points running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>

Other

Table 23: Other Fixed Issue

Bug ID	Description
152060	<p>Symptom: 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 IAP uses the specified MTU value for GRE fragmentation.</p> <p>Scenario: This issue was observed in IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>

Platform

Table 24: Platform Fixed Issues

Bug ID	Description
135764	<p>Symptom: Some 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.</p> <p>Scenario: : This issue was observed in IAP-205 access points running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>
152825	<p>Symptom: Some 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.</p> <p>Scenario: : This issue was observed in IAP-205 access points running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>
154738	<p>Symptom: Some IAPs were encountering bitflip memory corruption. The fix ensures that the bitflip memory corruption issue is resolved.</p> <p>Scenario: : This issue occurred as the IAPs were using old SBL2 firmware. This issue was observed in IAP-315 access points running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>

SNMP

Table 25: *SNMP Fixed Issue*

Bug ID	Description
155081	<p>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.</p> <p>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 IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>

UI

Table 26: *UI Fixed Issue*

Bug ID	Description
155081	<p>Symptom: The response for the XML API query did not provide the correct XML API statistics. The fix ensures that the XML API statistics are periodically updated and the response to the XML API query provides the correct information.</p> <p>Scenario: This issue was observed in IAP-205H access points running Instant 6.5.0.0-4.3.0.0 or later versions.</p>

VPN

Table 27: *VPN Fixed Issues*

Bug ID	Description
149319	<p>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.</p> <p>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 IAP-215 access points running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>
156175	<p>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.</p> <p>Scenario: This issue was observed in IAPs running Instant 6.5.0.0-4.3.0.0 release or later versions.</p>

Wi-Fi Driver

Table 28: *Wi-fi Driver Fixed Issues*

Bug ID	Description
118039 156391	<p>Symptom: AnIAP-275 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.</p> <p>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 IAP-275 access points running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>
138637	<p>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.</p> <p>Scenario: : This issue was observed in IAP-275 access points running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>
150704	<p>Symptom: IAP did not send all the interference SSID details to AirWave. This issue is resolved by extending the maximum number of entries in the IDS table to 2048.</p> <p>Scenario: This issue occurred as the IDS table was full and was observed in all IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>
151866	<p>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.</p> <p>Scenario: This issue occurred as the default value of the beacon interval was altered and was observed in IAP-325 access points running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>
154237	<p>Symptom: AnIAP crashed and rebooted unexpectedly. The fix ensures that the IAP does not crash due to kernel panic.</p> <p>Scenario: This issue occurred as the IAP experienced a kernel panic due to softlockup hung tasks. This issue was observed in IAPs running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>
154370	<p>Symptom: Motorola handheld scanners connected to IAP-325 access points were getting disconnected every 10 seconds. This issue is resolved by making a change to the default CCA threshold value.</p> <p>Scenario:This issue was observed in IAP-325 access points running a software version prior to Instant 6.5.0.3-4.3.0.3.</p>

Resolved Issues in Instant 6.5.0.0-4.3.0.2

Captive Portal

Table 29: *Captive Portal Fixed Issue*

Bug ID	Description
151119	<p>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.</p> <p>Scenario: This issue was observed in IAPs running Instant 6.5.0.0-4.3.0.0 release and later versions.</p>

Datapath/Firewall

Table 30: *Datapath/Firewall Fixed Issues*

Bug ID	Description
146942	<p>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:</p> <ul style="list-style-type: none">■ On the server side the ports for voice and video must be clearly defined to a specific subset.■ On the 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. <p>Scenario: This issue was observed in IAPs running Instant 6.5.0.0-4.3.0.0 and later releases.</p>
152782	<p>Symptom: IAP-275 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.</p> <p>Scenario: This issue was observed in IAP-275 access points running a software version prior to Instant 6.5.0.0-4.3.0.2.</p>

Mesh

Table 31: *Mesh Fixed Issue*

Bug ID	Description
145637	<p>Symptom: IAP-225 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.</p> <p>Scenario: This issue was observed in IAP-225 access points running a software version prior to Instant 6.5.0.0-4.3.0.2.</p>

Platform

Table 32: *Platform Fixed Issues*

Bug ID	Description
145634 150907	Symptom: AnIAP crashed unexpectedly when using a 10Mbps half-duplex uplink and upstream traffic exceed 10Mbps. The log file of the event listed the reason as kernel panic. The fix ensures that the IAP works as expected. Scenario: This issue was observed in IAP-215 and IAP-225 access points running a software version prior to Instant 6.5.0.0-4.3.0.2.
152840 153318	Symptom: AnIAP crashed and rebooted unexpectedly due to kernel panic. The fix ensures that the 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 IAP-215 access points running a software version prior to Instant 6.5.0.0-4.3.0.2.

Wi-Fi Driver

Table 33: *Wi-fi Driver Fixed Issue*

Bug ID	Description
151995	Symptom: AnIAP crashed and rebooted with the reason: Reboot caused by kernel panic: Fatal exception. The fix ensures that the IAP does not crash during compiler optimization. Scenario: This issue occurred when the compiler optimization was in progress and was observed in IAP-215 access points running a software version prior to Instant 6.5.0.0-4.3.0.2.

Resolved Issues in Instant 6.5.0.0-4.3.0.1

AirWave

Table 34: *AirWave Fixed Issue*

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

Authentication

Table 35: *Authentication Fixed Issues*

Bug ID	Description
148759	<p>Symptom: 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.</p> <p>Scenario: This issue was not limited to a specific IAP model or Instant software version.</p>
149532	<p>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.</p> <p>Scenario: This issue was observed in all IAPs running a software version prior to Instant 6.5.0.0-4.3.0.1.</p>

CLI

Table 36: *CLI Fixed Issue*

Bug ID	Description
151137	<p>Symptom: The CLI for anIAP-205 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.</p> <p>Scenario: This issue was observed in IAP-205 access points running a software version prior to Instant 6.5.0.0-4.3.0.1.</p>

Platform

Table 37: *Platform Fixed Issue*

Bug ID	Description
147826	<p>Symptom: IAP-325 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.</p> <p>Scenario: This issue occurred due to duplicate entries in the subnet table and was observed in IAP-325 access points running a software version prior to Instant 6.5.0.0-4.3.0.1.</p>

VC Management

Table 38: *VC Management Fixed Issue*

Bug ID	Description
147826	<p>Symptom: Some IAPs were intermittently getting disconnected from the cluster. The fix resolves the out of memory issue that caused the IAPs to disconnect from the cluster.</p> <p>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 IAPs running a software version prior to Instant 6.5.0.0-4.3.0.1.</p>

Wi-Fi Driver

Table 39: *Wi-fi Driver Fixed Issue*

Bug ID	Description
147682	<p>Symptom: A slave IAP incorrectly classified another IAP belonging to the same cluster as a rogue IAP. The fix ensures that the IAPs can correct the wrong entry in very short time.</p> <p>Scenario: This issue occurred as the slave IAP lost the messages of the updated MAC address list from the VC. This issue was observed in all IAPs running a software version prior to Instant 6.5.0.0-4.3.0.1.</p>

Resolved Issues in Instant 6.5.0.0-4.3.0.0

AppRF

Table 40: *AppRF Fixed Issue*

Bug ID	Description
120228	<p>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 IAP.</p> <p>Scenario: This issue was observed in all the IAPs running a software version prior to Instant 6.5.0.0-4.3.0.0.</p>
142278 141891	<p>Symptom: Some 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.</p> <p>Scenario: The memory utilization on the affected IAPs was very high. This issue was observed in all IAPs running Instant 6.4.4.3-4.2.2.0 and later versions.</p>
145714	<p>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</p> <p>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 IAPs running Instant 6.4.4.3-4.2.2.1 and later versions.</p>

Authentication

Table 41: *Authentication Fixed Issue*

Bug ID	Description
137879	<p>Symptom: The LDAP custom filters were not correctly managed in anIAP. The issue is resolved by inserting quotes to the custom filter strings of the IAP.</p> <p>Scenario: This issue occurred when spaces were found in the custom filter strings of the IAP. This issue was observed in all the IAPs running a software version prior to Instant 6.5.0.0-4.3.0.0.</p>
148693	<p>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 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.</p> <p>Scenario: This issue impacted all scenarios where captive portal is used and was observed in all IAPs running a software version prior to Instant 6.5.0.0-4.3.0.0.</p>

Configuration

Table 42: Configuration Fixed Issue

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

DHCP Server

Table 43: DHCP Server Fixed Issue

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

Platform

Table 44: Platform Fixed Issue

Bug ID	Description
120526 115821 138155	<p>Symptom: When an 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 IAPs rebooted. The fix ensures that the new upgrade is triggered without rebooting the IAPs.</p> <p>Scenario: This issue was observed in all the IAPs running a software version prior to Instant 6.5.0.0-4.3.0.0.</p>

UI

Table 45: UI Fixed Issue

Bug ID	Description
141904	<p>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.</p> <p>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 IAP model or software version.</p>

Wi-Fi Driver

Table 46: *Wi-Fi Driver Fixed Issue*

Bug ID	Description
133845 138557 138559	<p>Symptom: Clients were facing network issues when scanners were connected to the IAPs. This issue is resolved by modifying the maximum retries of frames launched by the IAPs.</p> <p>Scenario: This issue occurred when clients were unable to respond to 802.11 packets sent by the 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.</p>
145298	<p>Symptom: After reaching the allowed maximum client threshold, IAP-2xx series access points and IAP-3xx series access points did not send an alert when a new client attempted to connect to the IAP. The fix ensures that an alert is sent when a new client tries to connect to the IAP after it reaches the maximum client threshold.</p> <p>Scenario: This issue was observed in all IAP-2xx series access points and IAP-3xx series access points running a software version prior to Instant 6.5.0.0-4.3.0.0.</p>
145718	<p>Symptom: Starting from Instant 6.4.4.4-4.2.3.2, DFS channels were not broadcasted by IAP-225-US access points unless they were specifically customized under the ARM profiles for IAP-225-US. Additionally, the radio should be disabled on the Master IAP but enabled on the slave IAPs. However, the IAP-225-US devices were displaying DFS channels without the special configuration. As a fix, the master and slave IAPs will each randomly select a valid channel under the special configuration.</p> <p>Scenario: This issue occurred due to an error in the channel select logic for the ARM channels and was observed in all IAP-225-US access points running Instant 6.4.4.4-4.2.3.2 and later versions.</p>

This chapter describes the known issues in the Aruba Instant 6.5.0.x-4.3.0.x releases.

Datapath/Firewall

Table 47: *Datapath/Firewall Known Issue*

Bug ID	Description
148017	<p>Symptom: Media classification does not happen for Skype for Business calls during L2 roaming.</p> <p>Scenario: This issue occurs rarely when there are packets lost on a wired network during client roaming. This results in loss of media classified information. This issue is observed in IAPs running Instant 6.5.0.0-4.3.0.0 or later versions.</p> <p>Workaround: None.</p>

SNMP

Table 48: *SNMP Known Issue*

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

VC Management

Table 49: *VC Management Known Issue*

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

VPN

Table 50: *VPN Known Issue*

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

The following table provides a brief description of the terminology used in this guide.

3DES

Triple Data Encryption Standard. 3DES is a symmetric-key block cipher that applies the DES cipher algorithm three times to each data block.

3G

Third Generation of Wireless Mobile Telecommunications Technology. See W-CDMA.

3GPP

Third Generation Partnership Project. 3GPP is a collaborative project aimed at developing globally acceptable specifications for third generation mobile systems.

4G

Fourth Generation of Wireless Mobile Telecommunications Technology. See LTE.

802.11

802.11 is an evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and Carrier Sense Multiple Access with collision avoidance (CSMA/CA) for path sharing.

802.11 bSec

802.11 bSec is an alternative to 802.11i. The difference between bSec and standard 802.11i is that bSec implements Suite B algorithms wherever possible. Notably, Advanced Encryption Standard-Counter with CBC-MAC is replaced by Advanced Encryption Standard - Galois/Counter Mode, and the Key Derivation Function (KDF) of 802.11i is upgraded to support SHA-256 and SHA-384.

802.11a

802.11a provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5 GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.

802.11ac

802.11ac is a wireless networking standard in the 802.11 family that provides high-throughput WLANs on the 5 GHz band.

802.11b

802.11b is a WLAN standard often called Wi-Fi and is backward compatible with 802.11. Instead of the Phase-Shift Keying (PSK) modulation method used in 802.11 standards, 802.11b uses Complementary Code Keying (CCK) that allows higher data speeds and makes it less susceptible to multipath-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.

802.11d

802.11d is a wireless network communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate. Configuration can be fine-tuned at the Media Access Control (MAC) layer level to comply with the rules of the country or district in which the network is to be used. Rules are subject to variation and include allowed frequencies, allowed power levels, and allowed signal bandwidth. 802.11d facilitates global roaming.

802.11e

802.11e is an enhancement to the 802.11a and 802.11b specifications that enhances the 802.11 Media Access Control layer with a coordinated Time Division Multiple Access (TDMA) construct. It adds error-correcting mechanisms for delay-sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability between business, home, and public environments such as airports and hotels, and offers all subscribers high-speed Internet access with full-motion video, high-fidelity audio, and VoIP.

802.11g

802.11g offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b standard. 802.11g employs Orthogonal Frequency Division Multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speed of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.

802.11h

802.11h is intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with military RADAR systems and medical devices. Dynamic Frequency Selection (DFS) detects the presence of other devices on a channel and automatically switches the network to another channel if and when such signals are detected. Transmit Power Control (TPC) reduces the radio frequency (RF) output power of each network transmitter to a level that minimizes the risk of interference.

802.11i

802.11i provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards. It requires new encryption key protocols, known as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

802.11j

802.11j is a proposed addition to the 802.11 family of standards that incorporates Japanese regulatory extensions to 802.11a; the main intent is to add channels in the radio frequency (RF) band of 4.9 GHz to 5.0 GHz.

802.11k

802.11k is an IEEE standard that enables APs and client devices to discover the best available radio resources for seamless BSS transition in a WLAN.

802.11m

802.11m is an Initiative to perform editorial maintenance, corrections, improvements, clarifications, and interpretations relevant to documentation for 802.11 family specifications.

802.11n

802.11n is a wireless networking standard to improve network throughput over the two previous standards, 802.11a and 802.11g. With 802.11n, there will be a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz.

802.11r

802.11r is an IEEE standard for enabling seamless BSS transitions in a WLAN. 802.11r standard is also referred to as Fast BSS transition.

802.11u

802.11u is an amendment to the IEEE 802.11 WLAN standards for connection to external networks using common wireless devices such as smartphones and tablet PCs. The 802.11u protocol provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users to roam between partner networks without additional authentication. An 802.11u-capable device supports the Passpoint technology from the Wi-Fi Alliance Hotspot 2.0 R2 Specification that simplifies and automates access to public Wi-Fi.

802.11v

802.11v is an IEEE standard that allows client devices to exchange information about the network topology and RF environment. This information is used for assigning best available radio resources for the client devices to provide seamless connectivity.

802.1Q

802.1Q is an IEEE standard that enables the use of VLANs on an Ethernet network. 802.1Q supports VLAN tagging.

802.1X

802.1X is an IEEE standard for port-based network access control designed to enhance 802.11 WLAN security. 802.1X provides an authentication framework that allows a user to be authenticated by a central authority.

802.3af

802.3af is an IEEE standard for Power over Ethernet (PoE) version that supplies up to 15.4W of DC power. See PoE.

802.3at

802.3at is an IEEE standard for PoE version that supplies up to 25.5W of DC power. See PoE+.

AAA

Authentication, Authorization, and Accounting. AAA is a security framework to authenticate users, authorize the type of access based on user credentials, and record authentication events and information about the network access and network resource consumption.

ABR

Area Border Router. ABR is used for establishing connection between the backbone networks and the Open Shortest Path First (OSPF) areas. ABR is located near the border of one or more OSPF areas.

AC

Access Category. As per the IEEE 802.11e standards, AC refers to various levels of traffic prioritization in Enhanced Distributed Channel Access (EDCA) operation mode. The WLAN applications prioritize traffic based on the Background, Best Effort, Video, and Voice access categories. AC can also refer to Alternating Current, a form of electric energy that flows when the appliances are plugged to a wall socket.

ACC

Advanced Cellular Coexistence. The ACC feature in APs enable WLANs to perform at peak efficiency by minimizing interference from 3G/4G/LTE networks, distributed antenna systems, and commercial small cell/femtocell equipment.

Access-Accept

Response from the RADIUS server indicating successful authentication and containing authorization information.

Access-Reject

Response from RADIUS server indicating that a user is not authorized.

Access-Request

RADIUS packet sent to a RADIUS server requesting authorization.

Accounting-Request

RADIUS packet type sent to a RADIUS server containing accounting summary information.

Accounting-Response

RADIUS packet sent by the RADIUS server to acknowledge receipt of an Accounting-Request.

ACE

Access Control Entry. ACE is an element in an ACL that includes access control information.

ACI

Adjacent Channel Interference. ACI refers to interference or interruptions detected on a broadcasting channel, caused by too much power on an adjacent channel in the spectrum.

ACL

Access Control List. ACL is a common way of restricting certain types of traffic on a physical port.

Active Directory

Microsoft Active Directory. The directory server that stores information about a variety of things, such as organizations, sites, systems, users, shares, and other network objects or components. It also provides authentication and authorization mechanisms, and a framework within which related services can be deployed.

ActiveSync

Mobile data synchronization app developed by Microsoft that allows a mobile device to be synchronized with either a desktop or a server running compatible software products.

ad hoc network

An ad hoc network is a network composed of individual devices communicating with each other directly. Many ad hoc networks are Local Area Networks (LANs) where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point.

ADO

Active X Data Objects is a part of Microsoft Data Access Components (MDACs) that enables client applications to access data sources through an (Object Linking and Embedding Database) OLE DB provider. ADO supports key features for building client-server and Web-based applications.

ADP

Aruba Discovery Protocol. ADP is an Aruba proprietary Layer 2 protocol. It is used by the APs to obtain the IP address of the TFTP server from which it downloads the AP boot image.

AES

Advanced Encryption Standard. AES is an encryption standard used for encrypting and protecting electronic data. The AES encrypts and decrypts data in blocks of 128 bits (16 bytes), and can use keys of 128 bits, 192 bits, and 256 bits.

AIFSN

Arbitrary Inter-frame Space Number. AIFSN is set by the AP in beacon frames and probe responses. AIFS is a method of prioritizing a particular category of traffic over the other, for example prioritizing voice or video messages over email.

AirGroup

The application that allows the end users to register their personal mobile devices on a local network and define a group of friends or associates who are allowed to share them. AirGroup is primarily designed for colleges and other institutions. AirGroup uses zero configuration networking to allow Apple mobile devices, such as the AirPrint wireless printer service and the AirPlay mirroring service, to communicate over a complex access network topology.

AirWave Management Client

AirWave Management Client is a Windows software utility that enables client devices (such as a laptop) to act as passive RF sensors and augments the AirWave RAPIDS module.

ALE

Analytics and Location Engine. ALE gives visibility into everything the wireless network knows. This enables customers and partners to gain a wealth of information about the people on their premises. This can be very important for many different verticals and use cases. ALE includes a location engine that calculates associated and unassociated device location periodically using context streams, including RSSI readings, from WLAN controllers or Instant clusters.

ALG

Application Layer Gateway. ALG is a security component that manages application layer protocols such as SIP, FTP and so on.

AM

Air Monitor. AM is a mode of operation supported on wireless APs. When an AP operates in the Air Monitor mode, it enhances the wireless networks by collecting statistics, monitoring traffic, detecting intrusions, enforcing security policies, balancing wireless traffic load, self-healing coverage gaps, and more. However, clients cannot connect to APs operating in the AM mode.

AMON

Advanced Monitoring. AMON is used in Aruba WLAN deployments for improved network management, monitoring and diagnostic capabilities.

AMP

AirWave Management Platform. AMP is a network management system for configuring, monitoring, and upgrading wired and wireless devices on your network.

A-MPDU

Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.

A-MSDU

Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.

ANQP

Access Network Query Protocol. ANQP is a query and a response protocol for Wi-Fi hotspot services. ANQP includes information Elements (IEs) that can be sent from the AP to the client to identify the AP network and service provider. The IEs typically include information about the domain name of the AP operator, the IP addresses available at the AP, and information about potential roaming partners accessible through the AP. If the client responds with a request for a specific IE, the AP will send a Generic Advertisement Service (GAS) response frame with the configured ANQP IE information.

ANSI

American National Standards Institute. It refers to the ANSI compliance standards for products, systems, services, and processes.

API

Application Programming Interface. Refers to a set of functions, procedures, protocols, and tools that enable users to build application software.

app

Short form for application. It generally refers to the application that is downloaded and used on mobile devices.

ARM

Adaptive Radio Management. ARM dynamically monitors and adjusts the network to ensure that all users are allowed ready access. It enables full utilization of the available spectrum to support maximum number of users by intelligently choosing the best RF channel and transmit power for APs in their current RF environment.

ARP

Address Resolution Protocol. ARP is used for mapping IP network address to the hardware MAC address of a device.

Aruba Activate

Aruba Activate is a cloud-based service that helps provision your Aruba devices and maintain your inventory. Activate automates the provisioning process, allowing a single IT technician to easily and rapidly deploy devices throughout a distributed enterprise network.

ASCII

American Standard Code for Information Interchange. An ASCII code is a numerical representation of a character or an action.

band

Band refers to a specified range of frequencies of electromagnetic radiation.

BGP

Border Gateway Protocol. BGP is a routing protocol for exchanging data and information between different host gateways or autonomous systems on the Internet.

BLE

Bluetooth Low Energy. The BLE functionality is offered by Bluetooth® to enable devices to run for long durations with low power consumption.

BMC

Beacon Management Console. BMC manages and monitors beacons from the BLE devices. The BLE devices are used for location tracking and proximity detection.

BPDU

Bridge Protocol Data Unit. A BPDU is a data message transmitted across a local area network to detect loops in network topologies.

B-RAS

Broadband Remote Access Server. A B-RAS is a server that facilitates and converges traffic from multiple Internet traffic resources such as cable, DSL, Ethernet, or Broadband wireless.

BRE

Basic Regular Expression. The BRE syntax standards designed by the IEEE provides extension to the traditional Simple Regular Expressions syntax and allows consistency between utility programs such as grep, sed, and awk.

BSS

Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists of an AP and all its associated clients.

BSSID

Basic Service Set Identifier. The BSSID identifies a particular BSS within an area. In infrastructure BSS networks, the BSSID is the MAC address of the AP. In independent BSS or ad hoc networks, the BSSID is generated randomly.

BYOD

Bring Your Own Device. BYOD refers to the use of personal mobile devices within an enterprise network infrastructure.

CA

Certificate Authority or Certification Authority. Entity in a public key infrastructure system that issues certificates to clients. A certificate signing request received by the CA is converted into a certificate when the CA adds a signature generated with a private key. See digital certificate.

CAC

Call Admission Control. CAC regulates traffic volume in voice communications. CAC can also be used to ensure or maintain a certain level of audio quality in voice communications networks.

CALEA

Communications Assistance for Law Enforcement Act. To comply with the CALEA specifications and to allow lawful interception of Internet traffic by the law enforcement and intelligence agencies, the telecommunications carriers and manufacturers of telecommunications equipment are required to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

Campus AP

Campus APs are used in private networks where APs connect over private links (LAN, WLAN, WAN or MPLS) and terminate directly on controllers. Campus APs are deployed as part of the indoor campus solution in enterprise office buildings, warehouses, hospitals, universities, and so on.

captive portal

A captive portal is a web page that allows the users to authenticate and sign in before connecting to a public-access network. Captive portals are typically used by business centers, airports, hotel lobbies, coffee shops, and other venues that offer free Wi-Fi hotspots for the guest users.

CCA

Clear Channel Assessment. In wireless networks, the CCA method detects if a channel is occupied or clear, and determines if the channel is available for data transmission.

CDP

Cisco Discovery Protocol. CDP is a proprietary Data Link Layer protocol developed by Cisco Systems. CDP runs on Cisco devices and enables networking applications to learn about the neighboring devices directly connected to the network.

CDR

Call Detail Record. A CDR contains the details of a telephone or VoIP call, such as the origin and destination addresses of the call, the start time and end time of the call, any toll charges that were added through the network or charges for operator services, and so on.

CEF

Common Event Format. The CEF is a standard for the interoperability of event or log-generating devices and applications. The standard syntax for CEF includes a prefix and a variable extension formatted as key-value pairs.

CGI

Common Gateway Interface. CGI is a standard protocol for exchanging data between the web servers and executable programs running on a server to dynamically process web pages.

CHAP

Challenge Handshake Authentication Protocol. CHAP is an authentication scheme used by PPP servers to validate the identity of remote clients.

CIDR

Classless Inter-Domain Routing. CIDR is an IP standard for creating and allocating unique identifiers for networks and devices. The CIDR IP addressing scheme is used as a replacement for the older IP addressing scheme based on classes A, B, and C. With CIDR, a single IP address can be used to designate many unique IP addresses. A CIDR IP address ends with a slash followed by the IP network prefix, for example, 192.0.2.0/24.

ClearPass

ClearPass is an access management system for creating and enforcing policies across a network to all devices and applications. The ClearPass integrated platform includes applications such as Policy Manager, Guest, Onboard, OnGuard, Insight, Profile, QuickConnect, and so on.

ClearPass Guest

ClearPass Guest is a configurable ClearPass application for secure visitor network access management.

ClearPass Policy Manager

ClearPass Policy Manager is a baseline platform for policy management, AAA, profiling, network access control, and reporting. With ClearPass Policy Manager, the network administrators can configure and manage secure network access that accommodates requirements across multiple locations and multivendor networks, regardless of device ownership and connection method.

CLI

Command-Line Interface. A console interface with a command line shell that allows users to execute text input as commands and convert these commands to appropriate functions.

CN

Common Name. CN is the primary name used to identify a certificate.

CNA

Captive Network Assistant. CNA is a popup page shown when joining a network that has a captive portal.

CoA

Change of Authorization. The RADIUS CoA is used in the AAA service framework to allow dynamic modification of the authenticated, authorized, and active subscriber sessions.

CoS

Class of Service. CoS is used in data and voice protocols for classifying packets into different types of traffic (voice, video, or data) and setting a service priority. For example, voice traffic can be assigned a higher priority over email or HTTP traffic.

CPE

Customer Premises Equipment. It refers to any terminal or equipment located at the customer premises.

CPsec

Control Plane Security. CPsec is a secure form of communication between a controller and APs to protect the control plane communications. This is performed by means of using public-key self-signed certificates created by each master controller.

CPU

Central Processing Unit. A CPU is an electronic circuitry in a computer for processing instructions.

CRC

Cyclic Redundancy Check. CRC is a data verification method for detecting errors in digital data during transmission, storage, or retrieval.

CRL

Certificate Revocation List. CRL is a list of revoked certificates maintained by a certification authority.

cryptobinding

Short for cryptographic binding. A procedure in a tunneled EAP method that binds together the tunnel protocol and the tunneled authentication methods, ensuring the relationship between a collection of data assets. Cryptographic binding focuses on protecting the server; mutual cryptographic binding protects both peer and server.

CSA

Channel Switch Announcement. The CSA element enables an AP to advertise that it is switching to a new channel before it begins transmitting on that channel. This allows the clients, which support CSA, to transition to the new channel with minimal downtime.

CSMA/CA

Carrier Sense Multiple Access / Collision Avoidance. CSMA/CA is a protocol for carrier transmission in networks using the 802.11 standard. CSMA/CA aims to prevent collisions by listening to the broadcasting nodes, and informing devices not to transmit any data until the broadcasting channel is free.

CSR

Certificate Signing Request. In PKI systems, a CSR is a message sent from an applicant to a CA to apply for a digital identity certificate.

CSV

Comma-Separated Values. A file format that stores tabular data in the plain text format separated by commas.

CTS

Clear to Send. The CTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See RTS.

CW

Contention Window. In QoS, CW refers to a window set for access categories based on the type of traffic. Based on the type and volume of the traffic, the minimum and maximum values can be calculated to provide a wider window when necessary.

DAI

Dynamic ARP inspection. A security feature that validates ARP packets in a network.

DAS

Distributed Antenna System. DAS is a network of antenna nodes strategically placed around a geographical area or structure for additional cellular coverage.

dB

Decibel. Unit of measure for sound or noise and is the difference or ratio between two signal levels.

dBm

Decibel-Milliwatts. dBm is a logarithmic measurement (integer) that is typically used in place of mW to represent receive-power level. AMP normalizes all signals to dBm, so that it is easy to evaluate performance between various vendors.

DCB

Data Center Bridging. DCB is a collection of standards developed by IEEE for creating a converged data center network using Ethernet.

DCE

Data Communication Equipment. DCE refers to the devices that establish, maintain, and terminate communication network sessions between a data source and its destination.

DCF

Distributed Coordination Function. DCF is a protocol that uses carrier sensing along with a four-way handshake to maximize the throughput while preventing packet collisions.

DDMO

Distributed Dynamic Multicast Optimization. DDMO is similar to Dynamic Multicast Optimization (DMO) where the multicast streams are converted into unicast streams on the AP instead of the controller, to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DES

Data Encryption Standard. DES is a common standard for data encryption and a form of secret key cryptography, which uses only one key for encryption and decryption.

designated router

Designated router refers to a router interface that is elected to originate network link advertisements for networks using the OSPF protocol.

destination NAT

Destination Network Address Translation. Destination NAT is a process of translating the destination IP address of an end route packet in a network. Destination NAT is used for redirecting the traffic destined to a virtual host to the real host, where the virtual host is identified by the destination IP address and the real host is identified by the translated IP address.

DFS

Dynamic Frequency Selection. DFS is a mandate for radio systems operating in the 5 GHz band to be equipped with means to identify and avoid interference with RADAR systems.

DFT

Discrete Fourier Transform. DFT converts discrete-time data sets into a discrete-frequency representation. See FFT.

DHCP

Dynamic Host Configuration Protocol. A network protocol that enables a server to automatically assign an IP address to an IP-enabled device from a defined range of numbers configured for a given network.

DHCP snooping

DHCP snooping enables the switch to monitor and control DHCP messages received from untrusted devices that are connected to the switch.

digital certificate

A digital certificate is an electronic document that uses a digital signature to bind a public key with an identity—information such as the name of a person or an organization, address, and so forth.

Digital wireless pulse

A wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance. Ultra Wideband radio can carry a huge amount of data over a distance up to 230 ft at very low power (less than 0.5 mW), and has the ability to carry signals through doors and other obstacles that tend to reflect signals at more limited bandwidths and a higher power.

Disconnect-Ack

Disconnect-Ack is a NAS response packet to a Disconnect-Request, which indicates that the session was disconnected.

Disconnect-Nak

Disconnect-Nak is NAS response packet to a Disconnect-Request, which indicates that the session was not disconnected.

Disconnect-Request

Disconnect-Request is a RADIUS packet type sent to a NAS requesting that a user or session be disconnected.

distribution certificate

Distribution certificate is used for digitally signing iOS mobile apps to enable enterprise app distribution. It verifies the identity of the app publisher.

DLNA

Digital Living Network Alliance. DLNA is a set of interoperability guidelines for sharing digital media among multimedia devices.

DMO

Dynamic Multicast Optimization. DMO is a process of converting multicast streams into unicast streams over a wireless link to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DN

Distinguished Name. A series of fields in a digital certificate that, taken together, constitute the unique identity of the person or device that owns the digital certificate. Common fields in a DN include country, state, locality, organization, organizational unit, and the “common name”, which is the primary name used to identify the certificate.

DNS

Domain Name System. A DNS server functions as a phone book for the intranet and Internet users. It converts human-readable computer host names into IP addresses and IP addresses into host names. It stores several records for a domain name such as an address 'A' record, name server (NS), and mail exchanger (MX) records. The Address 'A' record is the most important record that is stored in a DNS server, because it provides the required IP address for a network peripheral or element.

DOCSIS

Data over Cable Service Interface Specification. A telecommunication standard for Internet access through cable modem.

DoS

Denial of Service. DoS is any type of attack where the attackers send excessive messages to flood traffic and thereby preventing the legitimate users from accessing the service.

DPD

Dead Peer Detection. A method used by the network devices to detect the availability of the peer devices.

DPI

Deep Packet Inspection. DPI is an advanced method of network packet filtering that is used for inspecting data packets exchanged between the devices and systems over a network. DPI functions at the Application layer of the Open Systems Interconnection (OSI) reference model and enables users to identify, categorize, track, reroute, or stop packets passing through a network.

DRT

Downloadable Regulatory Table. The DRT feature allows new regulatory approvals to be distributed for APs without a software upgrade or patch.

DS

Differentiated Services. The DS specification aims to provide uninterrupted quality of service by managing and controlling the network traffic, so that certain types of traffic get precedence.

DSCP

Differentiated Services Code Point. DSCP is a 6-bit packet header value used for traffic classification and priority assignment.

DSL

Digital Subscriber Line. The DSL technology allows the transmission of digital data over telephone lines. A DSL modem is a device used for connecting a computer or router to a telephone line that offers connectivity to the Internet.

DSSS

Direct-Sequence Spread Spectrum. DSSS is a modulation technique used for reducing overall signal interference. This technique multiplies the original data signal with a pseudo random noise spreading code. Spreading of this signal makes the resulting wideband channel more noisy, thereby increasing

the resistance to interference. See FHSS.

DST

Daylight Saving Time. DST is also known as summer time that refers to the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

DTE

Data Terminal Equipment. DTE refers to a device that converts user information into signals or re-converts the received signals.

DTIM

Delivery Traffic Indication Message. DTIM is a kind of traffic indication map. A DTIM interval determines when the APs must deliver broadcast and multicast frames to their associated clients in power save mode.

DTLS

Datagram Transport Layer Security. DTLS communications protocol provides communications security for datagram protocols.

dynamic authorization

Dynamic authorization refers to the ability to make changes to a visitor account's session while it is in progress. This might include disconnecting a session or updating some aspect of the authorization for the session.

dynamic NAT

Dynamic Network Address Translation. Dynamic NAT maps multiple public IP addresses and uses these addresses with an internal or private IP address. Dynamic NAT helps to secure a network by masking the internal configuration of a private network.

EAP

Extensible Authentication Protocol. An authentication protocol for wireless networks that extends the methods used by the PPP, a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

EAP-FAST

EAP – Flexible Authentication Secure Tunnel (tunneled).

EAP-GTC

EAP – Generic Token Card. (non-tunneled).

EAP-MD5

EAP – Method Digest 5. (non-tunneled).

EAP-MSCHAP

EAP Microsoft Challenge Handshake Authentication Protocol.

EAP-MSCHAPv2

EAP Microsoft Challenge Handshake Authentication Protocol Version 2.

EAPoL

Extensible Authentication Protocol over LAN. A network port authentication protocol used in IEEE 802.1X standards to provide a generic network sign-on to access network resources.

EAP-PEAP

EAP-Protected EAP. A widely used protocol for securely transporting authentication data across a network (tunneled).

EAP-PWD

EAP-Password. EAP-PWD is an EAP method that uses a shared password for authentication.

EAP-TLS

EAP-Transport Layer Security. EAP-TLS is a certificate-based authentication method supporting mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints. See RFC 5216.

EAP-TTLS

EAP-Tunneled Transport Layer Security. EAP-TTLS is an EAP method that encapsulates a TLS session, consisting of a handshake phase and a data phase. See RFC 5281.

ECC

Elliptical Curve Cryptography or Error correcting Code memory. Elliptical Curve Cryptography is a public-key encryption technique that is based on elliptic curve theory used for creating faster, smaller, and more efficient cryptographic keys. Error Correcting Code memory is a type of computer data storage that can detect and correct the most common kinds of internal data corruption. ECC memory is used in most computers where data corruption cannot be tolerated under any circumstances, such as for scientific or financial computing.

ECDSA

Elliptic Curve Digital Signature Algorithm. ECDSA is a cryptographic algorithm that supports the use of public or private key pairs for encrypting and decrypting information.

EDCA

Enhanced Distributed Channel Access. The EDCA function in the IEEE 802.11e Quality of Service standard supports differentiated and distributed access to wireless medium based on traffic priority and Access Category types. See WMM and WME.

EIGRP

Enhanced Interior Gateway Routing Protocol. EIGRP is a routing protocol used for automating routing decisions and configuration in a network.

EIRP

Effective Isotropic Radiated Power or Equivalent Isotropic Radiated Power. EIRP refers to the output power generated when a signal is concentrated into a smaller area by the Antenna.

ESI

External Services Interface. ESI provides an open interface for integrating security solutions that solve interior network problems such as viruses, worms, spyware, and corporate compliance.

ESS

Extended Service Set. An ESS is a set of one or more interconnected BSSs that form a single sub network.

ESSID

Extended Service Set Identifier. ESSID refers to the ID used for identifying an extended service set.

Ethernet

Ethernet is a network protocol for data transmission over LAN.

EULA

End User License Agreement. EULA is a legal contract between a software application publisher or author and the users of the application.

FCC

Federal Communications Commission. FCC is a regulatory body that defines standards for the interstate and international communications by radio, television, wire, satellite, and cable.

FFT

Fast Fourier Transform. FFT is a frequency analysis mechanism that aims at faster conversion of a discrete signal in time domain into a discrete frequency domain representation. See also DFT.

FHSS

Frequency Hopping Spread Spectrum. FHSS is transmission technique that allows modulation and transmission of a data signal by rapidly switching a carrier among many frequency channels in a random but predictable sequence. See also DSSS.

FIB

Forwarding Information Base. FIB is a forwarding table that maps MAC addresses to ports. FIB is used in network bridging, routing, and similar functions to identify the appropriate interface for forwarding packets.

FIPS

Federal Information Processing Standards. FIPS refers to a set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies, and by government contractors and vendors who work with these agencies.

firewall

Firewall is a network security system used for preventing unauthorized access to or from a private network.

FQDN

Fully Qualified Domain Name. FQDN is a complete domain name that identifies a computer or host on the Internet.

FQLN

Fully Qualified Location Name. FQLN is a device location identifier in the format: AName.Floor.Building.Campus.

frequency allocation

Use of radio frequency spectrum as regulated by governments.

FSPL

Free Space Path Loss. FSPL refers to the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space (usually air), with no obstacles nearby to cause reflection or diffraction.

FTP

File Transfer Protocol. A standard network protocol used for transferring files between a client and server on a computer network.

GARP

Generic Attribute Registration Protocol. GARP is a LAN protocol that allows the network nodes to register and de-register attributes, such as network addresses, with each other.

GAS

Generic Advertisement Service. GAS is a request-response protocol, which provides Layer 2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps in determining a wireless network infrastructure before associating clients, and allows clients to send queries to multiple 802.11 networks in parallel.

gateway

Gateway is a network node that allows traffic to flow in and out of the network.

Gbps

Gigabits per second.

GBps

Gigabytes per second.

GET

GET refers HTTP request method or an SNMP operation method. The GET HTTP request method submits data to be processed to a specified resource. The GET SNMP operation method obtains information from the Management Information Base (MIB).

GHz

Gigahertz.

GMT

Greenwich Mean Time. GMT refers to the mean solar time at the Royal Observatory in Greenwich, London. GMT is the same as Coordinated Universal Time (UTC) standard, written as an offset of UTC +/- 00:00.

goodput

Goodput is the application level throughput that refers to the ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes.

GPS

Global Positioning System. A satellite-based global navigation system.

GRE

Generic Routing Encapsulation. GRE is an IP encapsulation protocol that is used to transport packets over a network.

GTC

Generic Token Card. GTC is a protocol that can be used as an alternative to MSCHAPv2 protocol. GTC allows authentication to various authentication databases even in cases where MSCHAPv2 is not supported by the database.

GVRP

GARP VLAN Registration Protocol or Generic VLAN Registration Protocol. GARP is an IEEE 802.1Q-compliant protocol that facilitates VLAN registration and controls VLANs within a larger network.

H2QP

Hotspot 2.0 Query Protocol.

hot zone

Wireless access area created by multiple hotspots that are located in close proximity to one another. Hot zones usually combine public safety APs with public hotspots.

hotspot

Hotspot refers to a WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can look up a local hotspot, contact it, and get connected through its network to reach the Internet.

HSPA

High-Speed Packet Access.

HT

High Throughput. IEEE 802.11n is an HT WLAN standard that aims to achieve physical data rates of close to 600 Mbps on the 2.4 GHz and 5 GHz bands.

HTTP

Hypertext Transfer Protocol. The HTTP is an application protocol to transfer data over the web. The HTTP protocol defines how messages are formatted and transmitted, and the actions that the w servers and browsers should take in response to various commands.

HTTPS

Hypertext Transfer Protocol Secure. HTTPS is a variant of the HTTP that adds a layer of security on the data in transit through a secure socket layer or transport layer security protocol connection.

IAS

Internet Authentication Service. IAS is a component of Windows Server operating systems that provides centralized user authentication, authorization, and accounting.

ICMP

Internet Control Message Protocol. ICMP is an error reporting protocol. It is used by network devices such as routers, to send error messages and operational information to the source IP address when network problems prevent delivery of IP packets.

IDS

Intrusion Detection System. IDS monitors a network or systems for malicious activity or policy violations and reports its findings to the management system deployed in the network.

IEEE

Institute of Electrical and Electronics Engineers.

IGMP

Internet Group Management Protocol. Communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.

IGMP snooping

IGMP snooping prevents multicast flooding on Layer 2 network by treating multicast traffic as broadcast traffic. Without IGMP snooping, all streams could be flooded to all ports on that VLAN. When multicast flooding occurs, end-hosts that happen to be in the same VLAN would receive all the streams only to be discarded without snooping.

IGP

Interior Gateway Protocol. IGP is used for exchanging routing information between gateways within an autonomous system (for example, a system of corporate local area networks).

IGRP

Interior Gateway Routing Protocol. IGRP is a distance vector interior routing protocol used by routers to exchange routing data within an autonomous system.

IKE

Internet Key Exchange. IKE is a key management protocol used with IPsec protocol to establish a secure communication channel. IKE provides additional feature, flexibility, and ease of configuration for IPsec standard.

IKEv1

Internet Key Exchange version 1. IKEv1 establishes a secure authenticated communication channel by using either the pre-shared key (shared secret), digital signatures, or public key encryption. IKEv1 operates in Main and Aggressive modes. See RFC 2409.

IKEv2

Internet Key Exchange version 2. IKEv2 uses the secure channel established in Phase 1 to negotiate Security Associations on behalf of services such as IPsec. IKEv2 uses pre-shared key and Digital Signature for authentication. See RFC 4306.

IoT

Internet of Things. IoT refers to the internetworking of devices that are embedded with electronics, software, sensors, and network connectivity features allowing data exchange over the Internet.

IPM

Intelligent Power Monitoring. IPM is a feature supported on certain APs that actively measures the power utilization of an AP and dynamically adapts to the power resources.

IPS

Intrusion Prevention System. The IPS monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, log the information, attempt to block the activity, and report it.

IPsec

Internet Protocol security. IPsec is a protocol suite for secure IP communications that authenticates and encrypts each IP packet in a communication session.

IPSG

Internet Protocol Source Guard. IPSG restricts IP address from untrusted interface by filtering traffic based on list of addresses in the DHCP binding database or manually configured IP source bindings. It prevents IP spoofing attacks.

IrDA

An industry-sponsored organization set up in 1993 to create international standards for the hardware and software used in infrared communication links. In this special form of radio transmission, a focused ray of light in the infrared frequency spectrum, measured in terahertz (THz), or trillions of hertz (cycles per second), is modulated with information and sent from a transmitter to a receiver over a relatively short distance.

ISAKMP

Internet Security Association and Key Management Protocol. ISAKMP is used for establishing Security Associations and cryptographic keys in an Internet environment.

ISP

Internet Service Provider. An ISP is an organization that provides services for accessing and using the Internet.

JSON

JavaScript Object Notation. JSON is an open-standard, language-independent, lightweight data-interchange format used to transmit data objects consisting of attribute-value pairs. JSON uses a "self-describing" text format that is easy for humans to read and write, and that can be used as a data format by any programming language.

Kbps

Kilobits per second.

KBps

Kilobytes per second.

keepalive

Signal sent at periodic intervals from one device to another to verify that the link between the two devices is working. If no reply is received, data will be sent by a different path until the link is restored. A keepalive can also be used to indicate that the connection should be preserved so that the receiving device does not consider it timed out and drop it.

L2TP

Layer-2 Tunneling Protocol. L2TP is a networking protocol used by the ISPs to enable VPN operations.

LACP

Link Aggregation Control Protocol. LACP is used for the collective handling of multiple physical ports that can be seen as a single channel for network traffic purposes.

LAG

Link Aggregation Group . A LAG combines a number of physical ports together to make a single high-bandwidth data path. LAGs can connect two switches to provide a higher-bandwidth connection to a public network.

LAN

Local Area Network. A LAN is a network of connected devices within a distinct geographic area such as an office or a commercial establishment and share a common communications line or wireless link to a server.

LCD

Liquid Crystal Display. LCD is the technology used for displays in notebook and other smaller computers. Like LED and gas-plasma technologies, LCDs allow displays to be much thinner than the cathode ray tube technology.

LDAP

Lightweight Directory Access Protocol. LDAP is a communication protocol that provides the ability to access and maintain distributed directory information services over a network.

LDPC

Low-Density Parity-Check. LDPC is a method of transmitting a message over a noisy transmission channel using a linear error correcting code. An LDPC is constructed using a sparse bipartite graph.

LEAP

Lightweight Extensible Authentication Protocol. LEAP is a Cisco proprietary version of EAP used in wireless networks and Point-to-Point connections.

LED

Light Emitting Diode. LED is a semiconductor light source that emits light when an electric current passes through it.

LEEF

Log Event Extended Format. LEEF is a type of customizable syslog event format. An extended log file contains a sequence of lines containing ASCII characters terminated by either the sequence LF or CRLF.

LI

Lawful Interception. LI refers to the procedure of obtaining communications network data by the Law Enforcement Agencies for the purpose of analysis or evidence.

LLDP

Link Layer Discovery Protocol. LLDP is a vendor-neutral link layer protocol in the Internet Protocol suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, which is principally a wired Ethernet.

LLDP-MED

LLDP–Media Endpoint Discovery. LLDP-MED facilitates information sharing between endpoints and network infrastructure devices.

LMS

Local Management Switch. In multi-controller networks, each controller acts as an LMS and terminates user traffic from the APs, processes, and forwards the traffic to the wired network.

LNS

L2TP Network Server. LNS is an equipment that connects to a carrier and handles the sessions from broadband lines. It is also used for dial-up and mobile links. LNS handles authentication and routing of the IP addresses. It also handles the negotiation of the link with the equipment and establishes a session.

LTE

Long Term Evolution. LTE is a 4G wireless communication standard that provides high-speed wireless communication for mobile phones and data terminals. See 4G.

MAB

MAC Authentication Bypass. Endpoints such as network printers, Ethernet-based sensors, cameras, and wireless phones do not support 802.1X authentication. For such endpoints, MAC Authentication Bypass mechanism is used. In this method, the MAC address of the endpoint is used to authenticate the endpoint.

MAC

Media Access Control. A MAC address is a unique identifier assigned to network interfaces for communications on a network.

MAM

Mobile Application Management. MAM refers to software and services used to secure, manage, and distribute mobile applications used in enterprise settings on mobile devices like smartphones and tablet computers. Mobile Application Management can apply to company-owned mobile devices as well as BYOD.

Mbps

Megabits per second

MBps

Megabytes per second

MCS

Modulation and Coding Scheme. MCS is used as a parameter to determine the data rate of a wireless connection for high throughput.

MD4

Message Digest 4. MD4 is an earlier version of MD5 and is an algorithm used to verify data integrity through the creation of a 128-bit message digest from data input.

MD5

Message Digest 5. The MD5 algorithm is a widely used hash function producing a 128-bit hash value from the data input.

MDAC

Microsoft Data Access Components. MDAC is a framework of interrelated Microsoft technologies that provides a standard database for Windows OS.

MDM

Mobile Device Management. MDM is an administrative software to manage, monitor, and secure mobile devices of the employees in a network.

mDNS

Multicast Domain Name System. mDNS provides the ability to perform DNS-like operations on the local link in the absence of any conventional unicast DNS server. The mDNS protocol uses IP multicast User Datagram Protocol (UDP) packets, and is implemented by the Apple Bonjour and Linux NSS-mDNS services. mDNS works in conjunction with DNS Service Discovery (DNS-SD), a companion zero-configuration technique specified. See RFC 6763.

MFA

Multi-factor Authentication. MFA lets you require multiple factors, or proofs of identity, when authenticating a user. Policy configurations define how often multi-factor authentication will be required, or conditions that will trigger it.

MHz

Megahertz

MIB

Management Information Base. A hierarchical database used by SNMP to manage the devices being monitored.

microwave

Electromagnetic energy with a frequency higher than 1 GHz, corresponding to wavelength shorter than 30 centimeters.

MIMO

Multiple Input Multiple Output. An antenna technology for wireless communications in which multiple antennas are used at both source (transmitter) and destination (receiver). The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed.

MISO

Multiple Input Single Output. An antenna technology for wireless communications in which multiple antennas are used at the source (transmitter). The antennas are combined to minimize errors and optimize data speed. The destination (receiver) has only one antenna.

MLD

Multicast Listener Discovery. A component of the IPv6 suite. It is used by IPv6 routers for discovering multicast listeners on a directly attached link.

MPDU

MAC Protocol Data Unit. MPDU is a message exchanged between MAC entities in a communication system based on the layered OSI model.

MPLS

Multiprotocol Label Switching. The MPLS protocol speeds up and shapes network traffic flows.

MPPE

Microsoft Point-to-Point Encryption. A method of encrypting data transferred across PPP-based dial-up connections or PPTP-based VPN connections.

MS-CHAP

Microsoft Challenge Handshake Authentication Protocol. MS-CHAP is Password-based, challenge-response, mutual authentication protocol that uses MD4 and DES encryption.

MS-CHAPv1

Microsoft Challenge Handshake Authentication Protocol version 1. MS-CHAPv1 extends the user authentication functionality provided on Windows networks to remote workstations. MS-CHAPv1 supports only one-way authentication.

MS-CHAPv2

Microsoft Challenge Handshake Authentication Protocol version 2. MS-CHAPv2 is an enhanced version of the MS-CHAP protocol that supports mutual authentication.

MSS

Maximum Segment Size. MSS is a parameter of the options field in the TCP header that specifies the largest amount of data, specified in bytes, that a computer or communications device can receive in a single TCP segment.

MSSID

Mesh Service Set Identifier. MSSID is the SSID used by the client to access a wireless mesh network.

MSTP

Multiple Spanning Tree Protocol. MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree.

MTU

Maximum Transmission Unit. MTU is the largest size packet or frame specified in octets (eight-bit bytes) that can be sent in networks such as the Internet.

MU-MIMO

Multi-User Multiple-Input Multiple-Output. MU-MIMO is a set of multiple-input and multiple-output technologies for wireless communication, in which users or wireless terminals with one or more antennas communicate with each other.

MVRP

Multiple VLAN Registration Protocol. MVRP is a Layer 2 network protocol used for automatic configuration of VLAN information on switches.

mW

milliWatts. mW is 1/1000 of a Watt. It is a linear measurement (always positive) that is generally used to represent transmission.

NAC

Network Access Control. NAC is a computer networking solution that uses a set of protocols to define and implement a policy that describes how devices can secure access to network nodes when they initially attempt to connect to a network.

NAD

Network Access Device. NAD is a device that automatically connects the user to the preferred network, for example, an AP or an Ethernet switch.

NAK

Negative Acknowledgement. NAK is a response indicating that a transmitted message was received with errors or it was corrupted, or that the receiving end is not ready to accept transmissions.

NAP

Network Access Protection. The NAP feature in the Windows Server allows network administrators to define specific levels of network access based on identity, groups, and policy compliance. The NAP Agent is a service that collects and manages health information for NAP client computers. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

NAS

Network Access Server. NAS provides network access to users, such as a wireless AP, network switch, or dial-in terminal server.

NAT

Network Address Translation. NAT is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

NetBIOS

Network Basic Input/Output System. A program that lets applications on different computers communicate within a LAN.

netmask

Netmask is a 32-bit mask used for segregating IP address into subnets. Netmask defines the class and range of IP addresses.

NFC

Near-Field Communication. NFC is a short-range wireless connectivity standard (ECMA-340, ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they touch or are brought closer (within a few centimeters of distance). The standard specifies a way for the devices to establish a peer-to-peer (P2P) network to exchange data.

NIC

Network Interface Card. NIC is a hardware component that allows a device to connect to the network.

Nmap

Network Mapper. Nmap is an open-source utility for network discovery and security auditing. Nmap uses IP packets to determine such things as the hosts available on a network and their services, operating systems and versions, types of packet filters/firewalls, and so on.

NMI

Non-Maskable Interrupt. NMI is a hardware interrupt that standard interrupt-masking techniques in the system cannot ignore. It typically occurs to signal attention for non-recoverable hardware errors.

NMS

Network Management System. NMS is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework.

NOE

New Office Environment. NOE is a proprietary VoIP protocol designed by Alcatel-Lucent Enterprise.

NTP

Network Time Protocol. NTP is a protocol for synchronizing the clocks of computers over a network.

OAuth

Open Standard for Authorization. OAuth is a token-based authorization standard that allows websites or third-party applications to access user information, without exposing the user credentials.

OCSP

Online Certificate Status Protocol. OCSP is used for determining the current status of a digital certificate without requiring a CRL.

OFDM

Orthogonal Frequency Division Multiplexing. OFDM is a scheme for encoding digital data on multiple carrier frequencies.

OID

Object Identifier. An OID is an identifier used to name an object. The OIDs represent nodes or managed objects in a MIB hierarchy. The OIDs are designated by text strings and integer sequences and are formally defined as per the ASN.1 standard.

OKC

Opportunistic Key Caching. OKC is a technique available for authentication between multiple APs in a network where those APs are under common administrative control. Using OKC, a station roaming to any AP in the network will not have to complete a full authentication exchange, but will instead just perform the 4-way handshake to establish transient encryption keys.

onboarding

The process of preparing a device for use on an enterprise network, by creating the appropriate access credentials and setting up the network connection parameters.

OpenFlow

OpenFlow is an open communications interface between control plane and the forwarding layers of a network.

OpenFlow agent

OpenFlow agent. OpenFlow is a software module in Software-Defined Networking (SDN) that allows the abstraction of any legacy network element, so that it can be integrated and managed by the SDN controller. OpenFlow runs on network devices such as switches, routers, wireless controllers, and APs.

Optical wireless

Optical wireless is combined use of conventional radio frequency wireless and optical fiber for telecommunication. Long-range links are provided by using optical fibers; the links from the long-range endpoints to end users are accomplished by RF wireless or laser systems. RF wireless at Ultra High Frequencies and microwave frequencies can carry broadband signals to individual computers at substantial data speeds.

OSI

Open Systems Interconnection. OSI is a reference model that defines a framework for communication between the applications in a network.

OSPF

Open Shortest Path First. OSPF is a link-state routing protocol for IP networks. It uses a link-state routing algorithm and falls into the group of interior routing protocols that operates within a single Autonomous System (AS).

OSPFv2

Open Shortest Path First version 2. OSPFv2 is the version 2 of the link-state routing protocol, OSPF. See RFC 2328.

OUI

Organizationally Unique Identifier. Synonymous with company ID or vendor ID, an OUI is a 24-bit, globally unique assigned number, referenced by various standards. The first half of a MAC address is OUI.

OVA

Open Virtualization Archive. OVA contains a compressed installable version of a virtual machine.

OVF

Open Virtualization Format. OVF is a specification that describes an open-standard, secure, efficient, portable and extensible format for packaging and distributing software for virtual machines.

PAC

Protected Access Credential. PAC is distributed to clients for optimized network authentication. These credentials are used for establishing an authentication tunnel between the client and the authentication server.

PAP

Password Authentication Protocol. PAP validates users by password. PAP does not encrypt passwords for transmission and is thus considered insecure.

PAPI

Process Application Programming Interface. PAPI controls channels for ARM and Wireless Intrusion Detection System (WIDS) communication to the master controller. A separate PAPI control channel connects to the local controller where the SSID tunnels terminate.

PBR

Policy-based Routing. PBR provides a flexible mechanism for forwarding data packets based on policies configured by a network administrator.

PDU

Power Distribution Unit or Protocol Data Unit. Power Distribution Unit is a device that distributes electric power to the networking equipment located within a data center. Protocol Data Unit contains protocol control information that is delivered as a unit among peer entities of a network.

PEAP

Protected Extensible Authentication Protocol. PEAP is a type of EAP communication that addresses security issues associated with clear text EAP transmissions by creating a secure channel encrypted and protected by TLS.

PEF

Policy Enforcement Firewall. PEF provides context-based controls to enforce application-layer security and prioritization.

PFS

Perfect Forward Secrecy. PFS refers to the condition in which a current session key or long-term private key does not compromise the past or subsequent keys.

PHB

Per-hop behavior. PHB is a term used in DS or MPLS. It defines the policy and priority applied to a packet when traversing a hop (such as a router) in a DiffServ network.

PIM

Protocol-Independent Multicast. PIM refers to a family of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the Internet.

PIN

Personal Identification Number. PIN is a numeric password used to authenticate a user to a system.

PKCS#n

Public-key cryptography standard n. PKCS#n refers to a numbered standard related to topics in cryptography, including private keys (PKCS#1), digital certificates (PKCS#7), certificate signing requests (PKCS#10), and secure storage of keys and certificates (PKCS#12).

PKI

Public Key Infrastructure. PKI is a security technology based on digital certificates and the assurances provided by strong cryptography. See also certificate authority, digital certificate, public key, private key.

PLMN

Public Land Mobile Network. PLMS is a network established and operated by an administration or by a Recognized Operating Agency for the specific purpose of providing land mobile telecommunications services to the public.

PMK

Pairwise Master Key. PMK is a shared secret key that is generated after PSK or 802.1X authentication.

PoE

Power over Ethernet. PoE is a technology for wired Ethernet LANs to carry electric power required for the device in the data cables. The IEEE 802.3af PoE standard provides up to 15.4 W of power on each port.

PoE+

Power over Ethernet+. PoE+ is an IEEE 802.3at standard that provides 25.5W power on each port.

POST

Power On Self Test. An HTTP request method that requests data from a specified resource.

PPP

Point-to-Point Protocol. PPP is a data link (layer 2) protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption, and compression.

PPPoE

Point-to-Point Protocol over Ethernet. PPPoE is a method of connecting to the Internet, typically used with DSL services, where the client connects to the DSL modem.

PPTP

Point-to-Point Tunneling Protocol. PPTP is a method for implementing virtual private networks. It uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

private key

The part of a public-private key pair that is always kept private. The private key encrypts the signature of a message to authenticate the sender. The private key also decrypts a message that was encrypted with the public key of the sender.

PRNG

Pseudo-Random Number Generator. PRNG is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers.

PSK

Pre-shared key. A unique shared secret that was previously shared between two parties by using a secure channel. This is used with WPA security, which requires the owner of a network to provide a passphrase to users for network access.

PSU

Power Supply Unit. PSU is a unit that supplies power to an equipment by converting mains AC to low-voltage regulated DC power.

public key

The part of a public-private key pair that is made public. The public key encrypts a message and the message is decrypted with the private key of the recipient.

PVST

Per-VLAN Spanning Tree. PVST provides load balancing of VLANs across multiple ports resulting in optimal usage of network resources.

PVST+

Per-VLAN Spanning Tree+. PVST+ is an extension of the PVST standard that uses the 802.1Q trunking technology.

QoS

Quality of Service. It refers to the capability of a network to provide better service and performance to a specific network traffic over various technologies.

RA

Router Advertisement. The RA messages are sent by the routers in the network when the hosts send multicast router solicitation to the multicast address of all routers.

RADAR

Radio Detection and Ranging. RADAR is an object-detection system that uses radio waves to determine the range, angle, or velocity of objects.

RADIUS

Remote Authentication Dial-In User Service. An Industry-standard network access protocol for remote authentication. It allows authentication, authorization, and accounting of remote users who want to access network resources.

RAM

Random Access Memory.

RAPIDS

Rogue Access Point identification and Detection System. An AMP module that is designed to identify and locate wireless threats by making use of all of the information available from your existing infrastructure.

RARP

Reverse Address Resolution Protocol. RARP is a protocol used by a physical machine in a local area network for determining the IP address from the ARP table or cache of the gateway server.

Regex

Regular Expression. Regex refers to a sequence of symbols and characters defining a search pattern.

Registration Authority

Type of Certificate Authority that processes certificate requests. The Registration Authority verifies that requests are valid and comply with certificate policy, and authenticates the user's identity. The Registration Authority then forwards the request to the Certificate Authority to sign and issue the certificate.

Remote AP

Remote AP. Remote AP extends the corporate network to users working from home, or at temporary work sites.

REST

Representational State Transfer. REST is a simple and stateless architecture that the web services use for providing interoperability between computer systems on the Internet. In a RESTful web service, requests made to the URI of a resource will elicit a response that may be in XML, HTML, JSON or some other defined format.

RF

Radio Frequency. RF refers to the electromagnetic wave frequencies within a range of 3 kHz to 300 GHz, including the frequencies used for communications or RADAR signals.

RFC

Request For Comments. RFC is a commonly used format for the Internet standards documents.

RFID

Radio Frequency Identification. RFID uses radio waves to automatically identify and track the information stored on a tag attached to an object.

RIP

Routing Information Protocol. RIP prevents the routing loops by limiting the number of hops allowed in a path from source to destination.

RJ45

Registered Jack 45. RJ45 is a physical connector for network cables.

RMON

Remote Monitoring. RMON provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed LANs.

RoW

Rest of World. RoW or RW is an operating country code of a device.

RSA

Rivest, Shamir, Adleman. RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

RSSI

Received Signal Strength Indicator. RSSI is a mechanism by which RF energy is measured by the circuitry on a wireless NIC (0-255). The RSSI is not standard across vendors. Each vendor determines its own RSSI scale/values.

RSTP

Rapid Spanning Tree Protocol. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this.

RTCP

RTP Control Protocol. RTCP provides out-of-band statistics and control information for an Real-Time Transport Protocol session.

RTLS

Real-Time Location Systems. RTLS automatically identifies and tracks the location of objects or people in real time, usually within a building or other contained area.

RTP

Real-Time Transport Protocol. RTP is a network protocol used for delivering audio and video over IP networks.

RTS

Request to Send. RTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See CTS.

RTSP

Real Time Streaming Protocol. RTSP is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.

RVI

Routed VLAN Interface. RVI is a switch interface that forwards packets between VLANs.

RW

Rest of World. RoW or RW is an operating country code of a device.

SA

Security Association. SA is the establishment of shared security attributes between two network entities to support secure communication.

SAML

Security Assertion Markup Language. SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication.

SCEP

Simple Certificate Enrollment Protocol. SCEP is a protocol for requesting and managing digital certificates.

SCP

Secure Copy Protocol. SCP is a network protocol that supports file transfers between hosts on a network.

SCSI

Small Computer System Interface. SCSI refers to a set of interface standards for physical connection and data transfer between a computer and the peripheral devices such as printers, disk drives, CD-ROM, and so on.

SDN

Software-Defined Networking. SDN is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of the modern data center.

SDR

Server Derivation Rule. An SDR refers to a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on the rules defined under a server group. The SDRs override the default authentication roles and VLANs defined in the AAA and Virtual AP profiles.

SDU

Service Data Unit. SDU is a unit of data that has been passed down from an OSI layer to a lower layer and that has not yet been encapsulated into a PDU by the lower layer.

SD-WAN

Software-Defined Wide Area Network. SD-WAN is an application for applying SDN technology to WAN connections that connect enterprise networks across disparate geographical locations.

SFP

The Small Form-factor Pluggable. SFP is a compact, hot-pluggable transceiver that is used for both telecommunication and data communications applications.

SFP+

Small Form-factor Pluggable+. SFP+ supports up to data rates up to 16 Gbps.

SFTP

Secure File Transfer Protocol. SFTP is a network protocol that allows file access, file transfer, and file management functions over a secure connection.

SHA

Secure Hash Algorithm. SHA is a family of cryptographic hash functions. The SHA algorithm includes the SHA, SHA-1, SHA-2 and SHA-3 variants.

SIM

Subscriber Identity Module. SIM is an integrated circuit that is intended to securely store the International Mobile Subscriber Identity (IMSI) number and its related key, which are used for identifying and authenticating subscribers on mobile telephony devices.

SIP

Session Initiation Protocol. SIP is used for signaling and controlling multimedia communication session such as voice and video calls.

SIRT

Security Incident Response Team. SIRT is responsible for reviewing as well as responding to computer security incident reports and activity.

SKU

Stock Keeping Unit. SKU refers to the product and service identification code for the products in the inventory.

SLAAC

Stateless Address Autoconfiguration. SLAAC provides the ability to address a host based on a network prefix that is advertised from a local network router through router advertisements.

SMB

Server Message Block or Small and Medium Business. Server Message Block operates as an application-layer network protocol mainly used for providing shared access to files, printers, serial ports, and for miscellaneous communications between the nodes on a network.

SMS

Short Message Service. SMS refers to short text messages (up to 140 characters) sent and received through mobile phones.

SMTP

Simple Mail Transfer Protocol. SMTP is an Internet standard protocol for electronic mail transmission.

SNIR

Signal-to-Noise-Plus-Interference Ratio. SNIR refers to the power of a central signal of interest divided by the sum of the interference power and the power of the background noise. SINR is defined as the power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.

SNMP

Simple Network Management Protocol. SNMP is a TCP/IP standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMPv1

Simple Network Management Protocol version 1. SNMPv1 is a widely used network management protocol.

SNMPv2

Simple Network Management Protocol version 2. SNMPv2 is an enhanced version of SNMPv1, which includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications.

SNMPv2c

Community-Based Simple Network Management Protocol version 2. SNMPv2C uses the community-based security scheme of SNMPv1 and does not include the SNMPv2 security model.

SNMPv3

Simple Network Management Protocol version 3. SNMPv3 is an enhanced version of SNMP that includes security and remote configuration features.

SNR

Signal-to-Noise Ratio. SNR is used for comparing the level of a desired signal with the level of background noise.

SNTP

Simple Network Time Protocol. SNTP is a less complex implementation of NTP. It uses the same , but does not require the storage of state over extended periods of time.

SOAP

Simple Object Access Protocol. SOAP enables communication between the applications running on different operating systems, with different technologies and programming languages. SOAP is an XML-based messaging protocol for exchanging structured information between the systems that support web services.

SoC

System on a Chip. SoC is an Integrated Circuit that integrates all components of a computer or other electronic system into a single chip.

source NAT

Source NAT changes the source address of the packets passing through the router. Source NAT is typically used when an internal (private) host initiates a session to an external (public) host.

SSH

Secure Shell. SSH is a network protocol that provides secure access to a remote device.

SSID

Service Set Identifier. SSID is a name given to a WLAN and is used by the client to access a WLAN network.

SSL

Secure Sockets Layer. SSL is a computer networking protocol for securing connections between network application clients and servers over the Internet.

SSO

Single Sign-On. SSO is an access-control property that allows the users to log in once to access multiple related, but independent applications or systems to which they have privileges. The process authenticates the user across all allowed resources during their session, eliminating additional login prompts.

STBC

Space-Time Block Coding. STBC is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas and to exploit the various received versions of the data to improve the reliability of data transfer.

STM

Station Management. STM is a process that handles AP management and user association.

STP

Spanning Tree Protocol. STP is a network protocol that builds a logical loop-free topology for Ethernet networks.

subnet

Subnet is the logical division of an IP network.

subscription

A business model where a customer pays a certain amount as subscription price to obtain access to a product or service.

SU-MIMO

Single-User Multiple-Input Multiple-Output. SU-MIMO allocates the full bandwidth of the AP to a single high-speed device during the allotted time slice.

SVP

SpectraLink Voice Priority. SVP is an open, straightforward QoS approach that has been adopted by most leading vendors of WLAN APs. SVP favors isochronous voice packets over asynchronous data packets when contending for the wireless medium and when transmitting packets onto the wired LAN.

SWAN

Structured Wireless-Aware Network. A technology that incorporates a Wireless Local Area Network (WLAN) into a wired Wide Area Network (WAN). SWAN technology can enable an existing wired network to serve hundreds of users, organizations, corporations, or agencies over a large geographic area. SWAN is said to be scalable, secure, and reliable.

TAC

Technical Assistance Center.

TACACS

Terminal Access Controller Access Control System. TACACS is a family of protocols that handles remote authentication and related services for network access control through a centralized server.

TACACS+

Terminal Access Controller Access Control System+. TACACS+ provides separate authentication, authorization, and accounting services. It is derived from, but not backward compatible with, TACACS.

TCP

Transmission Control Protocol. TCP is a communication protocol that defines the standards for establishing and maintaining network connection for applications to exchange data.

TCP/IP

Transmission Control Protocol/ Internet Protocol. TCP/IP is the basic communication language or protocol of the Internet.

TFTP

Trivial File Transfer Protocol. The TFTP is a software utility for transferring files from or to a remote host.

TIM

Traffic Indication Map. TIM is an information element that advertises if any associated stations have buffered unicast frames. APs periodically send the TIM within a beacon to identify the stations that are using power saving mode and the stations that have undelivered data buffered on the AP.

TKIP

Temporal Key Integrity Protocol. A part of the WPA encryption standard for wireless networks. TKIP is the next-generation Wired Equivalent Privacy (WEP) that provides per-packet key mixing to address the flaws encountered in the WEP standard.

TLS

Transport Layer Security. TLS is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections above the Transport Layer by using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

TLV

Type-length-value or Tag-Length-Value. TLV is an encoding format. It refers to the type of data being processed, the length of the value, and the value for the type of data being processed.

ToS

Type of Service. The ToS field is part of the IPv4 header, which specifies datagrams priority and requests a route for low-delay, high-throughput, or a highly reliable service.

TPC

Transmit Power Control. TPC is a part of the 802.11h amendment. It is used to regulate the power levels used by 802.11a radio cards.

TPM

Trusted Platform Module. TPM is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.

TSF

Timing Synchronization Function. TSF is a WLAN function that is used for synchronizing the timers for all the stations in a BSS.

TSPEC

Traffic Specification. TSPEC allows an 802.11e client or a QoS-capable wireless client to signal its traffic requirements to the AP.

TSV

Tab-Separated Values. TSV is a file format that allows the exchange of tabular data between applications that use different internal data formats.

TTL

Time to Live. TTL or hop limit is a mechanism that sets limits for data expiry in a computer or network.

TTY

TeleTypeWriter. TTY-enabled devices allow telephones to transmit text communications for people who are deaf or hard of hearing as well as transmit voice communication.

TXOP

Transmission Opportunity. TXOP is used in wireless networks supporting the IEEE 802.11e Quality of Service (QoS) standard. Used in both EDCA and HCF Controlled Channel Access modes of operation, TXOP is a bounded time interval in which stations supporting QoS are permitted to transfer a series of frames. TXOP is defined by a start time and a maximum duration.

UAM

Universal Access Method. UAM allows subscribers to access a wireless network after they successfully log in from a web browser.

U-APSD

Unscheduled Automatic Power Save Delivery. U-APSD is a part of 802.11e and helps considerably in increasing the battery life of VoWLAN terminals.

UCC

Unified Communications and Collaboration. UCC is a term used to describe the integration of various communications methods with collaboration tools such as virtual whiteboards, real-time audio and video conferencing, and enhanced call control capabilities.

UDID

Unique Device Identifier. UDID is used to identify an iOS device.

UDP

User Datagram Protocol. UDP is a part of the TCP/IP family of protocols used for data transfer. UDP is typically used for streaming media. UDP is a stateless protocol, which means it does not acknowledge that the packets being sent have been received.

UDR

User Derivation Rule. UDR is a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on MAC address, BSSID, DHCP-Option, encryption type, SSID, and the location of a user. For example, for an SSID with captive portal in the initial role, a UDR can be configured for scanners to provide a role based on their MAC OUI.

UHF

Ultra high frequency. UHF refers to radio frequencies between the range of 300 MHz and 3 GHz. UHF is also known as the decimeter band as the wavelengths range from one meter to one decimeter.

UI

User Interface.

UMTS

Universal Mobile Telecommunication System. UMTS is a third generation mobile cellular system for networks. See 3G.

UPnP

Universal Plug and Play. UPnP is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi APs, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

URI

Uniform Resource Identifier. URI identifies the name and the location of a resource in a uniform format.

URL

Uniform Resource Locator. URL is a global address used for locating web resources on the Internet.

USB

Universal Serial Bus. USB is a connection standard that offers a common interface for communication between the external devices and a computer. USB is the most common port used in the client devices.

UTC

Coordinated Universal Time. UTC is the primary time standard by which the world regulates clocks and time.

UWB

Ultra-Wideband. UWB is a wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance.

VA

Virtual Appliance. VA is a pre-configured virtual machine image, ready to run on a hypervisor.

VBR

Virtual Beacon Report. VBR displays a report with the MAC address details and RSSI information of an AP.

VHT

Very High Throughput. IEEE 802.11ac is an emerging VHT WLAN standard that could achieve physical data rates of close to 7 Gbps for the 5 GHz band.

VIA

Virtual Intranet Access. VIA provides secure remote network connectivity for Android, Apple iOS, Mac OS X, and Windows mobile devices and laptops. It automatically scans and selects the best secure connection to the corporate network.

VLAN

Virtual Local Area Network. In computer networking, a single Layer 2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them through one or more routers; such a domain is referred to as a Virtual Local Area Network, Virtual LAN, or VLAN.

VM

Virtual Machine. A VM is an emulation of a computer system. VMs are based on computer architectures and provide functionality of a physical computer.

VoIP

Voice over IP. VoIP allows transmission of voice and multimedia content over an IP network.

VoWLAN

Voice over WLAN. VoWLAN is a method of routing telephone calls for mobile users over the Internet using the technology specified in IEEE 802.11b. Routing mobile calls over the Internet makes them free, or at least much less expensive than they would be otherwise.

VPN

Virtual Private Network. VPN enables secure access to a corporate network when located remotely. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

VRD

Validated Reference Design. VRDs are guides that capture the best practices for a particular technology in field.

VRF

VisualRF. VRF is an AirWave Management Platform (AMP) module that provides a real-time, network-wide views of your entire Radio Frequency environment along with floor plan editing capabilities. VRF also includes overlays on client health to help diagnose issues related to clients, floor plan, or a specific location.

VRF Plan

VisualRF Plan. A stand-alone Windows client used for basic planning procedures such as adding a floor plan, provisioning APs, and generating a Bill of Materials report.

VRRP

Virtual Router Redundancy Protocol. VRRP is an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN.

VSA

Vendor-Specific Attribute. VSA is a method for communicating vendor-specific information between NASs and RADIUS servers.

VTP

VLAN Trunking Protocol. VTP is a Cisco proprietary protocol for propagating VLANs on a LAN.

walled garden

walled garden is feature that allows blocking of unauthorized users from accessing network resources.

WAN

Wide Area Network. WAN is a telecommunications network or computer network that extends over a large geographical distance.

WASP

Wireless Application Service Provider. WASP provides a web-based access to applications and services that would otherwise have to be stored locally and makes it possible for customers to access the service from a variety of wireless devices, such as a smartphone or Personal Digital Assistant (PDA).

WAX

Wireless abstract XML. WAX is an abstract markup language and a set of tools that is designed to help wireless application development as well as portability. Its tags perform at a higher level of abstraction than that of other wireless markup languages such as HTML, HDML, WML, XSL, and more.

W-CDMA

Wideband Code-Division Multiple Access. W-CDMA is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices.

web service

Web services allow businesses to share and process data programmatically. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

WEP

Wired Equivalent Privacy. WEP is a security protocol that is specified in 802.11 b and is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN.

WFA

Wi-Fi Alliance. WFA is a non-profit organization that promotes Wi-Fi technology and certifies Wi-Fi products if they conform to certain standards of interoperability.

WIDS

Wireless Intrusion Detection System. WIDS is an application that detects the attacks on a wireless network or wireless system.

Wi-Fi

Wi-Fi is a technology that allows electronic devices to connect to a WLAN network, mainly using the 2.4 GHz and 5 GHz radio bands. Wi-Fi can apply to products that use any 802.11 standard.

WiMAX

Worldwide Interoperability for Microwave Access. WiMAX refers to the implementation of IEEE 802.16 family of wireless networks standards set by the WiMAX forum.

WIP

Wireless Intrusion Protection. The WIP module provides wired and wireless AP detection, classification, and containment. It detects Denial of Service (DoS) and impersonation attacks, and prevents client and network intrusions.

WIPS

Wireless Intrusion Prevention System. WIPS is a dedicated security device or integrated software application that monitors the radio spectrum of WLAN network for rogue APs and other wireless threats.

WISP

Wireless Internet Service Provider. WISP allows subscribers to connect to a server at designated hotspots using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers called stations, to access the Internet and the web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.

WISPr

Wireless Internet Service Provider Roaming. The WISPr framework enables the client devices to roam between the wireless hotspots using different ISPs.

WLAN

Wireless Local Area Network. WLAN is a 802.11 standards-based LAN that the users access through a wireless connection.

WME

Wireless Multimedia Extension. WME is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE) and background (AC_BK). See WMM.

WMI

Windows Management Instrumentation. WMI consists of a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification.

WMM

Wi-Fi Multimedia. WMM is also known as WME. It refers to a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK).

WPA

Wi-Fi Protected Access. WPA is an interoperable wireless security specification subset of the IEEE 802.11 standard. This standard provides authentication capabilities and uses TKIP for data encryption.

WPA2

Wi-Fi Protected Access 2. WPA2 is a certification program maintained by IEEE that oversees standards for security over wireless networks. WPA2 supports IEEE 802.1X/EAP authentication or PSK technology, but includes advanced encryption mechanism using CCMP that is referred to as AES.

WSDL

Web Service Description Language. WSDL is an XML-based interface definition language used to describe the functionality provided by a web service.

WSP

Wireless Service Provider. The service provider company that offers transmission services to users of wireless devices through Radio Frequency (RF) signals rather than through end-to-end wire communication.

WWW

World Wide Web.

X.509

X.509 is a standard for a public key infrastructure for managing digital certificates and public-key encryption. It is an essential part of the Transport Layer Security protocol used to secure web and email communication.

XAuth

Extended Authentication. XAuth provides a mechanism for requesting individual authentication information from the user, and a local user database or an external authentication server. It provides a method for storing the authentication information centrally in the local network.

XML

Extensible Markup Language. XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

XML-RPC

XML Remote Procedure Call. XML-RPC is a protocol that uses XML to encode its calls and HTTP as a transport mechanism. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

ZTP

Zero Touch Provisioning. ZTP is a device provisioning mechanism that allows automatic and quick provisioning of devices with a minimal or at times no manual intervention.

