

# AOS-W Instant 6.5.4.2

Alcatel·Lucent  
Enterprise



## **Copyright Information**

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

[enterprise.alcatel-lucent.com/trademarks](http://enterprise.alcatel-lucent.com/trademarks)

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

## **Open Source Code**

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

---

<b>Contents</b> .....	<b>3</b>
Revision History .....	4
<b>Release Overview</b> .....	<b>5</b>
Chapter Overview .....	5
Supported Browsers .....	5
Important Updates .....	6
Contacting Support .....	6
<b>New Features</b> .....	<b>8</b>
<b>Regulatory Updates</b> .....	<b>9</b>
<b>Resolved Issues</b> .....	<b>10</b>
<b>Known Issues</b> .....	<b>11</b>
<b>Upgrading an OAW-IAP</b> .....	<b>13</b>
Upgrading an OAW-IAP and Image Server .....	13
Upgrading an OAW-IAP Using Automatic Image Check .....	15
Upgrading an Image Using CLI .....	16
<b>Glossary of Terms</b> .....	<b>18</b>

## Revision History

The following table provides the revision history of this document.

**Table 1:** *Revision History*

Revision	Change Description
Revision 02	Added the CVE numbers of the vulnerabilities resolved in this release.
Revision 01	Initial release.

AOS-W Instant 6.5.4.2 is a software release that includes fixes to issues identified in previous releases as well as the known and outstanding issues in this release.

### Chapter Overview

- [New Features](#) provides a description of features and enhancements introduced in this release.
- [Regulatory Updates](#) describes the regulatory updates in this release.
- [Resolved Issues](#) describes the issues resolved in this release.
- [Upgrading an OAW-IAP](#) describes the upgrade procedures for OAW-IAPs.
- [Glossary of Terms](#) lists the acronyms and abbreviations used in the document.



---

For information regarding prior releases, refer to the corresponding Release Notes on <https://support.esd.alcatel-lucent.com/>.

---

### Supported Browsers

The following browsers are officially supported for use with AOS-W Instant 6.5.4.2 WebUI:

- Microsoft Internet Explorer 10.x and 11 on Windows 7 and Windows 8
- Mozilla Firefox 23 or later on Windows Vista, Windows 7, and Mac OS
- Apple Safari 5.1.7 or later on Mac OS
- Google Chrome 51.0.2704.103 m (64-bit)
- Microsoft Edge 25.10586.0.0 and Microsoft Edge HTML 13.10586

## Important Updates

### DPI

Starting from AOS-W 6.5.0.0-4.3.0.0 onwards, DPI is not supported on OAW-AP103 , OAW-RAP108, and OAW-RAP109 due to the existing memory limitations. The last release with full feature support for these platforms is AOS-W 6.4.x.x-4.2.x.x.

If you have deployed OAW-AP103, OAW-RAP108, or OAW-RAP109 and require DPI functionality, ensure that you remain on AOS-W 6.4.x.x-4.2.x.x or earlier versions. However, if you are willing to disable DPI functionality, upgrade to AOS-W 6.5.0.0-4.3.0.0 or later releases.

### IP-Mode

The IP-mode default value changes to **v4 only** in the AOS-W 6.5.4.0 release version. This change in value causes a mismatch warning for OmniVista customers that use a template file for configuration. We recommend you to change the template file in OmniVista to fix this mismatch. OmniVista UI users, please upgrade your respective versions.



---

The mismatch occurs only if the release versions used before the upgrade are from AOS-W 6.5.2.0 to AOS-W 6.5.3.1. There will be no mismatch if the release version used before the upgrade is earlier than AOS-W 6.5.2.0 or later than AOS-W 6.5.3.1.

---

## Contacting Support

**Table 2:** *Contact Information*

Contact Center Online	
Main Site	<a href="http://enterprise.alcatel-lucent.com">http://enterprise.alcatel-lucent.com</a>
Support Site	<a href="https://support.esd.alcatel-lucent.com">https://support.esd.alcatel-lucent.com</a>
Email	<a href="mailto:ebg_global_supportcenter@al-enterprise.com">ebg_global_supportcenter@al-enterprise.com</a>
Service & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526

## Contact Center Online

EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

There are no new features introduced in this release.



This chapter describes the regulatory updates in AOS-W Instant 6.5.4.2.

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 switch Command Line Interface (CLI) and execute the **show ap allowed-channels** command.

The following default Downloadable Regulatory Table (DRT) version is part of AOS-W 6.5.4.2:

- DRT-1.0\_61690

For a complete list of countries certified with different AP models, refer to the DRT Release Notes at [support.esd.alcatel-lucent.com](http://support.esd.alcatel-lucent.com).



---

This software release supports the channel requirements described in *ALE Support Advisory SA-N0033*, available for download from the [support.esd.alcatel-lucent.com](http://support.esd.alcatel-lucent.com) site.

---

This release includes fixes for vulnerability documented in:

- WPA2 Key Reinstallation Vulnerabilities ([CVE-2017-13077](#)) - [CVE-2017-13077](#), [CVE-2017-13078](#), [CVE-2017-13079](#), [CVE-2017-13080](#), [CVE-2017-13081](#), [CVE-2017-13082](#), [CVE-2017-13084](#), [CVE-2017-13086](#), [CVE-2017-13087](#), and [CVE-2017-13088](#)
- AOS-W Multiple Vulnerabilities - [CVE-2017-9000](#) and [CVE-2017-9003](#).
- Multiple Vulnerabilities in 'dnsmasq' - [CVE-2017-14491](#), [CVE-2017-14492](#), [CVE-2017-14493](#), [CVE-2017-14494](#), [CVE-2017-14495](#), and [CVE-2017-14496](#).

Additionally, the following issues are resolved in AOS-W 6.5.4.2.

**Table 3:** Resolved Issue in AOS-W 6.5.4.2

Bug ID	Description	Component	Platform	Reported Version	Resolved in Version
157287 169230	<p><b>Symptom:</b> A screencasting session from a Samsung Chromebook to a Chromecast device crashed, and failed to resume. This issue is resolved by ensuring that the OAW-IAP does not drop Rx data aggregates.</p> <p><b>Scenario:</b> This issue occurred because there was a large file transfer when the OAW-IAP was already heavily loaded during the screencasting session. This issue was observed in OAW-AP325 access points running AOS-W 6.5.3.0 or later versions.</p>	Wi-Fi Driver	OAW-AP325 access points	AOS-W 6.5.3.0	AOS-W 6.5.4.2

This chapter describes the known and outstanding issues identified in AOS-W 6.5.4.2.

**Table 4:** *Known Issues in AOS-W 6.5.4.2*

Bug ID	Description	Component	Platform	Reported Version
164019 164426 164893 165984 166654 166691	<p><b>Symptom:</b> OAW-IAPs reboot due to a kernel panic. The log file lists the reason for the event as <b>Reboot caused by kernel page fault at virtual address 001a000 when 11k enabled.</b></p> <p><b>Scenario:</b> This issue is observed in OAW-AP103 access points and is not limited to specific Instant release versions.</p> <p><b>Workaround:</b> None.</p>	Wi-Fi Driver	OAW-AP103 access points	AOS-W 6.5.4.0
165705	<p><b>Symptom:</b> A DNS server incorrectly resolves the FQDN of a RadSec server at the first attempt.</p> <p><b>Scenario:</b> This issue occurs when the RadSec FQDN is resolved to incorrect IP address. This issue is observed in OAW-IAPs running AOS-W 6.5.3.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Firewall	All platforms	AOS-W 6.5.3.0
166938	<p><b>Symptom:</b> OAW-IAPs are unable to respond to XML API requests sent from port 80.</p> <p><b>Scenario:</b> This issue is observed in OAW-IAPs running AOS-W 6.5.2.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Configuration	All platforms	AOS-W 6.5.2.0

**Table 4:** *Known Issues in AOS-W 6.5.4.2*

Bug ID	Description	Component	Platform	Reported Version
166984	<p><b>Symptom:</b> OAW-IAPs randomly reboot with the reason <b>System clock is too far ahead of NTP sync result.</b></p> <p><b>Scenario:</b> This issue occurs because a malformed UDP packet sent from a non-NTP server with source port 123 modifies the system clock. This issue is observed in OAW-IAPs running AOS-W 6.5.3.2 or later versions.</p> <p><b>Workaround:</b> None.</p>	Platform	All platforms	AOS-W 6.5.3.2
167091 168226	<p><b>Symptom:</b> OAW-IAPs randomly reboot because of a low memory.</p> <p><b>Scenario:</b> This issue occurs because the age out function for cached probe requests is not added to the OAW-IAPs. This issue is observed in OAW-IAPs running AOS-W 6.5.4.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Platform	All platforms	AOS-W 6.5.4.0
168123	<p><b>Symptom:</b> Clients are unable to authenticate against CPPM when authentication survivability is not reachable.</p> <p><b>Scenario:</b> This issue occurs due to a discrepancy in the free RADIUS server user name format. This issue is observed in OAW-IAPs running AOS-W 6.5.4.0 or later versions.</p> <p><b>Workaround:</b> None.</p>	Authentication	All platforms	AOS-W 6.5.4.0

This chapter describes the AOS-W software upgrade procedures and the different methods for upgrading the image on the OAW-IAP.



NOTE

---

While upgrading an OAW-IAP, you can use the image check feature to allow the OAW-IAP to find new software image versions available on a cloud-based image server hosted and maintained by Alcatel-Lucent Enterprise. The location of the image server is fixed and cannot be changed by the user. The image server is loaded with the latest versions of the AOS-W software.

---

Topics in this chapter include:

- [Upgrading an OAW-IAP and Image Server on page 13](#)
- [Upgrading an OAW-IAP Using Automatic Image Check on page 15](#)
- [Upgrading an Image Using CLI on page 16](#)

## Upgrading an OAW-IAP and Image Server

AOS-W supports mixed OAW-IAP-class AOS-W deployment with all OAW-IAPs as part of the same virtual switch cluster.

### Image Management Using OmniVista

If the multiclass OAW-IAP network is managed by OmniVista, image upgrades can only be done through the OmniVista UI. The OAW-IAP images for different classes must be uploaded on the AMP server. When new OAW-IAPs joining the network need to synchronize their software with the version running on the virtual switch, and if the new OAW-IAP belongs to a different class, the image file for the new OAW-IAP is provided by OmniVista. If OmniVista does not have the appropriate image file, the new OAW-IAP will not be able to join the network.



NOTE

---

The virtual switch communicates with the OmniVista server if OmniVista is configured. If OmniVista is not configured on the OAW-IAP, the image is requested from the image server.

---

### Image Management Using Cloud Server

If the multiclass OAW-IAP network is not managed by OmniVista, image upgrades can be done through the Cloud-Based Image Check feature. When a new OAW-IAP joining the network needs to synchronize its software version with the version on the VC and if the new OAW-IAP belongs to a different class, the image file for the new OAW-IAP is provided by the cloud server.

## Configuring HTTP Proxy on an OAW-IAP

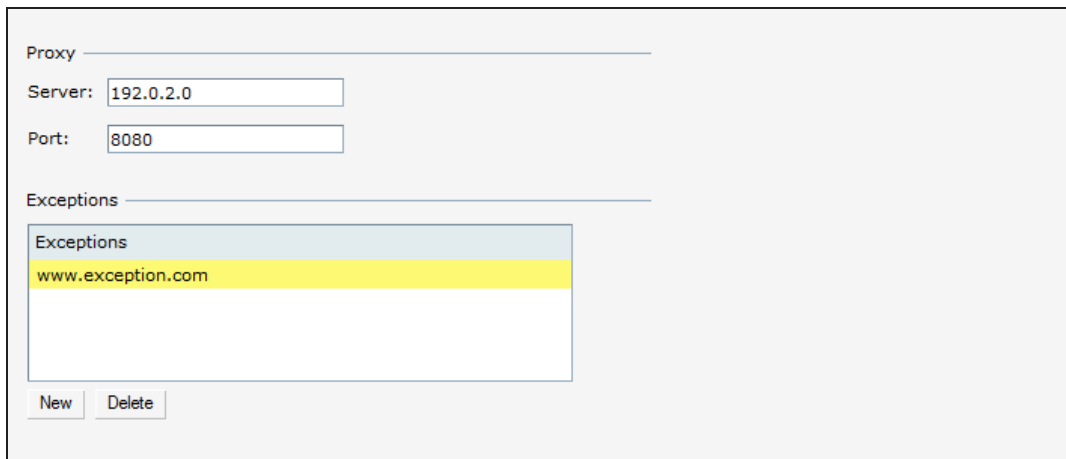
If your network requires a proxy server for Internet access, ensure that you configure the HTTP proxy on the OAW-IAP to download the image from the cloud server. After setting up the HTTP proxy settings, the OAW-IAP connects to the Activate server, AMP or OpenDNS server through a secure HTTP connection. You can also exempt certain applications from using the HTTP proxy (configured on an OAW-IAP) by providing their host name or IP address under exceptions.

### In the AOS-W UI

To configure the HTTP proxy settings:

1. Navigate to **System > Proxy**. The Proxy configuration window is displayed.

**Figure 1** Proxy Configuration Window



The screenshot shows the Proxy Configuration Window. It has a title bar 'Proxy' and a 'Server' section with two input fields: 'Server' (192.0.2.0) and 'Port' (8080). Below is an 'Exceptions' section with a list box containing 'www.exception.com' (highlighted) and two buttons: 'New' and 'Delete'.

2. Enter the HTTP proxy server IP address in the **Server** text box.
3. Enter the port number in the **Port** text box.
4. If you do not want the HTTP proxy to be applied for a particular host, click **New** to enter that IP address or domain name of that host in the **Exceptions** section.

### In the CLI

To configure the HTTP proxy settings:

```
(Instant AP) (config)# proxy server 192.0.2.1 8080
(Instant AP) (config)# proxy exception 192.0.2.2
(Instant AP) (config)# end
(Instant AP)# commit apply
```

## Upgrading an OAW-IAP Using Automatic Image Check

You can upgrade an OAW-IAP by using the Automatic Image Check feature. The automatic image checks are performed once, as soon as the OAW-IAP boots up and every week thereafter.

If the image check locates a new version of the AOS-W software on the image server, the New version available link is displayed on the AOS-W main window.



---

If OmniVista is configured, the automatic image check is disabled.

---

To check for a new version on the image server in the cloud:

1. Go to **Maintenance > Automatic > Check for New Version**. After the image check is completed, one of the following messages is displayed:
  - No new version available—If there is no new version available.
  - Image server timed out—Connection or session between the image server and the OAW-IAP is timed out.
  - Image server failure—If the image server does not respond.
  - A new image version found—If a new image version is found.
2. If a new version is found, the Upgrade Now button becomes available and the version number is displayed.
3. Click **Upgrade Now**.

The OAW-IAP downloads the image from the server, saves it to flash, and reboots. Depending on the progress and success of the upgrade, one of the following messages is displayed:

- Upgrading—While image upgrading is in progress.
- Upgrade successful—When the upgrading is successful.
- Upgrade failed—When the upgrading fails.

If the upgrade fails and an error message is displayed, retry upgrading the OAW-IAP.

### Upgrading to a New Version Manually

If the Automatic Image Check feature is disabled, you can obtain an image file from a local file system or from a TFTP or HTTP URL.

To manually check for a new firmware image version and obtain an image file:

1. Navigate to **Maintenance > Firmware**.
2. Under Manual section, perform the following steps:
  - Select the Image file option. This method is only available for single-class OAW-IAPs.
    - The following examples describe the image file format for different OAW-IAP models:
      - For OAW-AP203H—AlcatelInstant\_Vela\_6.5.4.2\_xxxx

- For OAW-AP334/335—AlcatelInstant\_Lupus\_6.5.4.2\_xxxx
  - For OAW-AP314/315 and OAW-AP324/325—AlcatelInstant\_Hercules\_6.5.4.2\_xxxx
  - For OAW-AP224/225, OAW-AP228, OAW-AP214/215, OAW-AP274/275, OAW-AP277—AlcatelInstant\_Centaurus\_6.5.4.2\_xxxx
  - For OAW-AP204/205 and OAW-AP205H—AlcatelInstant\_Taurus\_6.5.4.2\_xxxx
  - For OAW-RAP155/155P—AlcatelInstant\_Aries\_6.5.4.2\_xxxx
  - For OAW-RAP108/109, OAW-AP103, and OAW-AP114/115—AlcatelInstant\_Pegasus\_6.5.4.2\_xxxx
- Select the **Image URL** option. Select this option to obtain an image file from a HTTP, TFTP, or FTP URL.
    - HTTP - http://<IP-address>/<image-file>. For example, http://<IP-address>/AlcatelInstant\_Hercules\_6.5.4.2\_xxxx
    - TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/AlcatelInstant\_Hercules\_6.5.4.2\_xxxx
    - FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/AlcatelInstant\_Hercules\_6.5.4.2\_xxxx
    - FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://alcatel:123456@<IP-address>/AlcatelInstant\_Hercules\_6.5.4.2\_xxxx




---

The FTP server supports both **anonymous** and **username:password** login methods.

---

3. Clear the **Reboot all APs after upgrade** check box if required. The **Reboot all APs after upgrade** check box is selected by default to allow the OAW-IAPs to reboot automatically after a successful upgrade. To reboot the OAW-IAP at a later time, clear the **Reboot all OAW-IAPs after upgrade** check box.
4. Click **Upgrade Now** to upgrade the OAW-IAP to the newer version.

## Upgrading an Image Using CLI

To upgrade an image using a HTTP, TFTP, or FTP URL:

```
(Instant AP) # upgrade-image <ftp/tftp/http-URL>
```

To upgrade an image by using the username and password in the FTP URL :

```
(Instant AP) # upgrade-image ftp://Alcatel:123456@192.0.2.7/AlcatelInstant_Hercules_6.5.4.2_xxxx
```

To upgrade an image without rebooting the OAW-IAP:

```
(Instant AP) # upgrade-image2-no-reboot <ftp/tftp/http-URL>
```

To view the upgrade information:

```
(Instant AP) # show upgrade info
```

```
Image Upgrade Progress
```

```
-----
```

```
Mac IP Address AP Class Status Image Info Error Detail
```

```
-----
```



```
d8:c7:c8:c4:42:98 10.17.101.1 Hercules image-ok image file none
Auto reboot :enable
Use external URL :disable
```

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

---

**3DES**

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

**3G**

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

**3GPP**

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

**4G**

Fourth Generation of Wireless Mobile Telecommunications Technology. See LTE.

**802.11**

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

**802.11 bSec**

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

**802.11a**

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

**802.11ac**

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

---

**802.11b**

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

**802.11d**

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

**802.11e**

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

**802.11g**

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

**802.11h**

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

**802.11i**

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

**802.11j**

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

---

**802.11k**

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

**802.11m**

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

**802.11n**

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

**802.11r**

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

**802.11u**

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

**802.11v**

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

**802.1Q**

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

**802.1X**

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

**802.3af**

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

**802.3at**

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

---

**AAA**

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

**ABR**

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

**AC**

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

**ACC**

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

**Access-Accept**

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

**Access-Reject**

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

**Access-Request**

RADIUS packet sent to a RADIUS server requesting authorization.

**Accounting-Request**

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

**Accounting-Response**

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

**ACE**

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

**ACI**

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

---

**ACL**

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

**Active Directory**

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

**ActiveSync**

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

**ad hoc network**

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

**ADO**

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

**ADP**

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

**AES**

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

**AIFSN**

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

**AirGroup**

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

---

**AirWave Management Client**

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

**ALE**

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

**ALG**

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

**AM**

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

**AMON**

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

**AMP**

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

**A-MPDU**

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

**A-MSDU**

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

**ANQP**

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

---

**ANSI**

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

**API**

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

**app**

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

**ARM**

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

**ARP**

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

**Aruba Activate**

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

**ASCII**

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

**band**

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

**BGP**

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

**BLE**

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

**BMC**

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



---

**BPDU**

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

**B-RAS**

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

**BRE**

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

**BSS**

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

**BSSID**

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

**BYOD**

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

**CA**

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

**CAC**

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

**CALEA**

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

**Campus AP**

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

---

**captive portal**

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

**CCA**

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

**CDP**

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

**CDR**

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

**CEF**

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

**CGI**

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

**CHAP**

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

**CIDR**

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

**ClearPass**

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

**ClearPass Guest**

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

---

**ClearPass Policy Manager**

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

**CLI**

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

**CN**

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

**CNA**

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

**CoA**

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

**CoS**

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

**CPE**

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

**CPsec**

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

**CPU**

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

**CRC**

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

**CRL**

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

---

**cryptobinding**

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

**CSA**

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

**CSMA/CA**

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

**CSR**

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

**CSV**

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

**CTS**

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

**CW**

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

**DAI**

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

**DAS**

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

**dB**

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

---

**dBm**

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

**DCB**

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

**DCE**

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

**DCF**

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

**DDMO**

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

**DES**

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

**designated router**

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

**destination NAT**

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

**DFS**

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

**DFT**

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

---

**DHCP**

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

**DHCP snooping**

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

**digital certificate**

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

**Digital wireless pulse**

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

**Disconnect-Ack**

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

**Disconnect-Nak**

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

**Disconnect-Request**

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

**distribution certificate**

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

**DLNA**

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

**DMO**

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

**DN**

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

---

**DNS**

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

**DOCSIS**

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

**DoS**

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

**DPD**

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

**DPI**

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

**DRT**

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

**DS**

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

**DSCP**

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

**DSL**

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

**DSSS**

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

---

the resistance to interference. See FHSS.

**DST**

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

**DTE**

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

**DTIM**

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

**DTLS**

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

**dynamic authorization**

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

**dynamic NAT**

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

**EAP**

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

**EAP-FAST**

EAP – Flexible Authentication Secure Tunnel (tunneled).

**EAP-GTC**

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

**EAP-MD5**

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



---

**EAP-MSCHAP**

EAP Microsoft Challenge Handshake Authentication Protocol.

**EAP-MSCHAPv2**

EAP Microsoft Challenge Handshake Authentication Protocol Version 2.

**EAPoL**

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

**EAP-PEAP**

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

**EAP-PWD**

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

**EAP-TLS**

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

**EAP-TTLS**

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

**ECC**

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

**ECDSA**

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

**EDCA**

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

---

**EIGRP**

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

**EIRP**

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

**ESI**

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

**ESS**

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

**ESSID**

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

**Ethernet**

Ethernet is a network protocol for data transmission over LAN.

**EULA**

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

**FCC**

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

**FFT**

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

**FHSS**

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

**FIB**

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

---

**FIPS**

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

**firewall**

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

**FQDN**

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

**FQLN**

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

**frequency allocation**

Use of radio frequency spectrum as regulated by governments.

**FSPL**

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

**FTP**

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

**GARP**

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

**GAS**

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

**gateway**

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

**Gbps**

Gigabits per second.

---

**GBps**

Gigabytes per second.

**GET**

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

**GHz**

Gigahertz.

**GMT**

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

**goodput**

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

**GPS**

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

**GRE**

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

**GTC**

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

**GVRP**

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

**H2QP**

Hotspot 2.0 Query Protocol.

**hot zone**

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

---

**hotspot**

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

**HSPA**

High-Speed Packet Access.

**HT**

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

**HTTP**

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

**HTTPS**

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

**IAS**

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

**ICMP**

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

**IDS**

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

**IEEE**

Institute of Electrical and Electronics Engineers.

**IGMP**

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

---

**IGMP snooping**

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

**IGP**

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

**IGRP**

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

**IKE**

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

**IKEv1**

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

**IKEv2**

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

**IoT**

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

**IPM**

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

**IPS**

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

---

**IPsec**

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

**IPSG**

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

**IrDA**

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

**ISAKMP**

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

**ISP**

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

**JSON**

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

**Kbps**

Kilobits per second.

**KBps**

Kilobytes per second.

**keepalive**

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

**L2TP**

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

---

**LACP**

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

**LAG**

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

**LAN**

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

**LCD**

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

**LDAP**

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

**LDPC**

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

**LEAP**

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

**LED**

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

**LEEF**

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

**LI**

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



---

**LLDP**

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

**LLDP-MED**

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

**LMS**

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

**LNS**

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

**LTE**

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

**MAB**

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

**MAC**

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

**MAM**

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

**Mbps**

Megabits per second

**MBps**

Megabytes per second

---

**MCS**

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

**MD4**

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

**MD5**

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

**MDAC**

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

**MDM**

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

**mDNS**

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

**MFA**

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

**MHz**

Megahertz

**MIB**

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

**microwave**

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

**MIMO**

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

---

**MISO**

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

**MLD**

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

**MPDU**

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

**MPLS**

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

**MPPE**

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

**MS-CHAP**

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

**MS-CHAPv1**

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

**MS-CHAPv2**

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

**MSS**

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

**MSSID**

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

**MSTP**

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

---

**MTU**

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

**MU-MIMO**

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

**MVRP**

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

**mW**

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

**NAC**

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

**NAD**

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

**NAK**

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

**NAP**

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

**NAS**

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

**NAT**

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

---

**NetBIOS**

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

**netmask**

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

**NFC**

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

**NIC**

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

**Nmap**

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

**NMI**

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

**NMS**

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

**NOE**

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

**NTP**

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

**OAuth**

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

**OCSP**

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

---

**OFDM**

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

**OID**

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

**OKC**

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

**onboarding**

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

**OpenFlow**

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

**OpenFlow agent**

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

**Optical wireless**

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

**OSI**

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

**OSPF**

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

**OSPFv2**

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

---

**OUI**

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

**OVA**

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

**OVF**

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

**PAC**

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

**PAP**

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

**PAPI**

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

**PBR**

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

**PDU**

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

**PEAP**

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

**PEF**

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

---

**PEFNG**

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

**PEFV**

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

**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 APs extend corporate network to the users working from home or at temporary work sites. Remote APs are deployed at branch office sites and are connected to the central network on a WAN link.

**REST**

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

**RF**

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

**RFC**

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

**RFID**

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

**RIP**

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

**RJ45**

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

**RMA**

Return Merchandise Authorization. RMA is a part of the product returning process that authorizes users to return a product to the manufacturer or distributor for a refund, replacement, or repair. The customers who want to return a product within its Warranty period contact the manufacturer to initiate the product returning process. The manufacturer or the seller generates an authorization number for the RMA, which is used by the customers, when returning a product to the warehouse.

---

**RMON**

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

**RoW**

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

**RSA**

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

**RSSI**

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

**RSTP**

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

**RTCP**

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

**RTLS**

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

**RTP**

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

**RTS**

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

**RTSP**

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

**RVI**

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

---

**RW**

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

**SA**

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

**SAML**

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

**SCEP**

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

**SCP**

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

**SCSI**

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

**SDN**

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

**SDR**

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

**SDU**

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

**SD-WAN**

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

---

**SFP**

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

**SFP+**

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

**SFTP**

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

**SHA**

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

**SIM**

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

**SIP**

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

**SIRT**

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

**SKU**

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

**SLAAC**

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

**SMB**

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

**SMS**

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

**SMTP**

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

---

**SNIR**

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

**SNMP**

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

**SNMPv1**

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

**SNMPv2**

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

**SNMPv2c**

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

**SNMPv3**

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

**SNR**

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

**SNTP**

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

**SOAP**

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

**SoC**

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

---

**source NAT**

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

**SSH**

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

**SSID**

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

**SSL**

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

**SSO**

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

**STBC**

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

**STM**

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

**STP**

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

**subnet**

Subnet is the logical division of an IP network.

**subscription**

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

**SU-MIMO**

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



---

**SVP**

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

**SWAN**

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

**TAC**

Technical Assistance Center.

**TACACS**

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

**TACACS+**

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

**TCP**

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

**TCP/IP**

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

**TFTP**

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

**TIM**

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

**TKIP**

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

---

**TLS**

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

**TLV**

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

**ToS**

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

**TPC**

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

**TPM**

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

**TSF**

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

**TSPEC**

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

**TSV**

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

**TTL**

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

**TTY**

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

**TXOP**

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

---

frames. TXOP is defined by a start time and a maximum duration.

**UAM**

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

**U-APSD**

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

**UCC**

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

**UDID**

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

**UDP**

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

**UDR**

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

**UHF**

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

**UI**

User Interface.

**UMTS**

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

**UPnP**

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

---

**URI**

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

**URL**

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

**USB**

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

**UTC**

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

**UWB**

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

**VA**

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

**VBR**

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

**VHT**

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

**VIA**

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

**VLAN**

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

**VM**

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

---

**VoIP**

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

**VoWLAN**

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

**VPN**

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

**VRD**

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

**VRF**

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

**VRF Plan**

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

**VRRP**

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

**VSA**

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

**VTP**

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

**walled garden**

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

---

**WAN**

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

**WASP**

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

**WAX**

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

**W-CDMA**

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

**web service**

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

**WEP**

Wired Equivalent Privacy. WEP is a security protocol that is specified in 802.11b 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.

**WIDS**

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

**Wi-Fi**

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

**WiMAX**

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

---

**WIP**

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

**WIPS**

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

**WISP**

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

**WISPr**

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

**WLAN**

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

**WME**

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

**WMI**

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

**WMM**

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

**WPA**

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

---

**WPA2**

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

**WSDL**

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

**WSP**

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

**WWW**

World Wide Web.

**X.509**

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

**XAuth**

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

**XML**

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

**XML-RPC**

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

**ZTP**

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