ArubaOS 8.1.0.0

aruba
a Hewlett Packard
Enterprise company

Release Notes

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

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 04	Removed the **Migrating from ArubaOS 6.x to ArubaOS 8.x** section from **Upgrade Procedure** chapter, and removed **Migration Guide** from the documents listed under **Related Documents** section, as the **Migration Tool** is no longer be supported.
Revision 03	Added description of bug 134168 as a known issue.
Revision 02	Added information about MultiZone Support on VMC in New Features and Enhancements on page 8.
Revision 01	Initial release.

This release of ArubaOS includes new features and enhancements and fixes to issues identified in previous releases.

Throughout this document, branch controller and local controller are termed as managed device.

Use the following links to navigate to the corresponding topics:

- New Features and Enhancements on page 8 describes the new features and enhancements introduced in this release.
- Supported Hardware Platforms on page 19 describes the hardware platforms supported in this release.
- Regulatory Updates on page 21 lists the regulatory updates in this release.
- Resolved Issues on page 22 lists the issues resolved in this release.
- Known Issues on page 34 lists the issues identified in this release.
- Upgrade Procedure on page 45 describes the procedures for upgrading your WLAN network to the latest ArubaOS version.
- Glossary of Terms on page 56 lists the acronyms and abbreviations.

Related Documents

The following guides are part of the complete documentation for the Aruba user-centric network:

- *ArubaOS Release Notes*
- *ArubaOS Quick Start Guide*
- *ArubaOS User Guide*
- *ArubaOS CLI Reference Guide*
- *ArubaOS API Guide*
- *ArubaOS 8.x Syslog Message Guide*
- *Aruba Mobility Master Licensing Guide*
- *Aruba Mobility Master Hardware Appliance Installation Guide*
- *Aruba Mobility Master Virtual Appliance Installation Guide*
- *Aruba Wireless Access Point Installation Guide*

Supported Browsers

The following browsers are officially supported for use with the ArubaOS WebUI:

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Firefox 48 and higher on Windows 7, Windows 8, Windows 10 and Mac OS
- Apple Safari 8.0 or later on Mac OS
- Google Chrome

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/or enhancements introduced in ArubaOS 8.1.0.0.

AirMatch

AirMatch Support for Multiple Time Zones

Starting with ArubaOS 8.1.0.0, the AirMatch solution deployment time for each managed device is based upon the time zone configured for that device. In ArubaOS 8.0.x, the deployment time for all managed devices was based upon the time zone of the Mobility Master server.

Customizable Minimum Channel Bandwidth for AirMatch Solutions

The 5 GHz (802.11a) and 2.4 GHZ (802.11g) radio profiles include the **Minimum Channel Bandwidth** parameter that allow you to configure the minimum channel bandwidth used by an AirMatch solution. These parameter different from the **Maximum Channel Bandwidth** parameter in these profiles, as the maximum-channel-bandwith value allows the AP to implement an AirMatch solution that may select all possible channel widths up to the selected maximum value.

Customizable EIRP offset for AirMatch Solutions

The 5 GHz (802.11a) and 2.4 GHZ (802.11g) radio profiles include an EIRP Offset parameter that allow you to manually adjust EIRP levels by defining an additional EIRP offset value (from -6 to 6 dB) that will be added to the AirMatch solution.

AirWave

Clarity Live

Clarity Live helps diagnose client connectivity issues. It provides the network administrator or engineers with more information regarding the exact stage at which the client connectivity fails or provides data where the DHCP or RADIUS server is slow.

AP-Platform

Support for AP-207 Series Access Point

AP-207 Series access point supports IEEE 802.11ac standards for high-performance WLAN, and is equipped with a dual 2x2 radio. Multiple-Input Multiple-Output (MIMO) technology allows the AP to deliver high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a/b/g wireless services. AP-207 Series access point works in conjunction with a managed device.

AP-207 Series access point provides the following capabilities:

- Wireless transceiver
- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor
- Compatibility with IEEE 802.3af Power over Ethernet (PoE)
- Centralized management configuration and upgrade
- Integrated Bluetooth Low Energy (BLE) radio
- Mesh support

For more information, see the *AP-207 Series Access Points Installation Guide*.

Support for 300 Series Access Point

The 300 Series (AP-304 and AP-305) access points support IEEE 802.11ac standards for high-performance WLAN, and are equipped with a dual 2x2 radio on 2.4 GHz and 3x3 radio on 5 GHz, which provide network access and monitor the network simultaneously. These APs deliver high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while also supporting 802.11a/b/g wireless services. Multi-User Multiple-Input Multiple-Output (MU-MIMO) is enabled when operating in 5 GHz mode for optimal performance. The 300 Series access points work in conjunction with a managed device.

The 300 Series access points provide the following capabilities:

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

For more information, see the *300 Series Access Points Installation Guide*.

Authentication

Roaming RADIUS Accounting Service

Starting from ArubaOS 8.1.0.0, the Roaming RADIUS Accounting Service creates an Accounting session for each wireless client. The records in the session contain the same set of RADIUS attributes as compared to the timer-based RADIUS Interim-Update Accounting record, except the statistics attributes. Whenever a wireless client roams to a different AP, the Roaming triggered RADIUS Interim-Update Accounting record is sent to the configured RADIUS Accounting server. This record is used to track the current location of the wireless client.

Customizing the RADIUS Attributes

The users can now configure RADIUS modifier profile to customize the attributes that are included, excluded, and modified in the RADIUS request before it is sent to the authentication server.

Branch Offices

Extending VPN to Branch Offices.

Starting from ArubaOS 8.1.0.0, branch offices can be connected to data centers by extending VPN to branch offices. Such deployments can include Virtual Internet Gateway (VIG), branch WAN gateway, and management tunnel concentrator. A VIG may be located at a point-of-presence site or a data center.

A secure tunnel is established between a branch office and a VIG and another between the branch office and the management tunnel concentrator. The branch offices are configured to connect to the geographically closest VIG with fallback to a secondary VIG when the primary VIG fails. The VIG maps the tunnels originating from a branch office to the appropriate routing space and provides connectivity to the data center. A branch office site may include IAP and managed devices based deployment. The managed devices perform the WAN gateway related functions.

The management tunnel concentrator provides a secure transport to enable configuration, monitoring, AAA, and remote access to back office subnets.

Cluster

Active AP Load Balancing in Cluster

Starting with ArubaOS 8.1.0.0, load balancing can be performed for active APs in a cluster setup.

Upgrading Cluster

The Live Upgrade feature allows the managed devices and APs that are part of the cluster to automatically upgrade from ArubaOS 8.1 to higher ArubaOS versions.

Cluster Support for ArubaOS Switch

Starting with ArubaOS 8.1.0.0, managed devices support per-user tunnel node feature in cluster environment. This feature allows Aruba switch 16.04 to tunnel the user's traffic to the stand-alone controller or managed devices. To enable this feature, refer to *HP's Management Configuration Guide 16.04*.

Dashboard Monitoring

WAN Dashboard Viewable via Mobility Master

The **WAN** (Wide Area Network) dashboard, in the **Monitoring** section of the WebUI, is the default landing page for a managed device. Starting with ArubaOS 8.1.0.0, the WAN dashboard also appears in the Mobility Master WebUI when a branch office controller is selected in the network hierarchy.

IPv6

IPv6 Router Advertisement Proxy

Whenever a new client joins the network, a unicast or a multicast Router Advertisements (RA) is sent from the router to the client. If it is a multicast packet then existing clients also receive the RA, which results in increasing the traffic. Starting from ArubaOS 8.1.0.0, this issue is addressed by enabling IPv6 proxy RA to snoop incoming unsolicited Router Advertisement and Router Solicitations packets.

DHCPv6 Option-52

Starting with ArubaOS 8.1.0.0, APs can discover a managed device in an IPv6 deployment using DHCPv6 option-52.

Licensing

New Region-Specific Licenses for Mobility Master Virtual Appliance

ArubaOS 8.1.0.0 introduces the MC-VA-XX licenses, sharable license required to terminate APs on a Mobility Master Virtual Appliance. These licenses replaces the VMC license supported by earlier versions of ArubaOS] 8.x. The different MC-VA-XX license types are each region-specific, so any order for a MC-VA-XX license must specify the country where the MM-VA will be deployed.

If your deployment includes a Mobility Master Virtual Appliance running 8.x with a VMC license installed, that license must be regenerated and reinstalled as a MC-VA-xx license. For details, contact customer support.

The following MC-VA-XX license types enable APs to support regional channels for the specified countries:

- MC-VA-50-EG: License to terminate 50 APs on a MM-VA deployed in Egypt.
- MC-VA-50-IL: License to terminate 50 APs on a MM-VA deployed in Israel.
- MC-VA-50-JP: License to terminate 50 APs on a MM-VA deployed in Japan.
- MC-VA-50-RW: License to terminate 50 APs on a MM-VA deployed in a non-restricted country
- MC-VA-50-US: License to terminate 50 APs on a MM-VA deployed in the United States.
- MC-VA-250-EG: License to terminate 250 APs on a MM-VA deployed in Egypt.
- MC-VA-250-IL: License to terminate 250 APs on a MM-VA deployed in Israel.
- MC-VA-250-JP: License to terminate 250 APs on a MM-VA deployed in Japan.
- MC-VA-250-RW: License to terminate 250 APs on a MM-VA deployed in a non-restricted country
- MC-VA-250-US: License to terminate 250 APs on a MM-VA deployed in the United States.
- MC-VA-1K-EG: License to terminate 1000 APs on a MM-VA deployed in Egypt.
- MC-VA-1K-IL: License to terminate 1000 APs on a MM-VA deployed in Israel.
- MC-VA-1K-JP: License to terminate 1000 APs on a MM-VA deployed in Japan.

- MC-VA-1K-RW: License to terminate 1000 APs on a MM-VA deployed in a non-restricted country
- MC-VA-1K-US: License to terminate 1000 APs on a MM-VA deployed in the United States.
- MC-VA-1K-EG: License to terminate 1000 APs on a MM-VA deployed in Egypt.
- MC-VA-1K-IL: License to terminate 1000 APs on a MM-VA deployed in Israel.
- MC-VA-1K-JP: License to terminate 1000 APs on a MM-VA deployed in Japan.
- MC-VA-1K-RW: License to terminate 1000 APs on a MM-VA deployed in a non-restricted country
- MC-VA-1K-US: License to terminate 1000 APs on a MM-VA deployed in the United States
- MC-VA-10K-EG: License to terminate 1000 APs on a MM-VA deployed in Egypt.
- MC-VA-10K-IL: License to terminate 10,000 APs on a MM-VA deployed in Israel.
- MC-VA-10K-JP: License to terminate 10,000 APs on a MM-VA deployed in Japan.
- MC-VA-10K-RW: License to terminate 10,000 APs on a MM-VA deployed in a non-restricted country
- MC-VA-10K-US: License to terminate 10,000 APs on a MM-VA deployed in the United States

Nested Global Licensing Pools

Starting with ArubaOS 8.1.0.0, local license pools are shown as separate pools at the same level as the global licensing pool instead of within the global licensing hierarchy, to better indicate that those licenses are removed from the global pool.

Limitation

Controllers may be upgraded from ArubaOS 6.x to ArubaOS 8.1, but non-disruptive seamless upgrade is not supported. The configuration from ArubaOS 6.x is not maintained after upgrading to ArubaOS 8.1 because the ArubaOS 8.1 configuration model is different from the ArubaOS 6.x configuration model. After upgrading to ArubaOS 8.1, a controller boots with default configuration. Hence, it is recommended to take a backup of the ArubaOS 6.x configuration as a reference to re-configure the controller in ArubaOS 8.1.

Logging

Support for CEF Logging

Starting from ArubaOS 8.1.0.0, support for Common Event Format (CEF) logging is introduced. The ArcSight CEF is a log management standard that uses a standardized logging format so that data can easily be collected and aggregated for analysis by an enterprise management system.

Mobility Master Platform

Mobility Master Hardware Appliance

The Mobility Master Hardware Appliance is a wireless LAN device that manages, controls, and intelligently integrates wireless APs, managed devices, and Air Monitors (AMs) into a wired LAN system. This appliance includes the following specification:

- Two 10GBase-X (SFP+) ports

- Console Port
- Management Port

Table 3 lists the Mobility Master Hardware Appliance models.

Table 3: *Mobility Master Hardware Appliance Models*

Model	Number of Devices	Number of Clients
MM-HW-1K	1000	10000
MM-HW-5K	5000	50000
MM-HW-10K	10000	100000

Allow US Territory on US SKU Mobility Controller

ArubaOS 8.1.0.0 introduces the capability for US SKU Mobility Controller to accept all the US territory APs in addition to US APs. The list of US territories allowed on the US SKU Mobility Controller are:

- Puerto Rico
- Guam,
- US Virgin Islands
- Northern Mariana Islands
- American Samoa
- Federated States of Micronesia
- Marshall Islands

Integration of Trusted Platform Module

Starting from ArubaOS 8.1.0.0, the Trusted Platform Module (TPM) is integrated into the Mobility Master Hardware Appliance that serves only as Mobility Master. This enhancement is done to ensure secure traffic.

NTP Source

Starting from ArubaOS 8.1.0.0, you can specify the source address for NTP traffic originating from the Mobility Master. The source of the NTP client traffic can be either a loopback interface or a specific VLAN ID. To allow time synchronization to be independent of any physical interfaces that could be down, use the loop back interface as the NTP source address.

MultiZone

Non-CPsec support for MultiZone

Starting with ArubaOS 8.1.0.0, both CPsec and non-CPsec APs are supported for MultiZone configuration but the CPsec configuration for all the zones must be the same, either CPsec enabled or disabled.

MultiZone support on VMC

Starting from ArubaOS 8.1.0.0, MultiZone is supported on VMC only when CPsec is disabled.

OSPF

Redistribution of Static Routes over OSPF

Starting from ArubaOS 8.1.0.0, Mobility Master allows you to redistribute the static IP routes over OSPF using the **router ospf redirect static** CLI command.

PAN Firewall Integration

Full Support for Palo Alto Networks (PAN) Firewall Integration

ArubaOS 8.1.0.0 now fully supports integration with a Palo Alto Networks (PAN) firewall. This feature was available only as a beta feature in previous versions of ArubaOS 8.x. ArubaOS PAN firewall integration supports the following interactions with PAN firewall servers running PAN-OS 5.0 or later:

- Send login events for the client to the PAN firewall with its IP address, username, and device type, when classified.
- Send logout events for the client to PAN firewalls with its IP address.

Managed Device Integration with a Palo Alto Networks (PAN) Portal

Managed devices can leverage their networks' existing Palo Alto infrastructure to access more advanced security services, including antivirus services, malware detection and seamless integration with the Palo Alto Networks WildFire™ cloud-based threat detection. Enable Palo Alto firewall integration on Mobility Master to securely redirect internet inbound traffic from managed devices into the PAN firewall. Although this configuration setting can be used on a stand-alone Mobility Master, this feature can only be used in this types of deployments when used in conjunction with the Uplink VLAN manager feature.

Ping

Ping Enhancements

The following Ping options are introduced:

- Interval
- TTL

- Validate-Reply

QoS Enhancements

ArubaOS 6.5.1.0 introduces the following enhanced traffic QoS features.

QoS for AP Management Traffic:

Management traffic on the AP can now be marked with Differentiated Service Code Point (DSCP) values to apply a priority level to that traffic. The **Management DSCP** field is introduced in the AP system profile to support this feature.

DSCP to 802.1P mapping:

The AP system profile allows a user to map IP DSCP priorities (0-63) to a 802.1p priority level (0-7) at the AP's media access control (MAC) level. The **IP DSCP to VLAN 802.1P priority mapping** field is introduced in the AP system profile to support this feature.

QoS for EAP Auth Traffic

Extensible Authentication Protocol (EAP) traffic can be assigned to a specific Wi-Fi Multimedia (WMM) traffic class. By default, EAP traffic is mapped to the "best effort" traffic class. The **WMM Access Class of EAP traffic** field is introduced in the SSID profile to support this feature.

RADIUS

RADIUS VSA Enhancements

The following new RADIUS Vendor-Specific Attributes (VSA) are introduced to support the new traffic steering feature.

- **RTTS-Estimated-Throughput:** Used to transfer a UE through-put estimation value from a RADIUS authenticator to the CWC (via a RADIUS proxy).
- **RTTS-Result**: Used by the CWC to transfer the result of a traffic steering decision to the RADIUS authenticator.
- **RTTS-Backoff-Time**: Used by the CWC in the Access-Accept packet to indicate to the WLAN how long a rejected UE should be ignored before being considered again for entry into the WLAN.
- **RTTS-Reestimation-Period**: Included by the CWC in the Access-Accept packet when RTTS-Result is True to indicate to the WLAN the required interval of time between RTTS Throughput estimates to be sent to the CWC for the UE.
- **RTTS-Reest-Below-Throughput** : Included by the CWC in the Access-Accept packet when RTTS-Result is True to indicate to the WLAN the level below which RTTS Accounting-Request packets should be sent.
- **RTTS-Reest-Keepalive-Num** :This attribute is included by the CWC when RTTS-Result is True in order to ensure that not too many reestimations are skipped by the WLAN due to the UE Wi-Fi estimated throughput being constantly higher than the RTTS-Reestimate-When-Below-Tput threshold.

The following new RADIUS VSAs are introduced to support Hotspot 2.0 feature enhancements.

- **Hotspot2-Subscription-Remediation-URL**: Defines the provisioning supported by the subscription remediation server and a Subscription Server URL sent to a client that is unable to authenticate using its existing credentials.

- **Hotspot2-AP-Version**: Indicates the Hotspot release version supported by the AP. Supported values are **0** for Release 1, and **1** for Release 2.
- **Hotspot2-STA-Version**: Indicates the Hotspot release version supported by the mobile device. Supported values are **0** for Release 1, and **1** for Release 2.
- **Hotspot2-Deauthentication-Request**: Use this VSA to specify the reason the mobile device is being de-authenticated, define the delay time (in seconds) that a mobile device waits before attempting re-association to the same BSS, and define the URL of a server that explains why the mobile device was not authorized.
- **Hotspot2-Session-Info-URL**: Send a BSS Transition Management Request frame before the mobile device's session is terminated, warning the user their session is about to end. Specify a URL in this VSA to provide a link to a web page that provides the user with information on how to extend their session.

Server Load Balancing for RADIUS Accounting

The ArubaOScontrollers perform load balancing of RADIUS accounting packets that are destined to external RADIUS Servers to ensure accounting load gets distributed.

RADIUS Server Response Enhancement

Starting from ArubaOS 8.1.0.0, the **aaa test-server** command includes a new **verbose** option that will display the RADIUS server's response on a successful or failed authentication.

This enhancement applies to both the WebUI and the CLI.

Security

ANY-ANY Crypto Map

Starting from ArubaOS 8.1.0.0, any-any selectors are negotiated in IKEv1 to enable the option of having numerous tunnels.

Null Encryption

Starting from ArubaOS 8.1.0.0, 7000 Series and 7200 Seriescontrollers support null encryption for IKEv1. This helps in reducing the load on the local router for internet destined traffic.

Tunneled Node

Per-user Tunneled Node with ArubaOS Switch

Starting with ArubaOS 8.1.0.0, stand-alone controller or managed devices supports per-user tunnel node feature in stand-alone and cluster environment. The status of the tunneled node user can be viewed only through CLI and not via WebUI. (bug #154421)

UCC

Upstream UCC Score for Wired Clients

Starting with ArubaOS 8.1.0.0, Mobility Master calculates upstream UCC score for wired clients.

VIA

Certificate Criteria for VIA Connection Profiles

Admin users can set the certificate criteria for a VIA connection profile to filter the certificates that can be used to establish the IPsec connection when a user certificate or EAP-TLS is used as the authentication method. The certificate list displayed during VPN profile download only contains certificates that meet the specified certificate criteria, allowing users to avoid certificates that they have not issued. Refer to the *ArubaVIA 3.0.0 for Mobility Master User Guide* for details.

Certificate-Based Authentication for VIA Profile Download

Starting with ArubaOS 8.1.0.0, users can authenticate and download VPN profiles on Aruba VIA using either client certificate-based authentication or the existing credential-based authentication. Refer to the *Aruba VIA 3.0.0 for Mobility Master User Guide* for details.

WebUI

WebUI Enhancements

Starting with ArubaOS 8.1.0.0, the header in the Mobility Master user interface displays the Mobility Master or managed device's deployment mode and hostname.

Cluster WebUI Enhancement

Starting with ArubaOS 8.1.0.0, **Exclude VLAN** option is supported for a node of the managed device in the **Cluster** page.

AirWave WebUI Enhancement

Starting with ArubaOS 8.1.0.0, SNMP V2 **Community string** and SNMP V3 **Username** options are supported in the **AirWave** page.

Mesh Settings Associated with AP Groups

Starting with ArubaOS 8.1.0.0, the mesh cluster, radio, and high throughput settings associated with AP Groups are supported in the **Mesh** page.

Standard Role

Starting with ArubaOS 8.1.0.0, a management role, standard role, is supported in the WebUI. The purpose of creating this role is to prevent changes to the local account from externally authenticated management user.

Zero-touch Provisioning

Automatic ArubaOS 6.x Controller Upgrades via Activate

Starting with ArubaOS 8.1.0.0, a factory-default controller running ArubaOS 6.x can use Activate Zero-Touch Provisioning to upgrade its software as part of the provisioning process. If Activate detects that a factory-default managed device running ArubaOS 6.x has been assigned a **Managed Device to Master Controller** provisioning rule, Activate will automatically send that managed device the information it needs to automatically download and upgrade to the latest version of ArubaOS 8.x.

This chapter describes the hardware platforms supported in ArubaOS 8.1.0.0.

Controller Platforms

The following table displays the controller platforms supported in ArubaOS 8.1.0.0.

Table 4: *Supported Controller Platforms in ArubaOS 8.1.0.0*

Controller Family	Controller Model
7000 Series	7005, 7008, 7010, 7024, 7030
7200 Series	7205, 7210, 7220, 7240, 7240XM

AP Platforms

The following table displays the AP platforms supported in ArubaOS 8.1.0.0.

Table 5: *Supported AP Platforms in ArubaOS 8.1.0.0*

AP Family	AP Model
90 Series	AP-92, AP-93
—	AP-93H
—	AP-103, AP-103H
100 Series	AP-104, AP-105
110 Series	AP-114, AP-115
130 Series	AP-134, AP-135

Table 5: *Supported AP Platforms in ArubaOS 8.1.0.0*

AP Family	AP Model
170 Series	AP-175AC, AP-175AC-F1, AP-175DC, AP-175DC-F1, AP-175P, AP-175P-F1
200 Series	AP-204, AP-205
—	AP-205H
—	AP-207
210 Series	AP-214, AP-215
220 Series	AP-224, AP-225
—	AP-228
270 Series	AP-274, AP-275, AP-277
300 Series	AP-304, AP-305
310 Series	AP-314, AP-315
320 Series	AP-324, AP-325
330 Series	AP-334, AP-335
—	RAP-155, RAP-155P
RAP 100 Series	RAP-108, RAP-109
—	RAP-3WN, RAP-3WNP

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the controller Command Line Interface (CLI) and execute the **show ap allowed-channels country-code <country-code> ap-type <ap-model>** command.

For a complete list of countries and the regulatory domains in which the APs are certified for operation, refer to the Downloadable Regulatory Table or the DRT Release Notes at support.arubanetworks.com.

The following default DRT file version is part of ArubaOS 8.1.0.0:

- DRT-1.0_59118

This chapter describes the issues resolved in ArubaOS 8.1.0.0.

Table 6: *Resolved Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
124863	**Symptom:** Some managed device nodes formed a cluster group with VRRP IP and Wi-Fi clients could not connect to an AP. This issue is resolved by allowing the managed device to send a redirect message so that the AP connects to the managed device's switch IP. **Scenario:** This issue occurred when the managed device's VRRP IP was configured in the cluster group. This issue was observed in all platforms with cluster group-VRRP IP topology, running ArubaOS 6.4.2.6-cluster version.	AP-Platform	All AP Platforms	ArubaOS 6.4.2.6-Cluster	ArubaOS 8.1.0.0
130735	**Symptom:** AP was **UP** in the primary zone device with **Z** flag, if the primary zone IP is configured as datazone IP for the managed devices. This issue is resolved by checking for the following: ■ while configuring the datazone IP, check all the vlan interfaces on the current node and the sub nodes to ensure that there is no conflict. ■ while configuring the vlan IP, check to ensure that the same IP is not used by any multizone profile of the current node. **Scenario:** This issue was observed in managed devices running ArubaOS 8.0.0.0.	AP-Platform	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.1.0.0
132178	**Symptom:** The error log had **Auth GSM : MAC_USER lookup failed for mac f4:f1:5a:9d:06:d0 result error_htbl_key_not_found** error even when switchover never happened. This issue is resolved by not printing an error in a race condition scenario, which is already handled for this functionality. **Scenario:** The error print mostly appeared on the standby side when a client joined a cluster. This issue was observed in all platforms with cluster setup, running ArubaOS 8.0.0.0.	Base OS Security	All platforms with cluster setup	ArubaOS 8.0.0.0	ArubaOS 8.1.0.0

Table 6: *Resolved Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
137890	**Symptom:** The error message, **Invalid Input, input should be a time** was displayed in the **Configuration > Authentication > Internal Server** page of the WebUI. The fix ensures that the error does not appear in the WebUI. **Scenario:** This issue occurred when trying to edit a local user database entry from the **Configuration > Authentication > Internal Server** page of the WebUI. This issue was observed in Mobility Master running ArubaOS 8.0.0.0.	WebUI	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.1.0.0
141640	**Symptom:** The WebUI navigation froze when a user clicked on the **?** icon on the top right corner of the **Configuration** page in the WebUI. The fix ensures that the mouseover help system works as expected. **Scenario:** By clicking on the **?** icon, some of the WebUI fields should turn green indicating that the mouseover help was enabled. However, there was no indication of enabling the help system because the help system was not completely integrated into the **Configuration** pages of the WebUI. This issue was observed in Mobility Master running ArubaOS 8.0.0.0 or later versions.	WebUI	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.1.0.0
141641	**Symptom:** The mouse over help system was not enabled upon clicking the **?** icon on top right corner of the **Configuration** pages in the WebUI. The fix ensures that the mouse over help system works as expected. **Scenario:** This issue was observed in Mobility Master running ArubaOS 8.0.0.0.	WebUI	All platforms	ArubaOS 8.0	ArubaOS 8.1.0.0
143813	**Symptom:** The **Trend** graph in the **Dashboard > UCC > Call Quality** page of the WebUI did not display any data. The fix ensures that the graph displays with appropriate data. **Scenario:** This issue was seen even when there were active calls. This issue was observed in a stand-alone controller deployment running ArubaOS 8.0.0.0 or later versions.	UCC	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.1.0.0

Table 6: *Resolved Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
144156 145374 145759 150408 156415	**Symptom:** A managed device processed wrong instructions. The fix ensures that the managed device processes the correct instructions. **Scenario:** This issue was observed in Mobility Master running ArubaOS 8.0.0.0 or later versions.	Controller-Platform	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.1.0.0
144344	**Symptom:** The **client** page and the **performance** page in the **Dashboard > WLAN** page of the Mobility Master WebUI displayed incorrect distribution of clients among 2.4 GHz and 5 GHz band in comparison to the information on the dashboard of the managed device. The fix ensures that the dashboard displays correct values. **Scenario:** This issue was observed on a Mobility Master dashboard running ArubaOS 8.0.0.0.	Monitoring	Mobility Master	ArubaOS 8.0.0.0	ArubaOS 8.1.0.0
144663	**Symptom:** When the background logo was updated from Mobility Master, it did not synchronize with the managed devices. The fix ensures that the background logo gets updated successfully. **Scenario:** This issue occurred if Captive Portal was configured earlier on the managed device. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	Captive Portal	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.1.0.0
144981	**Symptom:** Incorrect client count was displayed on the dashboard for a managed device in a cluster setup. The fix ensures that the mon/amon AP information is not deleted when the standby tunnel goes down unless BSS is deleted. **Scenario:** This issue occurred when amon/mon entries were deleted from the AP when the AP changed the role of standby. Therefore, the entries for the clients connected were deleted from the dashboard. This issue was observed in managed devices running ArubaOS 8.0.0.0.	Station Management	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.1.0.0
144432	**Symptom:** In the WebUI, **WLANs** and **Usage** pages in **Dashboard** shows incorrect data. The fix ensures that the graphs display aggregated data when two managed devices have the same SSID. **Scenario:** This issue is observed when two managed devices has the same SSID and clients associated. In the **WLANs** or **Usage** pages, the graphs loaded only shows data for one SSID instead of aggregated. This issue is observed in managed devices running ArubaOS 8.0.0.0.	WebUI	All platforms	ArubaOS 8.0.0.0	ArubaOS

Table 6: *Resolved Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
145659	**Symptom:** An administrator could not edit the AirGroup configuration after migrating to ArubaOS 8.0.0.0 using the migration tool. This issue is resolved by skipping AirGroup initialization during migration. **Scenario:** This issue was observed in a 7200 Series stand-alone controller running ArubaOS 8.0.0.0.	AirGroup	7200 Series stand-alone controllers	ArubaOS 8.0.0.0	ArubaOS 8.1.0.0
148528 157388	**Symptom:** A Mobility Master sent AirGroup access request to ClearPass Policy Manager for MAC addresses of Managed Devices which were already known from the internal-state statistics command. This issue is resolved by: ■ Sending AirGroup access request to ClearPass Policy Manager with a delay. ■ Not sending AirGroup access request to ClearPass Policy Manager for the MAC address of a Managed Device if the MAC address is already known. **Scenario:** This issue was observed on Mobility Master running ArubaOS 8.0.1.0.	AirGroup	Mobility Master	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
149480 154920	**Symptom:** An AP failed to connect to a new AP Anchor Controller (AAC). The fix ensures that the APs connect to the newly elected AAC after a cluster failover. **Scenario:** This issue occurred when there was an AP failover from AAC to a Standby-AAC (S-AAC) due to a cluster failover. This issue was observed in a cluster configuration running ArubaOS 8.0.1.0.	IPsec	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.0.1.1
149660	**Symptom:** A VLAN name was case sensitive. This issue is resolved by making the VLAN name case insensitive. **Scenario:** This issue was observed in Mobility Master running ArubaOS 8.0.0.0.	VLAN	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
149799	**Symptom:** Creation of a **license-pool-profile** failed. The fix ensures that the **license-pool-profile** is created successfully. **Scenario:** This issue occurred only if the number of characters in the **license-pool-profile** name exceeded 63. This issue is observed in Mobility Master running ArubaOS 8.0.0.0 or later versions.	Licensing	Mobility Master	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0

Table 6: *Resolved Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
150457 154586	**Symptom:** The **Dashboard > WLANs** page in a Mobility Master showed a different number of clients in comparison to the **Clients** counter in the header of the WebUI. Similarly, the number of clients mismatched between the **Access Points > All Access Points** page and the radio table in the **Access Points > Clients** page. The fix ensures that the values are consistent. **Scenario:** This issue was observed in Mobility Master running ArubaOS 8.0.0.0.	WebUI	Mobility Master	ArubaOS 8.0.0.0	ArubaOS 8.1.0.0
150462	**Symptom:** The **Dashboard > WLANs** page in a Mobility Master showed less number of clients in comparison to the **Clients** page in the Mobility Master and the **Clients** and **WLANs** page in a Managed Device. The fix ensures that the **Dashboard > WLANs** page in the Mobility Master shows the correct number of clients. **Scenario:** This issue was observed in Mobility Master running ArubaOS 8.0.1.0.	Monitoring	Mobility Master	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
150582	**Symptom:** A Mobility Master generated empty DNS requests. The fix ensures that the **nbapi_helper** process does not send empty requests. **Scenario:** This issue occurred when a Mobility Master tried to establish a connection and the IP address for ALE was not present in the **nbapi.properties** file. This issue was observed in a Mobility Master running ArubaOS 8.0.1.0.	NBAPI-Helper	Mobility Master	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
150669	**Symptom:** Pre-staging of managed devices failed. The following changes are made to resolve this issue: ■ In case of trusted vlan, the command configured in the device node of the Mobility Master is prioritized over the configuration in the setup dialog file. ■ The setup dialog is modified to generate **allowed vlan add <id>** instead of **allowed vlan <id>**. **Scenario:** This issue occurred when the **trusted vlan** and **allowed vlan** pre-configured in the managed device were replaced with the configuration from the setup dialog of the device. This issue was observed in managed devices running ArubaOS 8.0.1.0.	Configuration	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0

Table 6: *Resolved Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
151333	**Symptom:** IPv6 routes with link local address were not migrated from ArubaOS 6.x deployment to ArubaOS 8.x. setup. The fix ensures that the IPv6 routes with link local address are migrated correctly. **Scenario:** This issue was observed in Mobility Master running ArubaOS 8.0.0.0 or later versions.	Migration	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
151453	**Symptom:** Telnet session to a managed device was not successful and displayed a **connection refused** message. This issue is resolved by ensuring that telnet works on IPv4 and IPv6. **Scenario:** This issue occurred when a telnet session with a managed device IPv6 was initiated. This issue was observed in managed devices running ArubaOS 8.0.1.0.	IPv6	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
151689	**Symptom:** WLAN deployments running ArubaOS 6.3.x failed to upgrade to ArubaOS 8.x. The fix ensures that deployments running ArubaOS 6.3.x can be upgraded to ArubaOS 8.x. **Scenario:** This issue was observed in WLAN deployments running UCC application on ArubaOS 8.0.1.0.	UCC	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
151740	**Symptom:** The **Dashboard > Traffic Analysis** page did not show all WLANs at the node level. The WLAN details in the **Dashboard > Traffic Analysis** page contained duplicated WLANs when selecting the Managed Device. The fix ensures that the **Dashboard > Traffic Analysis** page shows all WLANs at the node level and unique WLANs at the Managed Device. **Scenario:** This issue was observed in a Mobility Master running ArubaOS 8.0.1.0.	WebUI	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
151742 155284	**Symptom:** The **Dashboard > Managed Network** page showed more clients than actual number of clients. The fix ensures that the **Dashboard > Managed Network** page shows the correct number of clients. **Scenario:** This issue was observed in Managed Devices running ArubaOS 8.0.1.0.	Monitoring	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0

Table 6: *Resolved Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
152148	**Symptom:** When a user roamed to a different SSID, the new SSID was not updated in the **Dashboard > Traffic Analysis** page. The fix ensures that the new SSID replaces the old SSID in the **Dashboard > Traffic Analysis** page. **Scenario:** This issue was observed in Managed Devices running ArubaOS 8.0.1.0.	Monitoring	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
152252	**Symptom:** The management interface on a Mobility Master and Managed Device could be reached when the interface was configured with an IP address even though the interface was shutdown. The fix allows IP address configuration on the management interface only when the interface is not shut. **Scenario:** This issue was observed in managed devices running ArubaOS 8.0.1.0.	Interface	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
152270	**Symptom:** Multiple processes crashed in a Mobility Master and Managed Device. The fix ensures that the boot partition is not overwritten. **Scenario:** This issue occurred because the boot partition was over-written. This issue was observed when a Mobility Master or Managed Device was upgraded to ArubaOS 8.0.1.0.	WebCC	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
152572	**Symptom:** There were **do_ade** crashes in many applications as well as unaligned access. This issue is resolved by increasing the branch history table's depth to ten. **Scenario:** This issue occurred because of a complex sequence of internal CPU events. This in turn caused incorrect instruction fetch and execution of these instructions. This issue was observed in 7000 Series and 7200 Series controllers running ArubaOS 8.0.1.0.	Controller-Platform	7000 Series and 7200 Series controllers	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0

Table 6: *Resolved Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
152750	**Symptom:** On a VM boot-up, the following issues were noticed: ■ The error message did not contain the current and minimum required information for RAM and VCPUs. ■ AOS boot-up on a VM was allowed, although the VCPU value was lesser than the limit mentioned in documentation. The issues are resolved as follows: ■ Modifying the current and expected RAM and VCPU values in the error message. ■ Validating the RAM and VCPU values as per the details mentioned in documentation to prevent bootup. **Scenario:** This issue occurred when MM-VA device with 8 GB RAM and 3 VCPUs was brought up. The issue happened because the RAM and CPU values were lesser than the minimum required limits. This issue was observed in MM-VA and MC-VA platforms running ArubaOS 8.0.1.0.	Bootloader	MM-VA and MC-VA platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
152966	**Symptom:** While configuring RADIUS source-interface and nas-ip, users faced the following issues: ■ Received warning messages. ■ Configurations did not get saved. The fix ensures that these configuration issues are addressed. **Scenario:** This issue occurred because of the following reasons: ■ The **ip[v6] radius source-interface vlan** command could only be configured on device nodes; this was laborious for hundreds of devices. ■ The **ip[v6] radius source-interface vlan** and **ip[v6] radius nas-ip nas-vlan** commands for an unconfigured VLAN returned warning message; also, the configuration did not get saved. This issue was not limited to any specific platform or ArubaOS release version.	CLI	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
153213	**Symptom:** When the **show datapath session** command was executed an invalid IP address was displayed. This issue is resolved by adding a check to ensure that Health Check Monitoring (HCM) does not look for an IPv6 address. **Scenario:** This issue occurred when the Mobility Master connects to a managed device over IPv6. This issue was observed in a Mobility Master running ArubaOS 8.0.1.0.	IPv6	Mobility Master	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0

Table 6: *Resolved Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
153805	**Symptom:** An AP in AM mode did not update the AP name when it was configured in the whitelist database. The fix ensures that the AP name is updated successfully. This issue is resolved by updating the new AP name when the SAPD process gets the new AP name from the whitelist database. **Scenario:** This issue occurred when the AP name was configured in the whitelist database. This issue was observed in APs running ArubaOS 8.0.0.0 or later versions.	AP-Platform	All AP platforms	ArubaOS 8.0.0.0	ArubaOS 8.1.0.0
153841 153920	**Symptom:** The ToS and Dot1P values that were configured in an ACL reverted to the values specified in the UCC application. This issue is resolved by retaining the same ToS and Dot1P values in the ACL and UCC application. **Scenario:** This issue was observed in Mobility Master running ArubaOS 8.1.0.0.	UCC	All AP platforms	ArubaOS 8.1.0.0	ArubaOS 8.1.0.0
153951	**Symptom:** Datapath next hop was null. This issue is resolved by making sure that the incoming SPI and the SPI negotiated with the PAN Global Protect (PANGP) Gateway match. **Scenario:** This issue occurred because of incorrect modifications on incoming SPI values during decryption. This caused IP health check failure and the next hop null. This issues was observed in 7005 controller running ArubaOS 8.0.0.0 or later versions, in a stand-alone topology.	Base OS Security	All platforms	ArubaOS 8.0.0.0	ArubaOS 8.1.0.0
154583	**Symptom:** The **Dashboard** page of Mobility Master did not display the IP address of the client. The fix ensures that the IP address of the client is displayed correctly. **Scenario:** This issue occurred in a cluster deployment where one of the managed devices rebooted. This issue was observed in Mobility Master running ArubaOS 8.0.1.0.	WebUI	Mobility Master	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
155125	**Symptom:** CPsec-enabled APs went into an IKE authentication loop. This issue is resolved by ensuring that a SA request is not deleted if there are two Active IKE SAs with the peer. **Scenario:** This issue was observed in APs configured in a cluster running ArubaOS 8.0.1.0.	IPsec	All AP platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0

Table 6: *Resolved Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
155142	**Symptom:** When a port was added to the LACP group using the WebUI the configuration was partially pushed. This issue is resolved by programming trusted command for all port-channel interfaces from the CLI during the initial setup. **Scenario:** This issue occured due to a mismatch in default port-channel value, in the CLI and WebUI. This issue was observed in managed devices running ArubaOS 8.0.1.0.	Interface	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
155272	**Symptom:** The Mobility Master generated multiple warning messages with respect to licensing. This issue is resolved by changing the severity of the message from warning to debug. **Scenario:** This issue occurred when the configuration process received license limit updates from the license manager process. These messages had no impact on the network. This issue was observed in Mobility Master running ArubaOS 8.0.1.0.	Configuration	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
155287	**Symptom:** The **Dashboard > Performance** page of the WebUI incorrectly displayed the number of APs that were down as 0. The fix ensures that the count of the APs that are in **UP** status alone are displayed in the WebUI **Dashboard**. **Scenario:** This issue was observed in managed devices running ArubaOS 8.0.1.0.	UI Monitoring	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
155587	**Symptom:** When an AirMatch solution was generated, it failed to deploy a solution. Improvements in the computation of network cost and conflict fixed this issue. **Scenario:** This issue occurred when the operational network cost was compared with the cost for a new solution to decide on the deployment of a new solution. This issue was observed in managed devices running ArubaOS 8.0.1.0.	AirMatch	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
155866	**Symptom:** The **authentication** process crashed on the Mobility Master. The fix ensures that the authentication process succeeds. **Scenario:** This issue occurred when the response arrived on the server that was marked for delete was not handled correctly. This issue was observed in a Mobility Master running ArubaOS 8.0.1.0.	Base OS Security	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0

Table 6: *Resolved Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
155867	**Symptom:** The **switch daemon** process crashed on the Mobility Master. The fix ensures that the invalid hello message is processed correctly and the appropriate error value is returned. **Scenario:** This issue occurred when an invalid hello message was validated incorrectly. This issue was observed in a Mobility Master running ArubaOS 8.0.1.0.	SDN-Platform	Mobility Master	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
155925	**Symptom:** APs and clients were unable to connect to a cluster. This issue is resolved by adding checks to ensure that dormant user entries are deleted from the memory. **Scenario:** This issue was caused by stale dormant entries that filled up the memory. This issue was observed in APs connected to a cluster setup.	DDS	All AP platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
156134	**Symptom:** The **cluster manager** process crashed on managed devices. This issue is resolved by handling the ESSID change appropriately. **Scenario:** This issue occurred when there was a change in the ESSID configuration of the SSID profile. This issue was observed in managed devices running ArubaOS 8.0.0.0 or later versions.	Cluster-Manager	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
156374	**Symptom:** The output of the **show provisioning params** command incorrectly displayed **AP provisioning (Invalid)**, though the provisioning was valid. The fix ensures that the output is displayed correctly. **Scenario:** This issue occurred when the **show provisioning-params** command was executed after executing the **provision-ap read-bootinfo** command. This issue occurred when the global AP provisioning structure valid bit was over-written by the AP-specific provisioning structure. This issue was observed in APs connected to a managed devices running ArubaOS 8.0.1.0.	SNMP	All platforms	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0
156755	**Symptom:** An AP failed to download the ArubaOS image from a managed device. This issue is resolved by enabling an FTP server in the control plane for AP images that are available in datapath. **NOTE:** If DPI is enabled, port 2126 should be opened in the firewall on both IPv4 and IPv6. **Scenario:** This issue occurred when DPI was enabled. This issue was observed in 310 Series, 320 Series, and 330 Series access points connected to 7240 controllers running ArubaOS 8.0.1.0.	AP-Platform	310 Series, 320 Series, or 330 Series access points 7240controllers	ArubaOS 8.0.1.0	ArubaOS 8.1.0.0

Table 6: *Resolved Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
156817	**Symptom:** Few APs connected to the cluster were unable to upgrade. This issue is resolved by changing the target IP for the APs when the last managed device rebooted out of sequence. **Scenario:** This issue was observed when the last managed device upgraded out of sequence. This issue was observed in managed devices running ArubaOS 8.1.0.0.	Cluster-Manager	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.1.0.0
157556	**Symptom:** The **Configuration > System > Licensing** page in a Mobility Master did not display the OEM model numbers. This issue is resolved by using the MM license for OAW-MM branded devices and MC-VA-XX licenses for OAW-MC-VA branded devices. **Scenario:** This issue was observed in a Mobility Master running ArubaOS 8.1.0.0.	WebUI	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.1.0.0
158081	**Symptom:** The **show switches** command displayed a **CONFIG FAILURE** status. This issue is resolved by fixing the inconsistent configuration state. **Scenario:** This issue occurred when the spanning tree VLAN priorities were removed successfully from a managed device. This issue was observed in managed devices running ArubaOS 8.1.0.0.	Configuration	All platforms	ArubaOS 8.1.0.0	ArubaOS 8.1.0.0

This chapter describes the issues identified in ArubaOS 8.1.0.0.

Table 7: *Known Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version
113462	**Symptom:** A modem does not complete dialing out. **Scenario:** This issue is observed in controllers running ArubaOS 8.0.0.0. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.0.0.0
115215	**Symptom:** The Co-Channel Interference (CCI) test causes false non-wifi-interference in the output of the **show ap radio-summary** command. **Scenario:** This issue is observed in managed devices running ArubaOS 8.1.0.0. **Workaround:** None.	ARM	All platforms	ArubaOS 8.1.0.0
119350	**Symptom:** The WLAN count for APs in the **Access Points** page is incorrect when a Virtual AP is configured using **AP Name** specific configuration. **Scenario:** An increment in WLAN count is observed when an AP for which the Virtual AP is configured using **AP Name** specific configuration is rebooted. This issue is observed in managed devices running ArubaOS 8.1.0.0. **Workaround:** None.	Monitoring	All platforms	ArubaOS 8.1.0.0
119532	**Symptom:** Vlan status of a particular vlan id is shown as N/A when the **oper status** is **UP**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0.0.0
121019	**Symptom:** A few wireless clients are marked as internal in the user-table and assume ap-role. **Scenario:** This issue occurs when some wireless clients are assigned with the commonly used non-public IP addresses such as 192.168.1.*. These IP addresses collide with the IP address of APs. This issue is observed in managed devices running ArubaOS 8.1.0.0. **Workaround:** Do not assign commonly used non-public IP-addresses to APs.	Base OS Security	All platforms	ArubaOS 8.1.0.0

Table 7: *Known Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version
128448	**Symptom:** A managed device crashes and reboots unexpectedly. **Scenario:** After upgrading a managed device from ArubaOS 8.0.1.0 to ArubaOS 8.1.0.0, the managed device crashes while running some SNMPv3 queries if it is configured with VRRP. This issue is observed in 7240 managed devices running ArubaOS 8.1.0.0. **Workaround:** None.	Controller-Datapath	7240managed devices	ArubaOS 8.1.0.0
130088	**Symptom:** Existing VLANs are not displayed under **Virtual-AP** profile in the **Configuration > Controller > Profile** page of the WebUI. **Scenario:** This issue is observed in Mobility Master, managed devices, and stand-alone controllers running ArubaOS 8.0.0.0 **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0.0.0
130121	**Symptom:** In the **Configuration > Access Points > Whitelist** page of the WebUI, a user cannot filter the CPsec and RAP whitelist database entries based on the column names. **Scenario:** This issue is observed in the **Managed Network** node hierarchy in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** Use the following CLI command with appropriate filters: `(host) [mynode] # show whitelist-db cpsec <filter>`	WebUI	All platforms	ArubaOS 8.0.0.0
130161	**Symptom:** Cluster specific logs are displayed in the AP console when the user tries to establish a tunnel with the stand-alone Data zone device. **Scenario:** This display issue is observed in managed devices running ArubaOS 8.0.0.0. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.0.0.0
130274	**Symptom:** Datapath timeout is observed when traffic passes through ports of a managed device linked to a device with speed of 100 Mbps and half duplex. **Scenario:** This issue is observed in 7008 managed devices running ArubaOS 8.1.0.0. **Workaround:** None.	Controller-Datapath	7008managed devices	ArubaOS 8.1.0.0
130690	**Symptom:** An access point cannot be provisioned with an uplink VLAN configuration using IPv6 address. **Scenario:** A. This issue is observed in a Mobility Master running ArubaOS 8.0.0.0. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.0.0.0

Table 7: *Known Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version
130741	**Symptom:** Chromecast applications do not work when AirGroup is enabled on a Mobility Master. **Scenario:** This issue occurs because of changes to how the Google cast supported applications query for Chromecast. This issue is observed in a Mobility Master and stand-alone controllers running ArubaOS 8.0.0.0. **Workaround:** None.	AirGroup	All platforms	ArubaOS 8.0.0.0
130889	**Symptom:** The VRRP IP address is displayed in the **show ip interface brief** command but is not displayed in the WebUI along with IP interface data. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.1.0.0. **Workaround:** None.	VRRP	All platforms	ArubaOS 8.1.0.0
131133	**Symptom:** When the primary Local Mobility Switch (LMS) is down, AP does not failover to the backup LMS. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0 only in MultiZone mode, with Backup LMS configured. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.0.0.0
131390	**Symptom:** Client is deauthenticated due to inconsistency in the bucket map. **Scenario:** Load balancing algorithm is not functional when a Data zone with more than 12 zones is marked with an **L** flag and is disabled. This issue is observed in managed devices running ArubaOS 8.0.0.0. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.0.0.0
133036	**Symptom:** A managed device encounters kernel panic. **Scenario:** This issue occurs when the USB reclassification happens many times after a cellular modem is connected as uplink to a managed device in addition to the wired uplink. This issue is not limited to any specific managed device model or ArubaOS release version. **Workaround:** Either unplug and plug in the cellular modem or reboot the managed device.	Controller-Platform	All platforms	ArubaOS 8.1.0.0

Table 7: *Known Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version
133304	**Symptom:** A user is unable to assign static IP to a RAP using the WebUI. **Scenario:** This issue occurs because the Sample CSV file that is used to upload in the WebUI does not support static IPs for RAP. This issue is observed in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** Configure static IPs for RAPs individually using the following CLI command: `(host) [mynode] (config) #whitelist-db rap add mac-address <mac> ap-group <ap-group-name> ap-name <name> description <text> remote-ip <static-ip-address>`	WebUI	All platforms	ArubaOS 8.0.0.0
134168	**Symptom:** A tunnel-node does not move to complete state. **Scenario:** This issue is observed in MM-VA with tunnel-nodes between managed devices where PPTN/PUTN is disabled. **Workaround:** None.	Mux	All platforms	ArubaOS 8.0.0.0
134464 145568	**Symptom:** The **spectrum-mode** configuration in the **rf dot11a-radio-profile** and **rf dot11g-radio-profile** commands is not synchronized between the Mobility Master and the managed devices. **Scenario:** This issue is observed in 7240 managed devices running ArubaOS 8.1.0.0. **Workaround:** Add rfp license on the standby controller.	Licensing	7240managed devices	ArubaOS 8.1.0.0
135926	**Symptom:** After an Instant AP (IAP) or the VPN tunnel loses connectivity and returns to service, the nodes connected to VPN-NG centralized L2 VLANS behind IAPs becomes unreachable from behind the managed device through the VPN tunnels. The managed device shows L3 ARP entry for the node, but does not show L2 entry. **Scenario:** This issue is observed when an Instant AP is connected to a managed device VPN-NG IPSEC tunnels configured for centralized L2 operations with Broadcast Multicast (BCMC) optimization configured on the VLAN. When the VPN tunnel is down, the managed device deletes the learned L2 entries, but incorrectly keeps the L3 ARP entries. Once the VPN tunnel re-establishes, since the ARP entry exists, subsequent ARP frames are not flooded to the IAP and are not answered by the client allowing L2 re-learning. **Workaround:** Disable BCMC optimization on the affected VLAN by executing the following commands: **(host) [md] (config) #interface vlan <VLAN>** **(host) [md] (config-subif)#no bcmc-optimization**	RAP-NG	All platforms	ArubaOS 8.1.0.0

Table 7: *Known Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version
135939	**Symptom:** An option to create netdestination from the WebUI is not available. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** Configure netdestination using the following CLI commands: **For IPv4**— `(host) [mynode] (config) #netdestination <name>` **For IPv6**— `(host) [mynode] (config) #netdestination6 <name>`	WebUI	All platforms	ArubaOS 8.0.0.0
138009	**Symptom:** A 7220 managed device reboots because of datapath timeout. **Scenario:** This issue occurs after the managed device—supporting more than 1000 RAPs and 3000 wireless clients—is upgraded to ArubaOS 8.1.0.0. This issue is observed in 7220 managed devices running ArubaOS 8.1.0.0. **Workaround:** None.	Controller-Datapath	7220managed devices	ArubaOS 8.1.0.0
138224	**Symptom:** A managed device does not generate the syslog message 124821 when a remote AP has loop on Ethernet ports. **Scenario:** This issue is observed in managed devices running ArubaOS 8.1.0.0. **Workaround:** None.	Remote Access Points	All platforms	ArubaOS 8.1.0.0
138254	**Symptom:** The client which is not involved in UAC failover is deleted after its flapped uplink is up. The log files for the event lists the reason as **observed ip_user delete** in Mobility Master. **Scenario:** This issue occurs when shut is performed on the standby-UAC, and the sta/user/mac user/ip user entries are activated on the standby-UAC because it loses connectivity with the active UAC. This issue is observed in a cluster setup in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** The workaround is as follows: ■ Decrease the user idle timer to 30 secs in the cluster setup. ■ Once shut is performed, wait for at least a minute before performing no shut. This helps stabilizing the cluster environment.	Base OS Security	All platforms	ArubaOS 8.0.0.0
138808	**Symptom:** An error in AP wireless containment is observed. **Scenario:** This issue is observed when an AP in the AM mode cannot send containment related frames. This issue is observed in AP-205 access points running ArubaOS 8.1.0.0.. **Workaround:** None.	Air Management - IDS	AP-205 access points	ArubaOS 8.1.0.0
139377	**Symptom:** Datapath bandwidth contract is not applied to random users. **Scenario:** This issue is observed in 7220 managed devices running ArubaOS 8.1.0.0. **Workaround:** None.	Controller-Datapath	7220 managed devices	ArubaOS 8.1.0.0

Table 7: *Known Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version
139899	**Symptom:** The **Dashboard > Potential Issues** page in the WebUI displays incorrect number of clients. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0.0.0
140678	**Symptom:** The SNMP CLI commands are not case sensitive. **Scenario:** This issue is observed in a Mobility Master running ArubaOS 8.0.0.0. **Workaround:** None.	SNMP	All platforms	ArubaOS 8.0.1.0
141285	**Symptom:** The ports in a managed device move to **DOWN** state unexpectedly. **Scenario:** This issue is observed in 7200 Series managed devices running ArubaOS 8.1.0.0. **Workaround:** None.	Controller-Platform	7200 Seriesmanaged devices	ArubaOS 8.1.0.0
141558	**Symptom:** The Captive Portal redirection fails when using HTTP. **Scenario:** This issue occurs because the redirect URL from Captive Portal is appended with a string, **&arubalp**, when using HTTP. This issue is observed in managed devices running ArubaOS 8.1.0.0. **Workaround:** Bypass the Captive Portal landing page.	Captive Portal	All platforms	ArubaOS 8.1.0.0
141986	**Symptom:** The banner text does not appear in the WebUI **Logon** page though it is visible in the Command Line Interface. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0.0.0
142081	**Symptom:** Controller path IPv6 packets are not captured for both TCP and UDP sessions. **Scenario:** When the **show packet-capture contolpath-pcap** command is executed, the IPv6 packets are not filtered in the controlpath-pcap output. This issue is observed in Mobility Master and Managed Devices running ArubaOS 8.0.0.0. **Workaround:** None.	IPsec	All platforms	ArubaOS 8.1.0.0
142097	**Symptom:** User session terminates and the user is automatically logged out **Scenario:** This issue is observed when the user is on any page of Dashboard and when the WebUI remains idle for longer than the set Idle Timeout value. This issue is observed in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0.0.0

Table 7: *Known Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version
142463	**Symptom:** Clients are disconnected and reconnected randomly. **Scenario:** This issue is observed when the radio on the Data Zone Mobility Master is enabled or disabled resulting in resetting of the Basic Service Set (BSS). This issue is observed in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.0.0.0
143161	**Symptom:** ACL whitelist fails to display all the default ACLs. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0.0.0
143244	**Symptom:** Zone statistics are not segregated in the CLI output for the command, **show ap debug radio-stats ap-name <ap-name> radio <radio name> advanced**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.0.0 **Workaround:** None.	Station Management	All platforms	ArubaOS 8.0.0.0
143888	**Symptom:** User is unable to configure MAC address for IPsec authentication while setting master IP deployment from managed device. **Scenario:** This issue is observed in all groups and managed devices in Mobility Master running ArubaOS 8.0.0.0 or later versions. **Workaround:** Configure from CLI using the following command: `(host)[md](config) #masterip 10.15.92.5 ipsec ****** peer-mac-1 00:0C:29:D4:FF:D4 interface vlan 92`	WebUI	All platforms	ArubaOS 8.0.0.0
144520	**Symptom:** A customer defined application name is not supported as **appname** in the **interface gigabitethernet <port> bandwidth-contract app <appname> <bwc>** and **route acl** CLI commands. Only standard application names are supported. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0.0.0. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.0.0.0
145460	**Symptom:** The IPsec tunnel between the managed device and the VPNC goes down when load balancing is enabled. **Scenario:** This issue occurs only when the default gateway is configured before the uplink wired VLAN and when load balancing is enabled in managed devices running ArubaOS 8.0.0.0 or later versions. **Workaround:** Configure the default gateway only after configuring the uplink wired VLAN.	Controller-Datapath	All platforms	ArubaOS 8.0.0.0

Table 7: *Known Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version
146158	**Symptom:** Access points crash and rebooted unexpectedly. The log file for the event lists the reason as **Fatal exception at NIP d98945d4 LR d988a998 CTR: c000c724**. **Scenario:** This issue is observed in AP-225 access points running ArubaOS 8.1.0.0. **Workaround:** None.	AP-Wireless	AP-225 access points	ArubaOS 8.1.0.0
147563 158837	**Symptom:** An AP shuts down unexpectedly and its power LED glows solid red. **Scenario:** This issue is observed in POE enabled AP-325 access points connected to managed devices running ArubaOS 8.1.0.0.	BLE	AP-325 access points	ArubaOS 8.1.0.0
148053	**Symptom:** A managed device reboots unexpectedly. The log file for the event lists the reason as **Datapath timeout (SOS Assert) (Intent:cause:register 54:86:50:2)**. **Scenario:** This issue is observed in 7220 managed devices running ArubaOS 8.1.0.0. **Workaround:** None.	Controller-Datapath	7220 managed devices	ArubaOS 8.1.0.0
148172	**Symptom:** A user is unable to create VLANs as Trusted in BOC interface. **Scenario:** This issue is observed in 7200 Series managed devices running ArubaOS 8.1.0.0. **Workaround:** None.	WebUI	7200 Seriesmanaged devices	ArubaOS 8.1.0.0
149041	**Symptom:** AP comes up with an ID flag when CPsec is enabled. **Scenario:** This issue is observed when an AP is connected to a controller through two VLANs, where VLAN 1 is the controller IP and the AP is connected to VLAN 2 on the same controller directly. This issue is observed when CPsec is enabled. **Workaround:** Remove the IPv6 address from the VLAN 2.	AP-Platform	All platforms	ArubaOS 8.0.1.0
149222	**Symptom:** When a user configures a managed device from the **/mm/mynode** node hierarchy of the CLI, the Mobility Master does not display the devices in the WebUI. Only the devices configured from the **/mm** node hierarchy are displayed in the WebUI. **Scenario:** This issue is observed in the WebUI of a Mobility Master running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	IPsec	Mobility Master	ArubaOS 8.0.0.0

Table 7: *Known Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version
151701	**Symptom:** IPv6 ACLs applied on an interface from an ArubaOS 6.x deployment are not effective after migrating to ArubaOS 8.x. setup. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0.0.0 or later versions. **Workaround:** None.	Controller-Platform	All platforms	ArubaOS 8.0.1.0
151906	**Symptom:** Application classification does not work on managed devices if unique application ID or name is not used. **Scenario:** This issue occurs when custom application scripts are added, deleted, and re-added with the same custom application ID or name. This issue is observed in managed devices running ArubaOS 8.0.1.0. **Workaround:** If you are upgrading from ArubaOS 8.0.0.0 with custom applications configured, delete the customer applications and re-add them after upgrading to ArubaOS 8.0.1.0. If you are adding, deleting, and re-adding custom applications in ArubaOS 8.0.1.0, do not reuse the custom application ID or name. Instead, use different unique (previously unused) application ID or name.	Controller-Datapath	All platforms	ArubaOS 8.0.1.0
151952	**Symptom:** When the managed device reboots, APs and clients boot without IP address and other fields. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0 **Workaround:** None.	Monitoring	All platforms	ArubaOS 8.0.1.0
152360	**Symptom:** The **Dashboard > Traffic Analysis > WLAN** page in the WebUI shows repetitive WLANs. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0.1.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0.1.0.
152576	**Symptom:** Trusted CA and public certificate entries are not visible on the standby managed device when configured from the **/mm** node of the Mobility Master WebUI. **Scenario:** This issue is observed in standby managed devices running ArubaOS 8.0.1.0 or later versions. **Workaround:** Upload the certificate directly on the standby managed device.	Certificate Manager	All platforms	ArubaOS 8.0.1.0
153243	**Symptom:** HPE switches request licenses on Mobility Master. **Scenario:** This issue is observed in PUTN feature enabled HPE switches. **Workaround:** HPE switches do not consume any license on Mobility Master.	Tunnel-node-manager	All platforms	ArubaOS 8.1.0.0

Table 7: *Known Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version
154421	**Symptom:** A user cannot use monitoring for PUTN feature enabled HPE switches. **Scenario:** This issue is observed in PUTN feature enabled HPE switches. **Workaround:** PUTN feature enabled HPE switches do not support WebUI monitoring.	WebUI	All platforms	ArubaOS 8.1.0.0
154893	**Symptom:** Database module on managed devices crash unexpectedly. **Scenario:** This issue occurs in an idle setup. This issue is observed in 7200 Series managed devices running ArubaOS 8.1.0.0. **Workaround:** None.	Database	7200 Series managed devices	ArubaOS 8.1.0.0
156094	**Symptom:** Users receive duplicate copies of broadcast and multicast packets. **Scenario:** This issue is observed in per-user tunnel node users in a cluster running ArubaOS 8.1.0.0. **Workaround:** None.	Tunnel-node-manager	All platforms	ArubaOS 8.1.0.0
156700	**Symptom:** AP image preload fails on a 7240 managed device due to SOS errors. **Scenario:** This issue is observed on 7240 managed devices running ArubaOS 8.1.0.0. **Workaround:** Disable DPI and then, upgrade and enable DPI once the upgrade is successful.	Controller-Datapath	7240 managed devices	ArubaOS 8.1.0.0
158446	**Symptom:** In a cluster setup, multicast video stream stops after AP Anchor Controller (AAC) is modified during an active AP rebalance. **Scenario:**This issue is observed in managed device that is part of a cluster running ArubaOS 8.1.0.0. **Workaround:** None.	Multicast	All platforms	ArubaOS 8.1.0.0
158908	**Symptom:** The WebUI displays the **% Invalid input detected at '^' marker** error when a user attempts to create an IDS signature profile. **Scenario:** This Issue is observed when a user attempts to create an IDS signature profile from the WebUI and the RFP license is either disabled or not present. **Workaround:** Add an RFP license and enable it before attempting to create an IDS signature profile.	CLI	All platforms	ArubaOS 8.1.0.0

Table 7: *Known Issues in ArubaOS 8.1.0.0*

Bug ID	Description	Component	Platform	Reported Version
158911	**Symptom:** The **show license-usage ap** command on standalone license client (MC-VA-250 (US)) does not display the country to which it belongs. **Scenario:** This Issue is observed only in MC-VA-250 (US) and not in MC-VA-50 (US). **Workaround:** None.	Configuration	MC-VA-250	ArubaOS 8.1.0.0
158950	**Symptom:** License manager crashes on standby managed device. **Scenario:** This issue occurs when License pool-profile on active master is added or deleted and then, a failover to backup master occurs. This issue is observed in a Mobility Master or a Mobility Master Hardware Appliance running ArubaOS 8.1.0.0 **Workaround:** None	Licensing	All platforms	ArubaOS 8.1.0.0
159558	**Symptom:** The WebUI displays a generic error when a user attempts to create a new WLAN profile. **Scenario:** This issue is observed when a user attempts to create a new WLAN profile from the **Configuration > Tasks** page of the WebUI and the PEFNG license is either disabled or not present. **Workaround:** Add a PEFNG license and enable it before attempting to create a new WLAN profile.	Configuration	All platforms	ArubaOS 8.1.0.0

This chapter details software upgrade procedures. Aruba best practices recommend that you schedule a maintenance window for the upgrade.

Read all the information in this chapter before upgrading your Mobility Master, managed device, master controller, and/or stand-alone controller.

Topics in this chapter include:

Migrating from ArubaOS 8.0.x to ArubaOS 8.1.x

If you are migrating from ArubaOS 8.0.x to ArubaOS 8.1.x, migrate the MC-VA licenses if the country type is a restricted country type (US, JP, IL, EG).

Manually delete and add all MC-VA licenses after upgrading to the new ArubaOS version.

The following points are for reference:

- Upgrade from ArubaOS 8.0.1.x to ArubaOS 8.0.1.x
  - No change if MC-VA license is not used.
  - If country type is one of restricted country type (US, JP, IL, EG), there is no country lock behavior.
  - Aruba recommends to upgrade to ArubaOS 8.1.0.0 for the country lock feature.
- New order in ArubaOS 8.0.1
  - After My Networking Portal (MNP) is updated based on the new country lock, use the part numbers that are part of ArubaOS part 8.1.0.0.
  - Use only MC-VA-XX-RW from MNP.

- In ArubaOS 8.0.1 MC-VA-XX-US, MC-VA-XX-JP, MC-VA-XX-IL, MC-VA-XX-EG country licenses cannot be used after MNP update.

- Transfer to ArubaOS 8.0.1.x
  - Applicable in case of RMA of ArubaOS 8.0.1.x.
  - Transfer of license from MNP is supported only for RW license type.
- Upgrade from ArubaOS 8.0.1.x to ArubaOS 8.1.x
  - If you have configured one of the restricted country type (US, JP, IL, EG):
    - The existing licenses are considered as RW licenses. APs will be in unlicensed state for the restricted country types (US, JP, IL, EG).
    - Delete the existing MC-VA license.
    - Obtain a new license from MNP according to the country based on the order.
    - Apply the new license on standalone controller or Mobility Master to get country lock MC-VA.
    - Licenses other than MC-VA are not impacted.
  - If you have configured any country apart from the restricted country type (US, JP, IL, EG):
    - Existing licenses are considered as RW licenses.
    - APs will advertise the channels based on country if previous license are present.
    - No impact for non-restricted country types.

Important Points to Remember and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions provided in the following list. You should save this list for future use.

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any other changes to your network, such as configuration changes, hardware upgrades, or changes to the rest of the network during the upgrade. This simplifies troubleshooting.
- Know your network and verify the state of your network by answering the following questions:
  - How many APs are assigned to each managed device? Verify this information by navigating to the **Dashboard > Access Points** section of the WebUI, or by executing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the managed device (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS is currently on the managed device?
  - Are all managed devices running the same version of software?
  - Which services are used on the managed device (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.

- If possible, use FTP to load software images to the managed device. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to this version of ArubaOS, assess your software license requirements and load any new or expanded licenses you may require. For a detailed description of these new license modules, see the "Software Licenses" chapter in the *ArubaOS User Guide*.

Memory Requirements

All Aruba managed devices store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the managed device. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. To maintain the reliability of your WLAN network, the following compact memory best practices are recommended:

- Confirm that there is at least 100 MB of free memory available for an upgrade using the WebUI or CLI. Execute the **show memory** command to identify the amount of free memory available using the CLI. Do not proceed unless this much free memory is available. To recover memory, reboot the managed device. After the managed device comes up, upgrade immediately.
- Confirm that there is at least 150 MB of flash space available for an upgrade using the WebUI or CLI. Execute the **show storage** command to identify the amount of flash space available using the CLI.

In certain situations, a reboot or a shutdown could cause the managed device to lose the information stored in its compact flash card. To avoid such issues, it is recommended that you execute the **halt** command before power cycling.

If the output of the **show storage** command indicates that there is insufficient flash memory space, you must free up some used memory. Any managed device logs, crash data, or flash backups should be copied to a location off the managed device, then deleted from the managed device to free up flash space. You can delete the following files from the managed device to free up some memory before upgrading:

- **Crash Data:** Execute the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 48 to copy the **crash.tar** file to an external server, and then execute the **tar clean crash** command to delete the file from the managed device.
- **Flash Backups:** Use the procedures described in Backing up Critical Data on page 48 to back up the flash directory to a file named **flash.tar.gz**, and then execute the **tar clean flash** command to delete the file from the managed device.
- **Log files:** Execute the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 48 to copy the **logs.tar** file to an external server, and then execute the **tar clean logs** command to delete the file from the managed device.

The following procedure deletes a file.

In the WebUI

Navigate to **Maintenance > File > Delete Files** and remove any aging log files or redundant backups which may have been created by administrator.

In the CLI

```
(host) #delete filename <filename>
```

Backing up Critical Data

It is important to frequently back up all critical configuration data and files on the compact flash file system to an external server or mass storage device. At the very least, you should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Floor plan JPEGs
- Custom captive portal pages
- x.509 certificates
- Logs
- Flashbackup

Backing up and Restoring Compact Flash in the WebUI

The WebUI provides the easiest way to back up and restore the entire compact flash file system. The following steps describe how to back up and restore the compact flash file system using the WebUI on the managed device:

1. Click the **Configuration** tab.
2. Click **Save Configuration** at the top of the page.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.
5. Click **Copy Backup** to copy the file to an external server.

   You can later copy the backup file from the external server to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.
6. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page and click **Restore**.

Backing up and Restoring Compact Flash in the CLI

The following steps describe the backup and restore procedure for the entire compact flash file system using the command line:

1. Make sure you are in the **enable** mode in the CLI, and execute the following command:

   ```
   (host) # write memory
   ```

2. Execute the **backup** command to back up the contents of the compact flash file system to the **flashbackup.tar.gz** file.

   ```
   (host) # backup flash
   Please wait while we tar relevant files from flash...
   Please wait while we compress the tar file...
   Checking for free space on flash...
   Copying file to flash...
   File flashbackup.tar.gz created successfully on flash.
   ```

3. Execute the **copy** command to transfer the backup flash file to an external server or storage device.

   ```
   (host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword> <remote directory>
   (host) copy flash: flashbackup.tar.gz usb: partition <partition-number>
   ```

   You can later transfer the backup flash file from the external server or storage device to the compact flash file system by executing the **copy** command.

   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   (host) # copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
   ```

4. Execute the **restore** command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system.

   ```
   (host) # restore flash
   ```

Upgrading

The following sections provide the procedures for upgrading your WLAN network to the latest ArubaOS version using the WebUI or CLI.

ArubaOS 8.1.0.0 Upgrade Notes

Before you upgrade Mobility Master from ArubaOS 8.0.0.0 to ArubaOS 8.1.0.0, take a note of the following points:

- ArubaOS 8.1.0.0 supports only a maximum of 3 network adapters for Mobility Master and 4 network adapters for MM-VA. If you have 4 network adapters on your ArubaOS 8.0.0.0 MM-VA, you must remove one before upgrading to ArubaOS 8.1.0.0 to avoid upgrade failure. To remove a network adapter from ArubaOS 8.0.0.0 MM-VA:

Before you remove the additional network adapter from the MM-VA, ensure that you copy the ArubaOS 8.0.0.0 image on the system partition of MM-VA.

1. Log in to the vSphere client.
2. Select the Mobility Master VM instance and click **Shut down the virtual machine**.
3. Click **Edit Virtual machine settings**.

4. From the **Hardware** tab, select and remove a network adapter that is not active.

- Before upgrading to ArubaOS 8.1.0.0 from ArubaOS 8.0.0.0, ensure that you configure the MAC address of the management interface as the peer MAC address, if the peer is a MM-VA or Mobility Master. Before reloading the new image on Mobility Master, alter the peer MAC address using the following procedure in the WebUI:
  1. From the **Managed Network** node hierarchy, select the managed device.
  2. Navigate to **Configuration > Controllers** and enter the management interface MAC address in the **Peer MAC address of master** field.
  3. Click **Submit** and click **Continue** in the reload popup.
  4. Click **Pending Changes**.
  5. In the **Pending Changes** window, select the check box and click **Deploy changes**.

  Alternatively, you can execute the following CLI command on Mobility Master at the device level:

  ```
  (host) [<device-mac-address>] (config) #masterip <ipaddr> ipsec <key> peer-mac-1 <mgmt-interface-mac> peer-mac-2 <mgmt-interface-mac> interface vlan <id>
  ```
- Before upgrading to ArubaOS 8.1.0.0 from ArubaOS 8.0.0.0, move the **license-pool-profile-root** configuration from **/mm/mynode** to **/mm**.

In the WebUI

CAUTION

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash space available for an upgrade using the WebUI. For details, see Memory Requirements on page 47.

NOTE

When you navigate to the **Configuration** tab in the WebUI, the managed device may display the **Error getting information: command is not supported on this platform** message. This error occurs when you upgrade from the WebUI and navigate to the **Configuration** tab as soon as the managed device completes rebooting. This error is expected and disappears after clearing the Web browser cache.

You can install the software image from a TFTP or FTP server using the same WebUI page.

1. Download ArubaOS from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Validate the SHA hash for a software image:
   a. Download the **Aruba.sha256** file from the download directory.
   b. To verify the image, load the image onto a Linux system and execute the **sha256sum <filename>** command or use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
   c. Verify that the output produced by this command matches the hash value found on the support site.

NOTE

The ArubaOS image file is digitally signed, and is verified using RSA2048 certificates preloaded at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the managed device will not load a corrupted image.

4. Log in to the ArubaOS WebUI from the PC or workstation.
5. Navigate to the **Maintenance > Controller > Image Management** page.
   a. Select the **Local File** option.
   b. Click **Browse** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. Click the non-boot partition from the **Partition to Upgrade** option.
8. Click **Yes** in the **Reboot Controller After Upgrade** option to automatically reboot after upgrading. Click **No**, if you do not want to reboot immediately.

Note that the upgrade will not take effect until you reboot.

9. Click **Yes** in the **Save Current Configuration Before Reboot** option.
10. Click **Upgrade**.

    When the software image is uploaded, a popup window displays the **Changes were written to flash successfully** message.
11. Click **OK**.

    If you chose to automatically reboot in step 8, the reboot process starts automatically within a few seconds (unless you cancel it).
12. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > NETWORK > All WLAN Controllers** page to verify the upgrade.

When your upgrade is complete, perform the following steps to verify that the controller is functioning as expected.

1. Log in to the WebUI to verify all your controllers are up after the reboot.
2. Navigate to the **Monitoring > NETWORK > Network Summary** page to determine if your APs are up and ready to accept clients. In addition, verify that the number of access points and clients are what you would expect.
3. Verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 48 for information on creating a backup. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses.

In the CLI

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash space available for an upgrade using the CLI. For details, see Memory Requirements on page 47.

Upgrading From a Recent Version of ArubaOS

To install the ArubaOS software image from a PC or workstation using the CLI:

1. Download ArubaOS from the customer support site.
2. Open an SSH session on your master (and local) controllers.
3. Execute the **ping** command to verify the network connection from the target controller to the SCP/FTP/TFTP server.

   ```
   (host)# ping <ftphost>
   ```

   or

   ```
   (host)# ping <tftphost>
   ```

   or

   ```
   (host)# ping <scphost>
   ```

4. Execute the **show image version** command to check if the ArubaOS images are loaded on the controller's flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

   ```
   (host) #show image version
   ```

5. Execute the **copy** command to load the new image onto the non-boot partition.

   ```
   (host)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
   ```

   or

   ```
   (host)# copy tftp: <tftphost> <image filename> system: partition <0|1>
   ```

   or

   ```
   (host)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
   ```

   or

   ```
   (host)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
   ```

6. Execute the **show image version** command to verify that the new image is loaded.

   ```
   (host)# show image version
   ```

7. Reboot the controller.

   ```
   (host)# reload
   ```

8. Execute the **show version** command to verify that the upgrade is complete.

   ```
   (host)# show version
   ```

When your upgrade is complete, perform the following steps to verify that the controller is functioning as expected.

1. Log in to the CLI to verify that all your controllers are up after the reboot.
2. Execute the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Execute the **show ap database** command to verify that the number of access points and clients are what you expected.
4. Test a different type of client for each access method that you use and in different locations when possible.

5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 48 for information on creating a backup.

Downgrading

If necessary, you can return to your previous version of ArubaOS.

Before You Begin

Before you reboot the controller with the pre-upgrade software version, you must perform the following steps:

1. Back up your controller. For details, see Backing up Critical Data on page 48.
2. Verify that the control plane security is disabled.
3. Set the controller to boot with the previously saved pre-ArubaOS configuration file.
4. Set the controller to boot from the system partition that contains the previously running ArubaOS image.

   When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next controller reload. An error message is displayed if system boot parameters are set for incompatible image and configuration files.
5. After downgrading the software on the controller, perform the following steps:
   - Restore pre-ArubaOS flash backup from the file stored on the controller. Do not restore the ArubaOS flash backup file.
   - You do not need to reimport the WMS database or RF Plan data. However, if you have added changes to RF Plan in ArubaOS, the changes do not appear in RF Plan in the downgraded ArubaOS version.
   - If you installed any certificates while running ArubaOS, you need to reinstall the certificates in the downgraded ArubaOS version.

Downgrading Using the WebUI

The following section describes how to use the WebUI to downgrade the software on the controller

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the controller by navigating to the **Maintenance > File > Copy Files** page.
   a. For **Source Selection**, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the pre-upgrade configuration file.
   b. For **Destination Selection**, enter a file name (other than default.cfg) for Flash File System.
2. Set the controller to boot with your pre-upgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved pre-upgrade configuration file from the **Configuration File** drop-down list.
   b. Click **Apply**.

3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition) by performing the following steps:
   a. Enter the FTP/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
4. Navigate to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the system partition that contains the pre-upgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The controller reboots after the countdown period.
6. When the boot process is complete, verify that the controller is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

Downgrading Using the CLI

The following section describes how to use the CLI to downgrade the software on the controller.

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the controller:
   ```
   (host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
   ```
   or
   ```
   (host) # copy tftp: <tftphost> <image filename> system: partition 1
   ```
2. Set the controller to boot with your pre-upgrade configuration file.
   ```
   (host) # boot config-file <backup configuration filename>
   ```
3. Execute the **show image version** command to view the partition on which your previous software image is stored. You cannot load a new image into the active system partition (the default boot).
   ```
   #show image version
   ```
4. Set the backup system partition as the new boot partition.
   ```
   (host) # boot system partition 1
   ```
5. Reboot the controller.
   ```
   (host) # reload
   ```
6. When the boot process is complete, verify that the controller is using the correct software.
   ```
   (host) # show image version
   ```

Before You Call Technical Support

Before you place a call to Technical Support, follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the Aruba device with IP addresses and Interface numbers if possible).
2. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless Network Interface Card (NIC) make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
3. Provide the logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
4. Provide the syslog file at the time of the problem. Aruba strongly recommends that you consider adding a syslog server if you do not already have one to capture the logs.
5. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have an outage in a network that worked in the past, a network configuration that has never worked, or a brand new installation.
6. Let the support person know if there are any recent changes in your network (external to the Aruba device) or any recent changes to your Aruba device and/or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) of when the problem first occurred. If the problem is reproducible, list the exact steps taken to re-create the problem.
8. Provide any wired or wireless sniffer traces taken during the time of the problem.
9. Provide the Aruba device site access information, if possible.

Appendix A
Glossary of Terms

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+.

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.

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.

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.

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.

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.

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.

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.

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.

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: APname.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. GVRP 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 polices 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 documentss.

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.

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.

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.

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.

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.

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.

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.

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.

UAM

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

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.

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.

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.

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 802.11b 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.

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.

WIDS

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

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.